www.jusletter.ch

David Rosenthal

Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet

Mit mehr als drei Monaten Verspätung präsentierte der Bundesrat am 21. Dezember 2016 den Vorentwurf für ein totalrevidiertes Datenschutzgesetz. Vieles, was er bietet, war erwartet worden. Dennoch stösst das «Weihnachtsgeschenk» auf enorme Resonanz. Insbesondere die strafrechtlichen Sanktionen sorgen für heftige Kritik. Doch der Vorentwurf birgt noch ganz anderen Zündstoff, der allerdings erst auf den zweiten und dritten Blick sichtbar wird. Der Beitrag legt diesen offen und beleuchtet, welche Folgen die Regelungen des Vorentwurfs für die Schweizer Wirtschaft hätten. Denn eines wird klar: Es besteht noch erheblicher Nachbesserungsbedarf.

Beitragsarten: Beiträge
Rechtsgebiete: Datenschutz

Zitiervorschlag: David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20. Februar 2017

Inhaltsübersicht

[Rz 1] Viele Experten – so auch der Autor dieses Beitrags – sind der Ansicht, dass das bestehende Datenschutzgesetz (DSG) in der Sache vollauf genügt, selbst in Anbetracht der schnellen technischen Entwicklungen im Bereich der Informationstechnologie. In seiner Durchsetzung ist es wesentlich effizienter und kostengünstiger als es das neue DSG sein wird. Die Frage nach dem Sinn einer Revision des DSG ist jedoch aus zwei Gründen müssig: Erstens wird die revidierte Konvention 108 des Europarats[1], auf welchem schon das bisherige DSG aufbaut, diverse Anpassungen erforderlich machen.[2] Zweitens dominiert nicht nur in Bundesbern die Angst, die Schweiz könnte ihre Anerkennung als Land mit angemessenem Datenschutz durch die EU verlieren, sollte die Schweiz ihr DSG nicht massiv verschärfen. Ein solches Risiko besteht freilich nach der vorliegend vertretenen Auffassung nicht wirklich, und zwar schon gar nicht, wenn die Schweiz die revidierte Konvention 108 umsetzt, welche den freien Datenfluss mit der EU explizit vorsieht. Die Schweiz gibt sich in diesen Dingen viel zu wenig selbstbewusst. Wenn schon die Einhaltung des «Privacy Shield» für Exporte in die USA als ein datenschutzrechtlich angemessener Standard gilt[3], so wäre bereits das heutige Schweizer Recht hinreichend. Die Angst vor der EU ist somit ein schlechter Berater in dieser Sache. Schon gar nicht ist es angezeigt, in einem revidierten DSG über die Anforderungen der EU hinauszugehen.

[Rz 2] Noch bis zum 4. April 2017 ist es möglich, zum Vorentwurf für das revidierte DSG (VE DSG)[4] Stellung zu nehmen. Es ist davon auszugehen, dass die Vernehmlassung ein grosses Echo auslösen wird, was zu begrüssen ist. Das Bundesamt für Justiz dürfte versuchen, eine entspre-

1 Abrufbar unter http://www.coe.int/en/web/data-protection/modernisation-convention108 (bisher nur im Entwurf), Alle Websites zuletzt besucht am 13. Februar 2017.

2 Über deren Sinnhaftigkeit kann zwar gestritten werden, aber als die breitere politische Öffentlichkeit in Bundesbern von der Revision der Konvention Wind bekam, war es bereits zu spät. Zudem wird auch der Europarat von der EU dominiert, welche im Rahmen der Revision ihre Bedürfnisse, wie sie in der DSGVO ihren Niederschlag fanden, zu grossen Teilen durchgedrückt hat.

3 Vgl. etwa http://europa.eu/rapid/press-release_IP-16-2461_de.htm.

4 https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2016/2016-12-21.html; eine englische Fassung ist erhältlich unter http://datenrecht.ch/vorentwurf-des-dsg-englische-fassung/.

chende Botschaft auszuarbeiten, die der Bundesrat möglichst noch vor der Sommerpause dieses Jahres dem Parlament unterbreiten müsste. In der Herbstsession würde dann das Geschäft in der Kommission des Erstrates, in der Wintersession im Plenum beraten werden können. Genügt dies, wird der Zweitrat sich in der Frühjahres- und Sommersession damit befassen können und das revidierte DSG im Sommer oder Herbst 2018 verabschiedet werden können. Damit ist ein Inkrafttreten frühestens auf Januar 2019 möglich, also etwas mehr als ein halbes Jahr nach dem Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018, die bekanntlich für eine ganze Reihe von Schweizer Firmen ebenfalls Anwendung findet. Ein solcher Zeitplan würde es erforderlich machen, dass das Bundesamt für Justiz noch während der parlamentarischen Beratung an den Ausführungsverordnungen arbeitet. Inzwischen halten einige einen solchen Fahrplan für viel zu optimistisch.

[Rz 3] Im Folgenden werden die neuen Regelungen des VE DSG erörtert, welche die Privatwirtschaft betreffen. Auf den behördlichen Datenschutz wird hier nicht eingegangen, auch nicht auf die Anpassungen im Zusammenhang mit Schengen. Wie gezeigt werden wird, haben es einige der Bestimmungen in sich, und sie gehen durchaus über das hinaus, was nach der DSGVO erforderlich ist. Ob ein solcher «Swiss Finish» wirklich sinnvoll ist, wird im Rahmen der Vernehmlassung zu klären sein. Vorliegend wird die Ansicht vertreten, dass strengere oder inkompatible Schweizer Alleingänge zweifellos nicht sinnvoll sind. Dies dürfte auch dem gegenwärtigen politischen Trend entsprechen. Es ist somit noch mit einigen Änderungen zu rechnen.

[Rz 4] Dies gilt im Übrigen auch für die sprachliche Ausgestaltung insbesondere der deutschen Fassung des Gesetzes, die gegenüber der französischen deutlich abfällt, die vermutlich Ausgangspunkt der Arbeiten war. Auf diese Punkte wird in diesem Beitrag nicht näher eingegangen. Es wäre aber sinnvoll, auf die Einheitlichkeit der Begrifflichkeiten zu achten. So ist zum Beispiel nicht ersichtlich, warum in Art. 14 VE DSG das eine Mal von einer «Bekanntgabe» von Personendaten die Rede ist und im nächsten Absatz von deren «Übermittlung».

1. Geltungsbereich wird eingeschränkt und ausgeweitet

[Rz 5] Die wichtigste Änderung im Geltungsbereich des revidierten DSG war schon vor dem VE DSG klar: Der Schutz juristischer Personen fällt weg. Erfasst sein soll neu nur noch die Bearbeitung von Daten, die sich auf eine bestimmte oder bestimmbare *natürliche* Person beziehen. Das entspricht der Regelung in fast allen Ländern. Die Anpassung wird kaum zu Diskussionen Anlass geben, auch wenn sie weder systemtreu noch wirklich konsequent ist: Nach Art. 28 des Schweizerischen Zivilgesetzbuches (ZGB), welcher durch das DSG konkretisiert wird, geniessen auch juristische Personen Persönlichkeitsschutz, und sie tun es weiterhin; Art. 13 der Bundesverfassung (BV) gewährleistet den Schutz der Persönlichkeit auch von juristischen Personen. Eine Verletzung durch die Bearbeitung von Personendaten von juristischen Personen ist also über diesen Umweg nach wie vor möglich, wenngleich die Fälle eher selten sein werden.[5] Der Vorteil der Streichung wird sein, dass die formalen Vorschriften betreffend Daten über Firmen wegfallen. Dies wird etwa dem Schindluder mit dem Auskunftsrecht nach dem heutigen Art. 8 DSG (Art.

[5] Das DSG wird hierbei vermutlich analog beigezogen werden. Werden also Daten einer Firma zweckwidrig verwendet, kann argumentiert werden, dass dies Art. 28 ZGB verletzt, weil ein solches Verhalten gemäss DSG eine Persönlichkeitsverletzung darstellt.

20 VE DSG) bei Unterlagen betreffend juristische Personen Einhalt bieten; das Auskunftsrecht dient heute primär der Beschaffung von Beweismitteln für Prozesse und anderen, datenschutzfremden Zwecken, was aber durch die bisherige Gerichtspraxis leider ohne Not geschützt wird.[6] Allerdings darf die Wirkung der Streichung des Schutzes juristischer Personen nicht überbewertet werden: Unternehmen handeln regelmässig durch ihre Organe und Hilfspersonen, und deren Personendaten sind weiterhin durch das DSG erfasst und zwar auch im professionellen Kontext.[7]

[Rz 6] Geht es um Daten natürlicher Personen, wird dem Auskunftsrecht mit dem VE DSG allerdings eine noch grössere Bühne bereitet als bisher: Das DSG soll künftig – ausser für die Gerichte selbst[8] – selbst im Rahmen bereits hängiger Zivilprozesse und laufender Strafverfahren gelten. Somit kann neu selbst während solchen Verfahren weiterhin das Auskunftsrecht zur Beweisbeschaffung benutzt werden, was für eine betroffene Person zweifellos attraktiv ist, da für diese Form der Beweisbeschaffung weder etwas bezahlt werden muss, noch sonst die hohen Hürden der Zivilprozessordnung für Editionsbegehren gelten. Der Missbrauch ist damit leider vorprogrammiert und dürfte mangels sinnvoller Anpassung des Auskunftsrechts in Art. 20 f. VE DSG (vgl. Rz 54 ff., hinten) von den Gerichten weiterhin geschützt werden.

[Rz 7] Der Vorentwurf ändert nicht nur den Geltungsbereich, sondern auch die Begrifflichkeiten in einigen Bereichen. Die gewichtigste Anpassung dürfte die Abschaffung der «Persönlichkeitsprofile» und deren Ersatz durch den Begriff des «Profiling» sein. Dieser umfasst nach Art. 3 Bst. f VE DSG «jede Auswertung von Daten oder Personendaten, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, Intimsphäre oder Mobilität». Diese Definition ist extrem breit, und die Schweiz geht damit deutlich über die entsprechende Regelung der EU hinaus. Anders als in der DSGVO ist auch das Profiling von Hand erfasst, also beispielsweise das Ausfüllen einer Mitarbeiterbeurteilung oder die Einschätzung eines Arztes, wie sich die Krankheit einer Person entwickeln wird. Aber auch die Versicherung, die im Rahmen einer Police ein Alterskapital berechnet, nimmt nach dem Wortlaut der VE DSG ein Profiling vor, da sie eine Entwicklung bezüglich wirtschaftlicher Lage des Versicherten prognostiziert. Dies alles gilt neu nach Art. 23 Abs. 2 Bst. d VE DSG *per se* als Persönlichkeitsverletzung, was wiederum einen Rechtfertigungsgrund erfordert, falls nicht vorgängig eine ausdrückliche Einwilligung eingeholt worden ist. Eine solche Regelung erscheint doch etwas übertrieben.

[Rz 8] Ob für das Profiling Personendaten benutzt werden oder nicht, spielt zudem keine Rolle («Daten oder Personendaten»). Die Befürchtung, dass damit auch das Bearbeiten von nicht personenbezogenen Daten plötzlich erfasst wäre, dürfte zwar unberechtigt sein: Hier greift Art. 2 Abs. 1 VE DSG, wonach das DSG nur dann gilt, wenn Personendaten bearbeitet werden. Ein Profiling ist somit dann erfasst, wenn sich mindestens das Ergebnis auf eine bestimmte oder bestimmbare Person bezieht. Die Formulierung «Daten oder Personendaten» ist trotzdem unnötig

---

6 Vgl. statt vieler BGE 138 III 425 und Urteil des Bundesgerichts 4A_506/2014 vom 3. Juli 2015; vgl. auch David Rosenthal, Aktuelle Anwaltspraxis 2013, S. 731 ff.; ders., Aktuelle Anwaltspraxis 2015, S. 586 ff.

7 Hierbei ist auf Erwägung 14 der DSGVO hinzuweisen, die erklärt, dass die DSGVO keine Anwendung finden soll auf die Kontaktdaten juristischer Personen, was häufig natürliche Personen sind. Die Tragweite dieser Erklärung ist allerdings nicht klar. Es gibt etliche Daten natürlicher Personen in ihrer Eigenschaft als Arbeitnehmer einer juristischen Person, die ohne Weiteres schutzwürdig sind.

8 Der VE DSG regelt nur noch die eidgenössischen Gerichte; die Datenbearbeitung der kantonalen Gerichte wird von den kantonalen Datenschutzgesetzen geregelt werden müssen. Allerdings ist die diesbezügliche Regelung in Art. 57 VE DSG mit Bezug auf Art. 2 Abs. 3 VE DSG nicht korrekt formuliert. Es fehlt der Hinweis, dass die Regelungen für eidgenössische Gerichte im kantonalen Recht sinngemäss für kantonale Gerichte umzusetzen ist.

und irreführend: Handelt es sich beim Output eines Profilings um Personendaten, muss es sich naturgemäss auch beim Input um solche handeln, weil ein Personenbezug offenkundig möglich ist, wie das Profiling selbst beweist. Der Hinweis auf «Daten» ist daher zu streichen.

[Rz 9] Der Katalog der besonders schützenswerten Personendaten wurde wie von der revidierten Konvention 108 vorgegeben um genetische und biometrische Daten erweitert, letztere mit der Einschränkung, dass nur Daten gemeint sind, die eine natürliche Person eindeutig identifizieren. Diese Beschränkung ist allerdings wenig hilfreich: Jedes Gesichtsfoto soll nach dem Vorentwurf künftig als besonders schützenswertes Personendatum gelten. Gedacht war die Regelung an sich etwas enger: Gemäss dem Erläuterungsbericht sollen nur jene Fotos erfasst sein, die mit spezifischen technischen Mittel so bearbeitet wurden, dass eine eindeutige Identifizierung oder Authentisierung eines Individuums möglich ist. Gemeint sind also Fälle der Gesichtserkennung, wobei die meisten Fälle wiederum aufgrund fehlender Zuverlässigkeit in der Erkennung wegfallen dürften. Hier besteht somit noch Nachbesserungsbedarf in der Legaldefinition. Erfasst sein sollten nach Art. 3 Bst. c Ziff. 4 VE DSG nicht jene biometrische Daten, die eine natürliche Person eindeutig identifizieren, sondern nur solche, die zum Zweck bearbeitet werden, dies zu tun. Mehr verlangt auch die Konvention 108 nicht. Bilder in der Zeitung, auf welchen Personen zu erkennen sind, wären nach dieser Definition somit nicht mehr besonders schützenswerte Personendaten, während dies gemäss Vorentwurf noch so wäre.

[Rz 10] Weggefallen ist auch das Konzept der Inhaberschaft einer Datensammlung. Es wurde ersetzt durch den in der EU schon seit langem gebräuchlichen Begriff des «Verantwortlichen» (*Controller*) und des «Auftragsbearbeiters» (*Processor*). Die Definition des Verantwortlichen gibt aber nicht ganz das in Europa herrschende Begriffsverständnis wieder: Der Verantwortliche zeichnet sich nicht dadurch aus, dass er über Zweck, Mittel und Umfang der Bearbeitung der Daten entscheidet, sondern dass er dies *final* tut oder tun kann, also der «Herr der Daten» ist. In der Praxis wird der Entscheid über die Mittel und den Umfang der Datenbearbeitung häufig dem Auftragsbearbeiter delegiert, wie z.B. auch die Bestimmung der angemessenen Schutzmassnahmen. In den Erläuterungen wird ohne Begründung vertreten, dass die Arbeitnehmer eines Verantwortlichen nicht als Auftragsbearbeiter gelten, was systematisch und dogmatisch falsch ist. Die Regeln der Auftragsbearbeitung müssen auch im Verhältnis zu den eigenen Arbeitnehmern gelten, denen ein Unternehmen die Bearbeitung von Daten anvertraut, auch wenn die Genehmigung nach Art. 7 Abs. 3 VE DSG regelmässig implizit als erteilt gelten wird und die Information nach Art. 13 Abs. 4 VE DSG für diese Fälle keinen Sinn macht. Diese beiden Neuerungen sollten daher relativiert werden.

[Rz 11] Anpassungsbedarf besteht ferner bezüglich der Verantwortlichkeiten des Auftragsbearbeiters: Zahlreiche der neuen Bestimmungen nehmen nicht nur den Verantwortlichen in die Pflicht, sondern parallel auch den Auftragsbearbeiter. Dieser wird jedoch oftmals gar nicht in der Lage sein, aus eigenem Antrieb oder in eigener Verantwortlichkeit diesen Pflichten nachzukommen; in der DSGVO werden die Auftragsbearbeiter nicht derart in die Pflicht genommen. Beispiele hierfür sind die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (Art. 16 VE DSG), *Privacy by Design* und *Privacy by Default* (Art. 18 VE DSG) oder die Information von Datenempfängern über etwaige Berichtungen oder Löschungen von Daten (Art. 19 VE DSG). Für all diese Aufgaben kann sinnvollerweise nur der Verantwortliche verantwortlich sein, auch wenn er zu deren Umsetzung allenfalls die Hilfe eines Auftragsbearbeiters beanspruchen wird.

[Rz 12] Der Begriff der Datensammlung selbst soll im revidierten DSG ebenfalls weggefallen. Dogmatisch und systematisch war das Konzept der Inhaberschaft sauberer und differenzierter

als die neue Lösung, aber sie war seit je her selbst für Spezialisten schwer zu verstehen. Die Anpassung erscheint als Massnahme zur Harmonisierung mit den internationalen Gepflogenheiten im Datenschutzrecht daher sinnvoll. Sie hat immerhin die Folge, dass diverse Pflichten ausgeweitet werden: Das Auskunftsrecht nach Art. 8 DSG galt bisher nur für Daten in Datensammlungen; neu soll es jedenfalls nach dem Wortlaut für alle Daten, die ein Verantwortlicher bearbeitet, gelten (Art. 20 Abs. 1 VE DSG). Sinngemäss wird es freilich weiterhin nur für jene Daten zur Anwendung kommen können, die nach der betroffenen Person erschlossen werden können, denn wenn ein Verantwortlicher selbst nicht ohne Weiteres nach einer bestimmten Person in seinem Datenbestand suchen kann, weil es für seine Datenbearbeitung keine Rolle spielt, wird dies von ihm auch im Rahmen des Auskunftsrechts nicht verlangt werden können. Anwendungsfälle, wo sich der Unterschied zeigt, könnten zum Beispiel Aufnahmen von Sicherheitskameras sein: Sie sind regelmässig keine Datensammlung, da sie nicht nach betroffenen Personen erschlossen werden können. Gibt eine Person unter neuem Recht an, wann sie von einer Kamera erfasst wurde und will sie die Aufnahme sehen, wird ihr dieser Zugang unter neuem Recht gewährt werden müssen. Die praktische Relevanz ist in diesem Falle allerdings beschränkt: Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) stellt sich aufgrund des gefühlten Datenschutzes und ohne Rechtsgrundlage auf den Standpunkt, dass schon unter heutigem Recht eine Auskunftspflicht besteht, und kaum jemand wagte es bisher, ihm zu widersprechen.

2. Kein Methodenwechsel bei «Personendaten»

[Rz 13] Vom Wegfall des Schutzes juristischer Personen abgesehen, soll der Begriff der Personendaten auch im neuen Recht so bleiben, wie er ist[9]. Dies war ein mit Spannung erwarteter Punkt und der Entscheid ist richtig und wichtig. Es bleibt somit bei durch die bundesgerichtliche Rechtsprechung bestätigten «relativen» Methode, wenn es darum geht zu ermitteln, ob die betroffene Person bestimmbar ist. Danach genügt es nicht, dass der Aufwand zur Identifizierung objektiv gering genug ist, dass ein Interessent ihn nach allgemeiner Lebenserfahrung auf sich nimmt (objektive Komponente). Wesentlich ist ebenso, welches Interesse der Datenbearbeiter oder ein Dritter mit Zugang zu den Daten an der Identifizierung hat (subjektive Komponente), was vom konkreten Fall abhängig ist.[10] Es genügt daher nicht wie bei der «absoluten» Methode, dass irgendjemandem die Identifizierung möglich ist. Obwohl in der EU immer wieder die «absolute» Methode vertreten wird, hat der EuGH kürzlich auch für das geltende EU-Recht die relative Methode bestätigt.[11]

[Rz 14] Daran dürfte sich auch unter der DSGVO bei richtiger Auslegung nichts ändern. Zwar wird im Falle der DSGVO teilweise vertreten, dass bereits dann Personendaten vorliegen, wenn sie eine «Singularisierung» erlauben, also so spezifisch sind, dass sie sich nur noch auf eine bestimmte Person beziehen können, selbst wenn sich diese nicht identifizieren lässt. Dies übersieht

9 Erläuterungen VE DSG, S. 43.

10 BGE 136 II 508, E. 3.2.

11 Urteil des EuGH vom 19. Oktober 2016 C-582/14 *Breyer*, welches die Frage der Identifikation des Inhabers einer IP-Adresse zum Inhalt hatte. Während die Bestimmbarkeit der betroffenen Person für den Internet-Service-Provider klar war (RN 33 f., mit Hinweis auf den Urteil des EuGH vom 24. November 2011 C-70/10 *Scarlet Extended*), war sie gemäss EuGH für den Betreiber einer Website, der die IP-Adresse für den Fall von Cyberangriffen aufzeichnete, separat zu prüfen (RN 44–49). Damit folgte der EuGH wie schon zuvor BGE 136 II 508 auch für das EU-Recht der «relativen» Methode.

jedoch, dass die DSGVO die Singularisierung nur als Indiz für eine Identifizierbarkeit vorsieht[12] und sie als Konzept über massive Mängel verfügt, die sie untauglich werden lassen.[13] Wesentlich zuverlässiger ist hierbei der sog. Referenzdaten-Test, wie ihn auch der EuGH angewandt hat.[14]

[Rz 15] Das Festhalten am bisherigen Begriff des Personendatums im Vorentwurf bedeutet insbesondere, dass die Bekanntgabe von pseudonymisierten Daten an Personenkreise, die nicht über den Schlüssel zur Zuordnung der Daten zu betroffenen Personen verfügen, weiterhin *keine* Bekanntgabe von Personendaten darstellen wird und daher auch die diesbezüglichen datenschutzrechtlichen Kautelen nicht beachtet werden müssen. Dies gilt jedenfalls solange die Nichtidentifizierbarkeit der Daten durch die Dritten sichergestellt ist. Das macht auch Sinn. Wäre dem nämlich nicht so, wäre beispielsweise die Bekanntgabe von geschwärzten Unterlagen durch Behörden oder Unternehmen an vielen Orten nicht mehr zulässig, ebenso nicht die Speicherung von vollverschlüsselten Daten auf einem Speichersystem im Internet. Beides sind letztlich Formen der Pseudonymisierung.

3. Bisheriges Regelungskonzept mit Bearbeitungsgrundsätzen bleibt

[Rz 16] Das bisherige Regelungskonzept des DSG, welches von einer generellen Erlaubnis zur Bearbeitung von Personendaten ausgeht und einzelne Fälle definiert, in welchen sie verboten ist, soll bestehen blieben. Es gilt im privaten Bereich somit weiterhin das Prinzip des «opt-out», nicht des «opt-in». Eine Zustimmung zur Bearbeitung von Personendaten ist weiterhin nicht zwingend; anders als in der DSGVO soll es in der Schweiz nicht erforderlich sein, für eine Datenbearbeitung einen Rechtfertigungsgrund vorweisen zu können.[15] Ein Rechtfertigungsgrund wird nur und erst dann benötigt, wenn eine Datenbearbeitung die Persönlichkeit einer betroffenen Person verletzt, was sich neu aus Art. 24 VE DSG ergibt. In welchen Fällen eine Persönlichkeitsverletzung vorliegt, umschreibt Art. 23 VE DSG, welcher gegenüber dem heutigen Art. 12 DSG erweitert wurde.

[Rz 17] Aber auch hier bleibt das Grundkonzept dasselbe: In Art. 23 Abs. 2 VE DSG wird aufgezählt, in welchen Fällen eine Persönlichkeitsverletzung *per se* vorliegt, nämlich bei Verletzung der Bearbeitungsgrundsätze, bei einer Datenbearbeitung gegen den erklärten Willen einer betroffenen Person (wie bisher), bei der Bekanntgabe von besonders schützenswerten Personendaten an Dritte (wie bisher) und beim Profiling ohne ausdrückliche Einwilligung der betroffenen Person.

---

12 Erwägung 26 der DSGVO («To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, . . . »).

13 Beispielsweise wäre ein automatisches Foto einer Person in einer misslichen Lage aufgrund der Einmaligkeit der Aufnahme selbst dann ein Personendatum, wenn ausser dieser Person selbst kein Mensch auf der Welt herausfinden kann, um wen es sich handelt.

14 Hierbei wird geprüft, ob die bearbeiteten Daten bereits verfügbaren oder nach allgemeinem Ermessen wahrscheinlich verfügbaren Daten real existierender Personen eindeutig zugeordnet werden können. Können aus biologischem Material beispielsweise genetische Daten gewonnen werden, so werden diese erst dann zu Personendaten, wenn diese mit Referenzdaten realer, bekannter Personen abgeglichen werden können, wobei solche Referenzdaten oder Vergleichsproben normalerweise nicht verfügbar sein werden (vgl. Botschaft Humanforschungsgesetz, BB 2009 8045, 8096). Denselben Test wendete auch das Urteil des EuGH vom 19. Oktober 2016 C-582/14 *Breyer* an, um festzustellen, ob eine IP-Adressen für einen Website-Provider Personendaten darstellen, was es im konkreten Fall bejahte, da er davon ausging, dass er Zugang zu den Referenzdaten des Internet-Service-Providers erlangen würde. Die Frage der Zugänglichkeit zu Referenzdaten ist jeweils aus der Perspektive derjenigen zu beurteilen, die Zugang zu den bearbeiteten Personendaten haben («relative Methode»).

15 Vgl. Art. 6 DSGVO.

Letztere Regelung ist neu und insofern nicht ganz nachvollziehbar, als dass der Begriff des Profiling extrem breit definiert ist. Dies wird zweifellos noch für Diskussionen sorgen.

[Rz 18] Art. 23 Abs. 2 Bst. a VE DSG führt neu auch Art. 5 und 6 VE DSG auf, welche sich auf die Bekanntgabe ins Ausland beziehen. Dies ist lediglich eine redaktionelle Klarstellung, denn schon bisher war eine unerlaubte Bekanntgabe ins Ausland als Persönlichkeitsverletzung zu werten. Die Aufzählung von Art. 5 und 6 VE DSG in Art. 23 VE DSG ändert allerdings nichts daran, dass die Rechtfertigungsgründe in Art. 24 VE DSG, insbesondere der Rechtfertigungsgrund des überwiegenden privaten Interesses, in den Fällen von Art. 5 und 6 VE DSG keine Anwendung finden.

[Rz 19] Hinzuweisen ist in diesem Zusammenhang allerdings auf einen Fehler in den Erläuterungen: Diesen zufolge kommt Art. 23 Abs. 3 VE DSG (er handelt von veröffentlichten Daten) angeblich nur zum Tragen, wenn die Bearbeitung von Daten rechtmässig erfolge, d.h. die Grundsätze von Art. 4, 5, 6 und 11 eingehalten würde.[16] Das ist falsch. Abs. 3 führt dazu, dass die Bearbeitung von Daten, die mit Wissen und Willen einer Person publiziert wurden, in der Regel selbst dann rechtmässig ist, wenn sie unter Verletzung der Bearbeitungsgrundsätze erfolgt. Das war schon im bisherigen Recht so.

[Rz 20] Die exemplarische Aufzählung der Fälle, in welchen von einem überwiegenden Interesse auszugehen ist, wurde überarbeitet. Sie entsprechend im Kern der heutigen Regelung von Art. 13 Abs. 2 DSG, mit gewissen geringfügigen Anpassungen:

- Der Rechtfertigungsgrund der Kreditüberprüfung soll nur noch gelten, wenn die betroffene Person volljährig ist, was zwar auf den ersten Blick zum Schutz von Kindern einleuchten mag, aber bei näherer Betrachtung nicht sinnvoll erscheinen: Online-Shops, die auch von nicht volljährigen Kunden genutzt werden, stellen zum Beispiel häufig auf automatisierte Kreditprüfungen ab, in deren Rahmen sie auch erfahren, ob eine Person bereits volljährig ist oder nicht. Auf diese Datenquelle würde verzichtet werden müssen. Nicht volljährige Personen werden notabene mindestens bei gewissen Kreditauskunfteien zwar als solche ausgewiesen, erhalten aber automatisch ein positives Kreditrating. Diese Daten dürfen neu möglicherweise nicht mehr bereitgehalten werden. Weiterhin nicht bearbeitet werden dürfen auch besonders schützenswerte Personendaten, was in jenen Fällen als problematisch erscheint, als dass es sich um Daten zu Verurteilungen im Zusammenhang mit bestimmten Vermögensdelikten handelt, die durchaus von erheblicher Relevanz für die Kreditwürdigkeit einer Person sind.
- Der Rechtfertigungsgrund der nicht-personenbezogenen Bearbeitung erfordert nun nicht mehr nur, dass die Ergebnisse so veröffentlicht werden, dass keine Rückschlüsse auf die betroffenen Personen mehr möglich sind. Auch vorgängig darf Dritten nichts bekanntgegeben werden, was aus deren Sicht Personendaten sind. Sie müssen somit pseudonymisiert oder anonymisiert werden. Zudem wird in Erinnerung gerufen, dass Personendaten anonymisiert werden müssen, sobald es der Zweck der Bearbeitung erlaubt. Das ergab sich allerdings schon bisher aus dem Grundsatz der Verhältnismässigkeit.

[Rz 21] Die Formulierung von Art. 24 Abs. 2 VE DSG ist insofern zurückhaltender geworden, als dass nun davon die Rede ist, dass in den aufgeführten Fällen das überwiegende private Interesse nur noch «möglicherweise» gegeben ist. Gemäss den Erläuterungen soll dies darauf hinwirken,

16 Erläuterungen VE DSG, S. 69.

dass die spezifischen Umstände des Einzelfalls stärker berücksichtigt werden.[17] Für diese Einschränkung gibt es jedoch keinen Grund; die bisherige Regelung und Formulierung hat sich bestens bewährt. Durch die Einführung des Worts «möglicherweise» wird nunmehr die Rechtssicherheit, welche mit Art. 23 Abs. 2 VE DSG geschaffen werden soll, gleich wieder zunichtegemacht. Schon die bisherige Regelung galt nicht absolut, aber sie stellte klar: Gibt es keine gewichtigen Gründe von der Bewertung in Art. 13 Abs. 2 DSG abzuweichen, wird das überwiegende Interesse nach Ansicht des Gesetzgebers gegeben sein. Zu Problemen führte dieses System bisher nicht; dazu sind die aufgezählten Fälle zu klar.

[Rz 22] Die Bearbeitungsgrundsätze wurden im VE DSG sinnvollerweise in Art. 4 zusammengefasst. Es sind jedenfalls auf den ersten Blick keine grundlegenden Änderungen ersichtlich. Der Grundsatz der Zweckbindung und Erkennbarkeit wurde in Art. 4 Abs. 3 VE DSG zusammengefasst. Bisher genügte es für die Zweckbindung, dass eine bestimmte Bearbeitung vom Schweizer Recht vorgeschrieben war. Nach dem neuen Wortlaut und System scheint das nicht mehr der Fall zu sein. Dies würde bedeuten, dass Unternehmen auch auf gesetzlich vorgeschriebene Datenbearbeitungen hinweisen müssen, was wenig sinnvoll erscheint. Dieser Punkt bedarf der Klärung mindestens in den Erläuterungen, wonach die Tatsache, dass eine Bearbeitung gesetzlich vorgesehen ist, diese zugleich auch erkennbar macht.

[Rz 23] Das in Abs. 3 neu eingefügte Erfordernis der «klaren» Erkennbarkeit ist hingegen ersatzlos zu streichen: Es ist nicht ersichtlich, welchen Mehrwert dieser Zusatz hat; eine materielle Änderung gegenüber der heutigen Rechtslage ist erklärtermassen nicht beabsichtigt.[18] Die Deutlichkeit, mit welcher auf einen bestimmten Bearbeitungszweck hinzuweisen ist, ergibt sich schon unter dem heutigen Recht aus dem Risiko, dass mit ihm für die betroffene Person verbunden ist. Es gibt keinen Grund, daran etwas zu ändern. Das Wort «klar» im Zusammenhang mit der Erkennbarkeit des Bearbeitungszwecks sorgt lediglich für Verwirrung.

[Rz 24] Zu begrüssen ist hingegen die Einführung «kompatibler» Bearbeitungszwecke. Nach Art. 4 Abs. 3 Satz 2 VE DSG ist neu die Bearbeitung von Daten auch zu Zwecken erlaubt, die zwar nicht erkennbar, mit den erkennbaren Zwecken aber «vereinbar» sind. Damit greift die Formulierung ein Konzept auf, welches das EU-Recht bereits kennt und in der Praxis gewisse Erleichterungen mit sich bringt.[19] Ein typisches Beispiel ist die Anonymisierung von zu einem Zweck A beschafften Personendaten, um sie für den Zweck B zu verwenden. Der Vorgang der Anonymisierung ist eine Datenbearbeitung, die ihrerseits dem Zweckbindungsgrundsatz unterliegt. Ist dieser Zweck B nicht von Anfang an erkennbar gewesen, verlangt seine Verfolgung an sich einen Rechtfertigungsgrund. Das ist neu nicht mehr der Fall.

[Rz 25] Ein weiteres Praxisbeispiel ist die Beschaffung von Kundendaten zwecks Abwicklung von Verträgen. Will das Unternehmen diese Daten auch für eigene Targeting-, Analyse- oder Marketingzwecke verwenden und hat es dies im Rahmen der Datenbeschaffung nicht angekündigt, so stellt sich unter heutigem Recht die Frage, ob diese Nutzungen mindestens aus den Umständen ersichtlich waren. Ist dem (ausnahmsweise) nicht so, wäre ein Rechtfertigungsgrund erforderlich. Neu entfällt dieses Erfordernis: Beide Nutzungen dürften zwar vom ursprünglichen Be-

17 Erläuterungen VE DSG, S. 69.

18 Erläuterungen VE DSG, S. 46.

19 Art. 6 Abs. 4 DSGVO.

schaffungszweck nicht abgedeckt, mindestens aber mit diesem «vereinbar» sein.[20] Nicht richtig ist allerdings die Aussage in den Erläuterungen, dass eine Weiterbearbeitung dann als vereinbar gilt, wenn sie durch einen Rechtfertigungsgrund wie etwa eine Einwilligung des Betroffenen legitimiert ist;[21] hierbei werden zwei verschiedene Konzepte unzulässigerweise miteinander vermischt. Ob ein neuer Datenbearbeitungzweck mit dem ursprünglichen Zweck vereinbar ist, ergibt sich aus einer inhaltlichen Verwandtschaft, den möglichen Auswirkungen der Datenbearbeitung zum neuen Zweck, vorhandenen Massnahmen zum Schutz der betroffenen Person oder ihrem Verhältnis zum Verantwortlichen.

[Rz 26] Nur scheinbar neu ist der Grundsatz in Art. 4 Abs. 4 VE DSG, welcher eine Anonymisierung von Daten verlangt, sobald der Zweck der Bearbeitung dies erlaubt. In Tat und Wahrheit ergab sich dies schon bisher aus dem Grundsatz der Verhältnismässigkeit, der weiterhin gilt[22]. Neu formuliert wurde auch der Grundsatz der Datenrichtigkeit in Art. 4 Abs. 5 VE DSG, dessen neuer Wortlaut etwas absoluter abgefasst ist, als bisher. Da eine Änderung des bisherigen Rechts nicht beabsichtigt ist,[23] stellt sich allerdings die Frage, warum der Wortlaut angepasst wird; die bisherige Formulierung erscheint sachgerechter.

[Rz 27] Die Verletzung der Bearbeitungsgrundsätze in Art. 4 VE DSG wird notabene weiterhin nicht sanktioniert.

4. Einwilligung: Alles bleibt beim Alten

[Rz 28] Die Einwilligung schien bisher das Allerheilmittel im Datenschutz zu sein, geht es doch letztlich um informationelle Selbstbestimmung. Die Anpassungen der DSGVO in diesem Bereich liessen allerdings Böses erahnen. Auch hier haben sich die Befürchtungen nicht bewahrheitet: Der Wortlaut der Definition der Einwilligung in Art. 4 Abs. 6 VE DSG wurde zwar um den Hinweis erweitert, dass eine Einwilligung eindeutig sein muss, um gültig zu sein. Damit wird jedoch lediglich wiederholt, was heute schon gilt.[24] Es gilt auch im Bereich der Einwilligung weiterhin ein risikobasierter Ansatz: Je einschneidender die Folgen einer Einwilligung, desto klarer muss sie sein. Je ungewöhnlicher die beabsichtigte Datenbearbeitung, desto deutlicher muss darauf hingewiesen werden. Die Erläuterungen sind insofern nicht korrekt, als dass eine Einwilligung nicht den gesamten Zweck einer Bearbeitung abdecken muss[25]; es genügt, dass sie jenen Teil einer Bearbeitung abdeckt, für den sie eingeholt wird.

[Rz 29] Nach Schweizer Recht wird es aber weiterhin möglich sein, dass etwa ein Kästchen auf einem Online-Formular, das eine bestimmte Datenbearbeitung für erlaubt erklärt, standardmässig bereits angekreuzt ist. Dies wird unter der DSGVO mit der Begründung abgelehnt, dass die Einwilligung in Bezug auf diese Bearbeitung nicht mehr eine unmissverständliche sei, was dort be-

20 Erläuterungen VE DSG, S. 46, welche das Versenden von unverlangten Werbe-E-Mails als Beispiel für eine nicht vereinbare Nutzung nennt.

21 Erläuterungen VE DSG, S. 46.

22 Art. 4 Abs. 2 VE DSG.

23 Erläuterungen VE DSG, S. 47.

24 Erläuterungen VE DSG, S. 47.

25 Ebd.

grifflich ebenfalls verlangt wird.[26] Die Begründung verkennt jedoch den Gesamtzusammenhang und stimmt jedenfalls für die Schweiz nicht: Ist das Kästchen in seinem Zustand (angekreuzt oder nicht) Gegenstand einer Erklärung, die ihrerseits einer eindeutigen Willensbekundung der betroffenen Person unterliegt, so gilt dies auch für den Inhalt des Kästchens, und zwar gleichgültig, ob es zunächst angekreuzt war oder nicht. Entscheidend ist der Zustand zum Zeitpunkt der Willenserklärung. Sonst wäre auch jeder Satz, der ganz ohne Wahlmöglichkeit angezeigt wird («Es gelten die AGB und die Preisliste.») nicht von der Willenserklärung erfasst, was wohl niemand behaupten wird und auch den Grundkonzepten des Schweizer Rechts zuwiderlaufen würde. Wenn überhaupt müsste die Frage der Voreinstellung des Kästchens im Rahmen der Regelung zum «*Privacy by Default*» in Art. 18 Abs. 2 VE DSG beantwortet werden (dazu Rz 79 hinten).

[Rz 30] Verwirrend sind die Ausführungen der Erläuterung in Bezug auf die Frage, wann eine Einwilligung eines «ausdrückliche» ist, wie sie für besonders schützenswerte Personendaten und das Profiling erforderlich ist.[27] Hierzu gibt es verschiedene Ansichten, wobei nicht klar ist, worin sich diese wirklich unterscheiden.[28] Zur vermeintlichen Klärung wurden im VE DSG die französischen und italienischen Begriffe «explicite» und «explicito» durch «exprès» und «espresso» ersetzt. Es wird ausgeführt, dass dies auch durch ein Zeichen geschehen kann, wie etwa das Anklicken einer Schaltfläche.[29] Die Frage, wann eine Einwilligung eine ausdrückliche ist, wird damit freilich nicht geklärt.

[Rz 31] Hierzu ist es nötig, das Wesen der Einwilligung in seine Einzelteile zu zerlegen. Leider herrscht auch in der Grundlagenliteratur zum Obligationenrecht bezüglich den verschiedenen Arten der Willenserklärung, wie sie auch jeder Einwilligung zugrunde liegt, ein Wildwuchs.[30] Die meisten Definitions- und Erklärungsversuche erweisen sich bei näherer Betrachtung als nicht zu Ende gedacht oder sogar in sich widersprüchlich. Dabei werden Begriffe wie «ausdrücklich», «konkludent» und «Stillschweigen» beliebig gemischt und gegenübergestellt.[31] So wird teilweise behauptet, die Frage der Ausdrücklichkeit beziehe sich nur auf die Form einer Willenserklärung, was schon begrifflich falsch ist, weil das Gegenstück zur ausdrücklichen Willenserklärung – die konkludente – sich sachlogisch überhaupt nur aus einer inhaltlichen Komponente ergeben kann. Wird nur von der Form einer Willenserklärung gesprochen, so ist zwischen aktivem und passivem Verhalten und den dazu benutzten Elementen wie Sprache, Gestik, Schrift oder sonstigen Bewegungen zu unterscheiden. Ein solches Verhalten muss jedoch immer in einen inhaltlichen Kontext gesetzt werden, um zur Willenserklärung zu werden; auch ein simples «Ja» oder der

---

26 Art. 4 Ziff. 11 DSGVO, Erwägung 32 DSGVO (wonach ein bereits angekreuztes Kästchen dem Stillschweigen gleichgestellt wird).

27 Es stellt sich die Frage, ob es überhaupt in allen vorgesehenen Fällen sinnvoll ist, eine ausdrückliche Einwilligung zu verlangen; gerade der Begriff des Profiling ist so breit angelegt, dass er auch viele nicht sensible Konstellationen erfasst. Dass trotzdem Ausdrücklichkeit verlangt wird, wird rein historische Gründe haben, da sie bisher auch für Persönlichkeitsprofile verlangt wurde.

28 Erläuterungen VE DSG, S. 47, m.w.H.

29 Erläuterungen VE DSG, S. 47 f.

30 Vgl. Alfred Koller, Schweizerisches Obligationenrecht Allgemeiner Teil, § 3, Rn. 127, der von einem «eigentlichen Wirrwarr» spricht.

31 Claire Huguenin, Obligationenrecht Allgemeiner und Besonderer Teil, Rn. 175, stellt der ausdrücklichen Willenserklärung die konkludente gegenüber, wobei die stillschweigende Erklärung als Unterfall der konkludenten und ausnahmsweise auch der ausdrücklichen Willenserklärung erachtet wird. Gl.M. Ernst Kramer/Bruno Schmidlin, in: Berner Kommentar, Arthur Meier-Hayoz (Hrsg.), Art. 1, Rn. 9; Andreas Furrer/Markus Müller-Chen, Obligationenrecht Allgemeiner Teil, Kapitel 2, Rn. 52. Andreas von Tuhr, Allgemeiner Teil des Schweizerischen Obligationenrechts, S. 163, bezeichnet die konkludente Willenserklärung hingegen als Unterfall der stillschweigenden; so auch Max Keller/Christian Schöbi, das Schweizerische Schuldrecht, Band I, S. 32.

Klick auf den «Ich stimme zu»-Knopf auf einer Website sagt für sich nichts aus.[32] Erst aus diesem Zusammenspiel von Form und Inhalt ergibt sich, ob eine Willenserklärung eine ausdrückliche oder – dem Gegenstück – eine konkludente ist.

[Rz 32] Ausdrücklich ist eine Einwilligung in eine Datenbearbeitung korrekterweise dann, wenn ein (i) aktives Verhalten oder ein solches vorliegt, das als affirmativ vereinbart wurde[33], und (ii) die Bedeutung dieses affirmativen Verhaltens sich direkt auf die betreffende Datenbearbeitung bezieht. Nicht ausdrücklich und somit konkludent ist eine Einwilligung in eine Datenbearbeitung dann, wenn das affirmative Verhalten sich lediglich auf eine Handlung bezieht, welche die fragliche Datenbearbeitung zur Folge hat und nicht auf die Datenbearbeitung selbst.

[Rz 33] Ein Beispiel illustriert dies: Wer ein Produkt auf die Ladentheke legt, gibt kund, dass er dieses Produkt kaufen möchte. Dies ergibt sich aus den Umständen. Nimmt die Person die gleiche Handlung zu Hause am Küchentisch vor, würde dies hingegen nicht bedeuten, dass sie das Produkt kaufen möchte; der Wille das Produkt kaufen zu wollen, wird nicht ausdrücklich kundgetan, sondern geht lediglich aus den Umständen hervor. Ausdrücklich ist hierbei höchstens die Tatsache, dass die Sache auf die Theke gelegt worden ist. Wer für den Kauf eines Produkts ein Formular mit seinen Personendaten ausfüllt und dieses einem Vertragspartner übergibt, nimmt ein affirmatives Verhalten vor. Eine lediglich konkludente Einwilligung in Bezug auf die mit dem Kauf zusammenhängende Datenbearbeitung liegt vor, wenn auf dem Formular nur auf den Kauf Bezug genommen wird, auch wenn aus den Umständen (d.h. implizit) hervorgeht, dass der Vertragspartner zur Abwicklung die übergebenen Personendaten bearbeiten wird. Dies ist dementsprechend auch nicht als ausdrückliche, sondern konkludente Einwilligung in eine Datenbearbeitung zu werten.[34] Steht auf dem Formular hingegen (auch), dass die Daten für Marketingzwecke bearbeitet werden, so resultiert aus der Übergabe des Formulars – also der exakt derselben Handlung bzw. Form – eine ausdrückliche Einwilligung bezüglich der Marketingzwecke.[35] Entscheidend ist somit vereinfacht formuliert, ob die Datenbearbeitung, in welche eingewilligt werden soll, beim Namen genannt wird. Dieses Begriffsverständnis wird auch dem Schutzzweck, den das Erfordernis der Ausdrücklichkeit hat, optimal gerecht.

[Rz 34] Eine in der Praxis wichtige Detailfrage ist die Möglichkeit der Einwilligung durch Stillschweigen oder rein passives Verhalten. Hierzu halten die Erläuterungen fest, dass ein passives Verhalten nie eine ausdrückliche Einwilligung sein kann. Das ist nicht richtig. Es ist auch hier zu differenzieren: Stillschweigen ist normalerweise keine Zustimmung, sondern nur unter den Voraussetzungen von Art. 6 des Obligationenrechts (OR). Wenn jedoch zwei Parteien miteinander vereinbart haben, dass Stillschweigen als Zustimmung gilt, dann stellt ein Stillschweigen in der definierten Situation ein affirmatives Verhalten, mithin ein vereinbartes Zeichen der Zustimmung

---

32 So auch Alfred Koller, Schweizerisches Obligationenrecht Allgemeiner Teil, §3, Rn. 116. Vgl. auch Ernst Kramer/Bruno Schmidlin, in: Berner Kommentar, Arthur Meier-Hayoz (Hrsg.), Art. 1, Rn. 7.

33 Es wurde z.B. vereinbart, dass Stillschweigen Zustimmung bedeuten soll.

34 Aus diesem Grund trägt die Anpassung der Begrifflichkeiten von «explicite» zu «exprès» im Vorentwurf nicht zur Klärung bei; die Verwendung des Begriffspaars «explizit» und «implizit» wäre weiterhin richtig, sofern der Bezug stimmt. Die EU übersetzt den Begriff der «ausdrücklichen Einwilligung» in der DSGVO im Übrigen mit «explicit consent» (vgl. z.B. Art. 9 abs. 2 Bst. a DSGVO).

35 Nicht entscheidend ist, ob auf dem Formular nur steht, dass die Daten für Marketingzwecke verwendet werden oder ob eine Einwilligungserklärung umfassender formuliert wird («Durch Abgeben des Formulars stimme ich zu, dass meine Daten für Marketingzwecke bearbeitet werden») oder das Formular gar unterschrieben wird. Letzteres wäre nur dann erforderlich, wenn die Einwilligung auch eine schriftliche sein müsste, was das DSG und der Vorentwurf jedoch nicht verlangt.

dar und wird auch in der Literatur zum Obligationenrecht als ausdrückliche Willenserklärung anerkannt.[36] Dies ist vor allem in einem Anwendungsfall der Praxis von zentraler Bedeutung: Der Anpassung von AGB. Diese wird normalerweise mit einer Klausel bewerkstelligt, wonach dem Kunden zugestellte Anpassungen von AGB als genehmigt gelten, wenn er ihnen nicht innert Frist widerspricht. Es handelt sich um eine klassische stillschweigende Zustimmung (*deemed consent*), die durchaus wirksam ist. Beschreiben die AGB, wie die Daten des Kunden bearbeitet werden, und widerspricht der Kunde nicht, so liegt diesbezüglich eine ausdrückliche Zustimmung im Sinne von Art. 4 Abs. 6 VE DSG vor. Das Schweigen als Zeichen der Zustimmung ist vereinbart und damit hinreichend, und die Zustimmung bezieht sich direkt auf den Inhalt der AGB und damit auch auf die darin explizit erwähnte Datenbearbeitung. Ob diese Datenbearbeitung so ungewöhnlich ist, dass darauf besonders hingewiesen werden muss, ist eine weitere Frage, die aber nichts mit jener der Ausdrücklichkeit zu tun hat. Die Frage der Ausdrücklichkeit hat auch nichts direkt mit der Frage der Information zu tun, die für eine informierte Einwilligung erforderlich ist, da diese Information sich auch auf die Konsequenzen der Einwilligung bezieht und daher ohne Weiteres breiter sein kann als der Bedeutungsgehalt des zustimmenden Verhaltens. Diese einzelnen Aspekte sind sauber zu trennen, und es bleibt zu hoffen, dass die Botschaft zum revidierten DSG diesbezüglich klarer ausfällt.

[Rz 35] Sinnvollerweise verzichtet wurde im VE DSG auf eine besondere Regelung zum Rückzug von Einwilligungen und zum *Bundling* von solchen, wie es in Art. 7 Abs. 4 DSGVO diskutiert wird; vor allem letztere Regelung ist auch im EU-Recht unklar und umstritten, da ein Bundling von Einwilligungen nach Art. 7 Abs. 4 DSGVO zwar verpönt, aber nicht *per se* unzulässig sein soll. Im Schweizer Recht können schon heute Einwilligungen in die Datenbearbeitung in der Regel zurückgezogen werden, wobei dies nur für die Zukunft gilt und entsprechende vertragliche Konsequenzen nach sich ziehen kann, wie etwa ein ausserordentliches Kündigungsrecht des betroffenen Unternehmens. Auch eine Regelung, wonach Datenschutzeinwilligungen in AGB oder sonst in Verträgen von anderen Einwilligungen getrennt erfolgen müssen, findet sich im VE DSG sinnvollerweise nicht. Es wäre auch nicht einzusehen, warum für den Datenschutz andere Standards gelten sollen als für andere Regelungsbereiche wie die Haftung, Gewährleistung oder Geheimhaltungspflichten.

5. Auslandtransfer: Komplizierter und langwieriger, aber nicht schwerer

[Rz 36] Die Regeln zur Bekanntgabe ins Ausland verändern sich grundsätzlich nicht. Es soll im revidierten DSG in materieller Hinsicht nicht schwieriger werden Daten ins Ausland zu übermitteln. Aber es wird aufgrund neuer Notifikations- und Genehmigungspflichten komplizierter, mitunter viel langwieriger und vor allem drohen neu empfindliche Sanktionen bei Verstössen.

[Rz 37] Die Eigenverantwortung im Rahmen der Bekanntgabe ins Ausland wird ein gutes Stück abgeschafft: War es bisher so, dass jeder Datenexporteur selbst beurteilen musste, ob seine Daten im Ausland noch angemessen geschützt sind, kann er sich neu auf den Entscheid des Bundesrates verlassen. Hat dieser festgestellt, dass das Recht im Zielstaat einen angemessenen Datenschutz

36 Ingeborg Schwenzer, Schweizerisches Obligationenrecht Allgemeiner Teil, Rn. 27.11; Ernst Kramer/Bruno Schmidlin, in: Berner Kommentar, Arthur Meier-Hayoz (Hrsg.), Art. 1, Rn. 8; Claire Huguenin, Obligationenrecht Allgemeiner und Besonderer Teil, Rn. 173; Wilhelm Schönenberger/Peter Jäggi, Zürcher Kommentar, Art. 1–17 OR, Art. 1, Rn. 145.

gewährleistet, so steht dem Art. 5 Abs. 1 VE DSG offenbar nichts mehr entgegen. Der Vorentwurf muss so zu verstehen sein, dass der Export selbst dann zulässig ist, wenn der Datenexporteur zum Schluss kommen sollte, dass er die Persönlichkeit der betroffenen Person schwerwiegend gefährdet, weil die Bekanntgabe die betroffene Person zum Beispiel einer Strafverfolgung im Ausland aussetzt.[37] Ist dies nicht die Absicht, dann wäre dieser Punkt zu klären. Ist diese Folge beabsichtigt, so kann und sollte Abs. 1 als überflüssig und verwirrend gestrichen und (etwa in Abs. 2) festgehalten werden, dass Personendaten *nur* dann exportiert werden dürfen, wenn einer der Fälle von Art. 5 und 6 VE DSG erfüllt ist (Angemessenheitsentscheid, Garantien, Ausnahmen). Wer einwendet, dass selbst bei Einhaltung der Fälle von Art. 5 und 6 VE DSG Situationen entstehen können, in welchen ein Export die Persönlichkeit einer betroffenen Person verletzt, so sei darauf hingewiesen, dass solche Konstellationen entweder über die Bearbeitungsgrundsätze in Art. 4 VE DSG oder aber über Art. 23 Abs. 1 VE DSG «gelöst» werden können, wenn auch ohne entsprechendes Sanktionsrisiko.

[Rz 38] Liegt kein Angemessenheitsbeschluss vor, kann weiterhin auf Basis von Standardklauseln, wie sie heute die Regel sind, exportiert werden. Eine Genehmigung ist nach wie vor nicht erforderlich; es gilt weiterhin nur eine Pflicht zur Information des EDÖB betr. den Einsatz solcher Verträge oder vergleichbaren Vorkehren (Art. 5 Abs. 6 VE DSG). In der Verordnung wird sich zeigen, ob hierzu neu weitere Angaben zu den konkreten Datentransfers nötig sind (wie sie der EDÖB heute ohne Rechtsgrundlage verlangt und einen unverhältnismässigen Aufwand mit sich bringen kann) oder weiterhin eine pauschale Information mit einem allgemeinen Hinweis auf die Verwendung der Standardklauseln ausreicht, was vollauf genügt. Welchen Sinn eine solche Informationspflicht hat und was sie zum Datenschutz beiträgt, ist allerdings schon unter dem heutigen Recht unklar; die Schweiz sollte die Informationspflicht streichen, wie schon die EU im Rahmen der DSGVO.

[Rz 39] Vom Standard abweichende Verträge («spezifische Garantien») können bei entsprechender Notifikation weiterhin benutzt werden (Art. 5 Abs. 3 Bst. b VE DSG). Binding Corporate Rules («BCRs») oder zu Deutsch «verbindliche unternehmensinterne Datenschutzvorschriften» benötigen hingegen neu eine Genehmigung durch den EDÖB (Art. 5 Abs. 3 Bst. d VE DSG). Dies ist inkonsequent, weil BCRs letztlich eine Untergruppe der «spezifischen Garantien» von Bst. b sind,[38] für welche lediglich eine Informationspflicht vorgesehen ist. Worin der Unterschied zwischen Garantien nach Bst. b und d besteht, bedarf daher einer Klärung, sollte an der Unterscheidung festgehalten werden; sie erscheint jedoch wenig sinnvoll. Offenbar gingen die Verfasser des Vorentwurfs davon aus, dass es Datenexportverträge für den «Einzelfall» gibt[39] und solche, die von Unternehmen (und Behörden) für mehrere verschiedene Datenübermittelungen eingesetzt werden, während nur letztere der Genehmigung bedürfen (Art. 5 Abs. 3 Bst. c Ziff. 1 und Bst. d VE DSG). Die meisten nicht standardisierten Verträge werden in letztere Kategorie fallen.

[Rz 40] Die Frist zur Genehmigung ist mit einem halben Jahr allerdings enorm lange angesetzt; bisher musste die Prüfung selbst von BCR innert 30 Tagen durchgeführt sein. Das wird dazu

37 Die Erläuterungen VE DSG betonen jedenfalls für den Fall eines Angemessenheitsbeschlusses die Zulässigkeit des freien Datenverkehrs (S. 48).

38 Auch BCR werden regelmässig über (multilaterale) Verträge der einzelnen Gruppengesellschaften vereinbart. Sie kommen in der Regel dann zum Tragen, wenn nicht mit den Standardklauseln operiert werden soll (da in vielen EU-Ländern individuelle Verträge nur in Form von BCR möglich sind).

39 Erläuterungen VE DSG, S. 49, welche auf die Verwendung des Begriffs «im Einzelfall» Bezug nehmen, der sich jedoch nicht (mehr?) im VE DSG befindet.

führen, dass gerade nicht standardisierte Datenexportverträge in der Praxis völlig uninteressant werden, da kaum jemand ein halbes Jahr warten will, bevor er seinen Datentransfer durchführen kann. Hinzu kommt, dass die tatsächliche Frist sehr viel länger sein kann, da der EDÖB sich jederzeit auf den Standpunkt stellen kann, er habe noch nicht alle erforderlichen Informationen und die Frist von sechs Monaten somit von neuem zu laufen beginnt. Für BCRs ist immerhin vorgesehen, dass die Anerkennung durch eine andere Datenschutzbehörde auch für die Schweiz genügt, was insofern nicht sinnvoll ist, da BCR nur dann für die Schweiz genügen, wenn auch die Datentransfers *aus der Schweiz* erfasst sind. Dies wird bei der Prüfung durch eine ausländische Behörde nicht sichergestellt und muss in der Praxis erfahrungsgemäss immer wieder nachträglich angepasst werden, weil es vergessen ging.

[Rz 41] Als weitere Neuerung ist auch der Auftragsbearbeiter der Informations- bzw. Genehmigungspflicht unterworfen, nicht nur der Verantwortliche. Bisher hatte nur der Inhaber der Datensammlung eine Pflicht zur Notifikation. Die neue Regelung ist insbesondere in Konstellationen, in welchen der Verantwortliche in einem Land ohne angemessenen Datenschutz befindet, problematisch, so zum Beispiel Schweizer Cloud-Provider mit Kunden von ausserhalb Europas: Anerkannte Musterklauseln gibt es für diese Fälle nicht[40], und eigene Klauseln erfordern ein langwieriges Genehmigungsverfahren. Der Provider könnte sich zwar auf den Standpunkt stellen, dass vertragliche Garantien gar nicht erforderlich sind, weil mutmasslich die Einwilligung der betroffenen Personen für den Re-Export der Daten aus der Schweizer Cloud in das Land des Verantwortlichen vorliegt. Ob sich ein Provider angesichts der Strafsanktionen jedoch auf das Restrisiko einlassen wollen wird, ist eher fraglich. Diese Regelung sollte daher überdacht werden.[41]

[Rz 42] Die weiteren Rechtfertigungsgründe zur Übermittlung von Personendaten in Länder ohne angemessenen Datenschutz finden sich neu in einem separaten Artikel (Art. 6 VE DSG). Als wichtige Anpassung ist hier der Fall zu nennen, dass Unterlagen zwecks Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen ins Ausland übermittelt werden. Solche Transfers waren in ein Land ohne angemessenen Datenschutz wie etwa die USA bisher nur möglich im Zusammenhang mit Gerichtsverfahren, nicht jedoch Untersuchungen durch andere Behörden. Letztere sind neu ebenfalls abgedeckt; gestützt auf dem Sinn und Zweck der Erweiterung sollte der verwendete Begriff der «Verwaltungsbehörde» nicht nur Aufsichtsbehörden erfassen, sondern alle Behörden, vor welchen Verfahren zur Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen stattfinden können, also etwa eine Kartellbehörde, eine Steuerbehörde oder auch eine Behörde, die strafrechtliche Tatbestände untersucht und allenfalls sogar vergleichsweise regelt, wie dies etwa die *Criminal Division des US Departement of Justice* regelmässig tut. Unter heutigem Recht fallen diese Fälle zwischen Stuhl und Bank, was in weit über hundert Datenschutzprozessen vor Schweizer Gerichten im Zusammenhang mit dem US-Steuerstreit zur Blockierung von Datenlieferungen in die USA führte.[42] Diese Fälle waren denn auch der Anlass für die Erweiterung. Um Verwirrungen über die Frage zu vermeiden, was genau mit «Verwaltungsbehörden» gemeint ist,

40 Die *Controller-Processor-Clauses* der EU funktionieren nur in die umgekehrte Richtung.

41 Immerhin ist zu erwähnen, dass es im Falle von «*Processor-BCRs*» durchaus Konstellationen gibt, in welchen der Auftragsbearbeiter in die Pflicht genommen werden muss. Im heutigen Recht wird so verfahren, dass solche Regelungen durch Auftragsbearbeiter dem EDÖB zur Vorprüfung vorgelegt werden, dieser dann aber im konkreten Einzelfall jeweils nochmals prüft, ob sie hinreichend sind.

42 Vgl. etwa David Rosenthal, Aktuelle Anwaltspraxis 2015, S. 594 ff.

empfiehlt es sich wie in der DSGVO[43] den Zusatz «vor einem Gericht oder einer Verwaltungsbehörde» zu streichen. Hierbei kann ferner die Wendung, dass die Bekanntgabe «unerlässlich» sein muss, an den Wortlaut der DSGVO angeglichen werden, die von «erforderlich» spricht. Zwar verwendet schon das bisherige Recht das Wort «unerlässlich». Es wird jedoch nicht wortwörtlich verstanden: Alles, was in einem entsprechenden Verfahren an Unterlagen Eingang finden soll oder von der Gegenpartei verlangt werden kann, ist damit erfasst.[44] Ebenso ist nicht nur die aktive Durchsetzung von Ansprüchen erfasst, sondern ebenso die Abwehr und Verteidigung gegen Rechtsansprüche. Damit der neue Wortlaut der Bestimmung überhaupt Sinn macht, ist der Begriff der «Rechtsansprüche» so zu verstehen, dass er auch straf- oder verwaltungsrechtliche Massnahmen umfasst. Dies wäre mindestens in der Botschaft klarzustellen.

[Rz 43] Gegenüber heutigem Recht nicht geändert, wurde die Ausnahmeregelung für Bekanntgaben im Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags mit der betroffenen Person. Damit ist die Schweiz allerdings strenger als die DSGVO. Letztere erlaubt die Bekanntgabe auch dann, wenn ein Vertrag lediglich im Interesse der betroffenen Person abgeschlossen worden ist.[45] Diese Ergänzung wäre auch für das Schweizer Recht sinnvoll. Sie sollte aus Gründen der Konsistenz auch im Rahmen von Art. 24 Abs. 2 Bst. a VE DSG vorgenommen werden.

[Rz 44] Eine besonders heikle neue Bestimmung findet sich schliesslich in Art. 6 Abs. 2 VE DSG: Sie verlangt, dass Datenexporte in etlichen Konstellationen dem EDÖB gemeldet werden müssen, so auch in allen Fällen, in welchen der Export durch Vertragsabschluss oder -erfüllung oder ein ausländisches Rechtsverfahren gerechtfertigt wird. Dies wird nicht nur zu zahlreichen Meldungen führen, die der EDÖB gar nicht vernünftig oder innert nützlicher Frist bearbeiten können wird. Sie zwingt Unternehmen faktisch auch, dem EDÖB sensible Geschäftsgeheimnisse wie etwa laufende ausländische Untersuchungen und Gerichtsverfahren offenzulegen, wofür es keinen guten Grund gibt. Hierbei ist zu beachten, dass alle dem EDÖB gelieferten Unterlagen gemäss Öffentlichkeitsgesetz öffentlich einsehbar sind, einschliesslich Meldungen nach Art. 6 VE DSG. Geschäftsgeheimnisse sind zwar nach dem Buchstaben des Gesetzes vom EDÖB zu schützen, doch hat er diesen Schutz bisher sehr eng ausgelegt. Geschwärzt wird in der Praxis nur sehr wenig. Zur Meldung ist zudem nicht nur der Verantwortliche verpflichtet, sondern auch der Auftragsbearbeiter, obwohl er regelmässig nicht über die erforderlichen Angaben verfügen wird und nicht Herr der Daten ist. Es ist zu hoffen, dass diese Meldepflicht ersatzlos gestrichen wird.

6. Deutlich erweiterte Informations- und Auskunftspflichten

[Rz 45] Die Informationspflicht in Art. 13 VE DSG wird in der Praxis eine der materiell wichtigsten Neuerungen des revidierten DSG für private Datenbearbeiter sein. Sie sieht eine Informationspflicht im Rahmen jeder Datenbeschaffung vor, die deutlich weitergeht als das, was bisher erforderlich war. Sie ist wie der bisherige Art. 14 DSG kein Bearbeitungsgrundsatz, sondern eine öffentlich-rechtliche Norm, deren Verletzung nicht zwingend eine Persönlichkeitsverletzung zur Folge hat, dafür strafrechtlich sanktioniert wird. Anders als bisher erfasst die neue Infor-

43 Vgl. Art. 49 Abs. 1 Bst. e DSGVO.

44 David Rosenthal, Handkommentar DSG, Art. 6, N 66.

45 Art. 49 Abs. 1 Bst. c DSGVO.

mationspflicht jede Datenbeschaffung, d.h. es muss immer informiert werden. Der Katalog der Ausnahmen ist wesentlich enger als bei der generellen Transparenzpflicht nach Art. 4 VE DSG.

[Rz 46] Die Bestimmung ist in verschiedener Hinsicht problematisch. Zunächst ist unklar, über welche Dinge informiert werden muss. Art. 13 Abs. 2–4 VE DSG zählen zwar einige konkrete Angaben auf, doch muss die Information alles umfassen, was für eine betroffene Person erforderlich ist, um ihre Rechte nach DSG geltend zu machen. Gemäss den Erläuterungen soll die Beschränkung auf Mindestangaben eine flexible Handhabung der Informationspflicht erlauben und so zu viele Informationen verhindern. Da die Informationspflicht aber strafrechtlich massiv sanktioniert ist und sogar die fahrlässige Verletzung strafbar sein soll, werden Verantwortliche und Auftragsbearbeiter zur Risikominimierung wesentlich mehr Informationen liefern, als sie müssen, da sie sich auf ihre eigene Beurteilung, was an Informationen wirklich sinnvoll ist, nicht verlassen werden wollen.

[Rz 47] Es ist daher davon auszugehen, dass viele Schweizer Unternehmen sich an die umfassenderen Vorgaben der DSGVO halten werden.[46] In einem Punkt geht der VE DSG allerdings über die DSGVO hinaus: Nach Art. 13 Abs. 4 VE DSG muss auch über die Identität und Kontaktdaten der Auftragsbearbeiter informiert werden. Dies geht nach der hier vertretenen Auffassung viel zu weit und bringt betroffenen Personen in der Regel keinen Mehrwert. Hier sollte die Regelung darauf beschränkt werden, dass diese Information wenn überhaupt nur im Rahmen des Auskunftsrechts auf spezifische Nachfrage geliefert werden muss.[47] Über die DSGVO hinaus geht auch Art. 13 Abs. 5 VE DSG, der eine Information der betroffenen Person bei indirekter Datenbeschaffung spätestens bei Speicherung vorsieht; die DSGVO gewährt hier eine Frist von bis zu einem Monat.[48]

[Rz 48] Unklar im Rahmen der Bestimmung bleibt ferner, ob dann, wenn nachträglich neue Bearbeitungszwecke hinzukommen, «nachinformiert» werden muss; das dürfte (weiterhin) wohl nicht der Fall sein. Das gilt auch für die anderen Punkte, über die informiert werden muss. Es wird daher nur darüber informiert werden müssen, was schon zum Zeitpunkt der Beschaffung feststand; liegt eine laufende Beschaffung vor, genügt es, die Information für die künftig erfolgenden Beschaffungen anzupassen. Sollen bestehende Daten zu einem neuen Zweck bearbeitet werden, wird hierfür eine Einwilligung oder ein anderer Rechtfertigungsgrund erforderlich werden, soweit es kein mit dem ursprünglichen Zweck vereinbarer Zweck darstellt (dazu Rz 24 oben). Der Schutz der betroffenen Person wird so z.B. auch bei der Erweiterung der Kategorien der Empfänger sichergestellt. Etwas anderes wäre in letzter Konsequenz auch absurd, wenn pauschal nachinformiert werden müsste, wenn sich die Umstände, über die informiert wurde, geändert haben: Man stelle sich vor, ein Unternehmen ändert seine Kontaktadresse und müsste deswegen alle Personen, von denen es je Daten beschafft hat, darüber in Kenntnis setzen. Natürlich könnte argumentiert werden, dass dies nötig sei, damit diese Personen weiterhin wissen, wo sie ihre Rechte geltend machen können, aber eine solche Regelung würde jedes vernünftige Mass missen.

[Rz 49] Ohnehin ist absehbar, dass die Informationspflicht zu einer unnötigen, ja sogar kontraproduktiven Überinformation der betroffenen Personen führen wird, die kaum einen wirksamen Beitrag zur Verbesserung des Datenschutzes leisten wird. Die DSGVO geht punkto Informations-

46 Vgl. Art. 13 und 14 DSGVO.

47 Art. 20 VE DSG sieht die Information ebenfalls vor.

48 Art. 14 Abs. 3 Bst. a DSGVO.

pflicht zwar bezüglich der Elemente, über die informiert werden muss, noch weiter, doch wird dort inzwischen ebenfalls deutliche Kritik laut. Eine risikobasierte Transparenzpflicht, wie sie in Art. 4 DSG und VE DSG enthalten ist, genügt völlig.

[Rz 50] Eine im Vorfeld vorgeschlagene Lösung, wonach es genügen soll, dass ein Unternehmen statt einer Detailinformation bei jeder Datenbeschaffung mit einer Information auf seiner Website arbeiten kann, fehlt leider im Vorentwurf. Sie ermöglicht einen einigermassen sinnvollen Umgang mit der Informationsflut für jene, die diese Informationen tatsächlich erhalten möchten. Diese wenigen betroffenen Personen könnten sich dann auf den Webseiten der betreffenden Unternehmen im Detail darüber ins Bild setzen, wofür diese ihre Daten verwenden. Die Information am Beschaffungspunkt könnte auf die Identität und Information für weitergehende Informationen beschränkt werden; da der Zugang zu dieser Information gesichert wäre, wären auch die Vorgaben der Konvention 108 erfüllt. Die Lösung entspricht auch der heutigen Praxis des EDÖB. Es soll jedoch gemäss den Erläuterungen zum Vorentwurf gerade nicht genügen, wenn die betroffene Person nach der Information suchen oder fragen muss.[49] Dies dürfte bedeuten, das inskünftig überall, wo im Alltag Personendaten beschafft werden mit entsprechend langen (und entsprechend kleingedruckten) Informationstexten gerechnet werden muss, damit die Vorgaben von Art. 13 VE DSG der guten Form halber erfüllt sind. Wird die Norm ernst genommen, wird beispielsweise neben Sicherheitskameras in einem Gebäude jeweils ein Schild mit einem entsprechenden Informationstext befestigt werden müssen. Bisher genügte es, dass die Kameras sichtbar waren; alles andere ergab sich aus dem Zusammenhang, und wer mehr wissen wollte, konnte nachfragen und Auskunft erhalten.

[Rz 51] Der Katalog der Ausnahmen in Art. 14 VE DSG entspricht in Teilen der bisherigen Ausnahmeregelung von Art. 9 DSG, ist jedoch nach der hier vertretenen Auffassung zu eng und enger, als sie es gemäss der revidierten Konvention 108 sein müsste. So ist die Berufung auf überwiegende private Interessen nur dann möglich, wenn die Personendaten nicht an Dritte weitergegeben werden (Art. 14 Abs. 4 Bst. a VE DSG). Es ist dies eine schon im bisherigen Recht vorgesehene Einschränkung, für die es keine Berechtigung gibt. Entscheidend kann letztlich nur sein, ob das Interesse des Datenbearbeiters dem Interesse an der Information der betroffenen Person überwiegt. Tut es das im konkreten Fall, ist damit bereits gesagt, dass eine Information nicht mehr sinnvoll und auch nicht legitim ist. So werden sich Konzerne, die ihre Daten konzernintern nicht nur für die Zwecke der Auftragsbearbeitung teilen, bei der heutigen Regel nie auf überwiegendes eigenes Interesse berufen können, während es Unternehmen, die aus nur einer einzigen juristischen Person bestehen, können. Auch die Weitergabe an Behörden – zum Beispiel eine Aufsichtsbehörde – führt dazu, dass ein Unternehmen sich nicht mehr auf die Ausnahmebestimmung berufen kann, selbst wenn es ansonsten gute Gründe dafür gäbe. Es ist zu hoffen, dass der betreffende Zusatz gestrichen wird.[50]

[Rz 52] Es sollte zudem erwogen werden, die typischen Ausnahmefälle im Gesetz analog dem heutigen Art. 13 Abs. 2 DSG (bzw. Art. 24 VE DSG) klarzustellen, wobei dies für das Auskunftsrecht nach Art. 20 VE DSG (dazu sogleich) wichtiger ist als für die Pflicht zur Information nach Art. 13 VE DSG. So besteht zum Beispiel heute und unter dem Vorentwurf kein pauschales Recht, die Herausgabe der Kommunikation zwischen Unternehmen und Anwalt zu verweigern. Wäh-

49 Erläuterungen VE DSG, S. 56.

50 Gemeint ist: «und er die Personendaten nicht Dritten bekannt gibt».

rend ein Unternehmen dies in einem zivilrechtlich, strafrechtlichen und verwaltungsrechtlichen Verfahren ohne Weiteres kann, ist dies beim Auskunftsrecht nicht der Fall. Hier muss, soweit überhaupt zulässig, mit überwiegenden eigenen Interessen im Einzelfall argumentiert werden. Das erscheint stossend. Als weitere überwiegende private Interessen fallen gemäss heute herrschender Lehre und Praxis insbesondere in Betracht Daten zur internen Meinungsbildung[51], Sicherheitsinteressen (z.B. keine Mitteilung der Aufbewahrungsdauer von Daten zur Bekämpfung von Missbräuchen), die Lieferung von Unterlagen, die der Auskunftspflichtige schon hat (z.B. nutzen Bankkunden das Auskunftsrecht heute, um kostenlos Kontoauszüge nachzubestellen, die sie verloren haben, da Datenschutzgründe immer vorgeschoben werden können), zum Schutz von eigenen Geheimhaltungsinteressen (heute führt das Auskunftsrecht mitunter zur absurden Situation, dass einem Mitarbeiter zwar verboten werden kann, Geschäftsunterlagen mit nach Hause zu nehmen oder privat zu nutzen, sie ihm aber kostenlos in Kopie zur privaten Nutzung übergeben werden müssen, wenn er darin erwähnt wird und er sie unter Vorwand des Datenschutzes nach Art. 8 DSG herausverlangt, selbst wenn er das Unternehmen längst verlassen hat).

[Rz 53] Dass die Informationspflicht nach Art. 14 Abs. 2 Bst. b VE DSG auch entfällt, wenn die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist, ist bezüglich der Berufung auf überwiegende eigene Interessen keine Lösung: Die Ausnahme gilt nur, wenn die Informationen nicht bei der betroffenen Person direkt beschafft werden, und sie soll gemäss den Erläuterungen eng ausgelegt werden.[52] Werden beispielsweise für ein Gerichtsverfahren Beweismittel zusammengetragen, so wird künftig bei wortgetreuer Auslegung der Norm versucht werden müssen, alle darin erwähnten Personen[53] zu kontaktieren, um sie darüber zu informieren, dass die Unterlagen möglicherweise im Prozess eingereicht werden, auch wenn das Verfahren sie aller Voraussicht nach nicht tangiert. Eine Berufung auf überwiegende private Interessen ist aufgrund der Weitergabe an Dritte nicht möglich. Findige Köpfe werden argumentieren, es liege ein Fall von Art. 14 Abs. 2 Bst. a VE DSG vor, nämlich dass die Speicherung oder die Bekanntgabe der Daten ausdrücklich im Gesetz vorgesehen ist, doch das gilt, wenn überhaupt, nur für Verfahren vor Schweizer Gerichten und zweitens nur für Dokumente, die als Beweismittel auch eingereicht werden. Auch Art. 14 Abs. 3 Bst. a VE DSG greift nicht, da diese Bestimmung nur dann den Verzicht auf die Information erlaubt, wenn ein Gesetz die Preisgabe der Information verbietet, wie z.B. der Bank mit Bezug auf vom Bankgeheimnis geschützte Daten. Schreibt das Gesetz die Bearbeitung von Daten lediglich vor, muss informiert werden; die Ausnahme von Art. 14 Abs. 2 Bst. a VE DSG greift nur, wenn die Daten über Dritte beschafft werden. Eine Bank müsste also genau genommen im Börsenhandel inskünftig jeden Händler, mit welchem sie zu tun hat, darüber informieren, dass die Telefonate aufgezeichnet und Daten über ihn aufbewahrt werden (mit allen Angaben gemäss Art. 13 VE DSG), weil die FINMA dies so verlangt, wobei sie dies nicht einmal in Form einer gesetzlichen Regelung, sondern im Rahmen ihrer «Rundschreiben» tut. Der Ausnahmekatalog von Art. 14 VE DSG sollte somit auch diesbezüglich erweitert werden, etwa indem in Abs. 1 auch jene Fälle erfasst werden, in denen sich die Datenbearbeitung aus Gesetz ergibt, in den betroffenen Verkehrskreisen als bekannt gilt oder sich aus den Umständen ergibt.

---

51 Vgl. Entscheid Bezirksgericht Zürich vom 2. Februar 2015, zitiert in: David Rosenthal, Aktuelle Anwaltspraxis 2015, S. 600.

52 Erläuterung VE DSG, S. 58.

53 Z.B. Mitarbeiter anderer Unternehmen, die E-Mails gesandt, Verträge unterzeichnet haben oder sonst erwähnt sind.

Dies kann allenfalls durch eine Pflicht abgefedert werden, die Detailinformationen online oder auf Nachfrage bereitzustellen.

[Rz 54] Die Ausnahmen von Art. 14 VE DSG werden auch für das Auskunftsrecht von Relevanz sein, welches neu in Art. 20 VE DSG geregelt ist und bezüglich seiner Ausnahmen ebenfalls auf Art. 14 VE DSG verweist. Hier war erwartet – oder erhofft – worden, dass der Vorentwurf Massnahmen vorsieht, um dem grassierenden Missbrauch des Auskunftsrechts für datenschutzfremde Zwecke Einhalt zu gebieten, was jedoch nicht geschah.[54]

[Rz 55] Stattdessen soll das Auskunftsrecht ausgebaut werden. Insbesondere sind weitere Informationen hinzugekommen, über die informiert werden muss, wie zum Beispiel die Aufbewahrungsdauer oder Kriterien zu ihrer Festlegung und die Identität und Kontaktdaten aller Auftragsbearbeiter. Weggefallen sind Angaben zu den Rechtsgrundlagen der Bearbeitung. Unter diesen Titel hatte das Zürcher Obergericht sogar die Herausgabe von Unterlagen angeordnet, welche keinerlei Personendaten der betroffenen Person enthielt – ein Fehlurteil.[55]

[Rz 56] In Art. 14 VE DSG fehlt auch ein Vorbehalt zugunsten von Datenbearbeitungen, welche gesetzlich vorgesehen sind.

[Rz 57] Gestrichen wurde immerhin die bisherige Regelung, wonach die Auskunft in der Regel schriftlich ist, in Form eines Ausdrucks oder einer Fotokopie zu erteilen ist. Sie muss aber kostenlos sein. Interessanterweise fehlt eine Norm, welche den Bundesrat ermächtigt, diese Punkte auf Verordnungsebene zu regeln, so namentlich Ausnahmen von der Kostenlosigkeit vorzusehen, wie dies die DSGVO tut.[56] Auch diese Aspekte des Auskunftsrechts hat in der Vergangenheit immer wieder zu Rechtsstreitigkeiten geführt, da das Auskunftsrecht von ehemaligen Mitarbeitern benutzt wurde, um für ihre Zwecke an Kopien ihrer eigenen Geschäftskorrespondenz und weiterer Geschäftsunterlagen, an denen sie beteiligt waren, zu gelangen. Da dem Bundesrat keine Kompetenz zur Definition von Ausnahmen von der Kostenlosigkeit eingeräumt werden soll, wird es nicht möglich sein, solche Fälle auf dem Verordnungsweg vorzusehen. Die Auskunft muss selbst bei querulatorischen, wiederholten und extrem aufwändigen Anfragen gratis sein, was stossend erscheint. Ein Auskunftsersuchen kann, wenn es eine etwas speziellere Materie betrifft, ohne Weiteres viele Tausend Franken kosten. Selbst beim Öffentlichkeitsgesetz (BGÖ) darf der Staat für seine Umtriebe Kostenersatz verlangen.

---

54 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.

55 OGer vom 5. Dezember 2014 (LB140073-O3-1), E. 7; dazu David Rosenthal, Aktuelle Anwaltspraxis 2015, S. 591 ff.

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

7. Profiling und Einzelfallentscheide

[Rz 58] Auf den neuen Begriff des Profiling wurde bereits eingegangen. Demnach soll ein Profiling ohne ausdrückliche Einwilligung der betroffenen Person neu *per se* eine Persönlichkeitsverletzung darstellen. Dies ist gegenüber dem heutigen Recht eine deutliche Verschärfung, da bisher nur die *Weitergabe* von Persönlichkeitsprofilen eine Rechtfertigung erforderte. Die DSGVO kennt keine solche Regelung. Da dort jedoch jede Datenbearbeitung eine Rechtfertigung erfordert und im Falle besonders schützenswerter Personendaten eine ausdrückliche und eine solche auch im Falle eines automatisierten Profiling erforderlich ist, welches rechtliche oder in ähnlich erheblicher Weise auf eine Person wirkt, fällt die Regelung der DSGVO im Ergebnis nur etwas milder aus als die Schweizer Regelung.

[Rz 59] Neu findet sich im Vorentwurf auch eine Regelung zu automatisierten Einzelfallentscheiden. Eine solche Regelung war schon im Rahmen der letzten Revision des DSG diskutiert, dann aber wieder verworfen worden. In der EU sind solche schon heute eingeschränkt. Nun verlangt sie die revidierte Konvention 108. Im Kern geht es darum, dass bei automatisierten Einzelentscheiden, welche rechtliche oder erhebliche Auswirkungen auf eine Person haben, dieser Person ein Recht auf Anhörung durch einen Menschen gewährt wird. Dieser Anspruch auf «menschliches Gehör» findet sich neu in Art. 15 VE DSG. Die Anhörung kann vor oder nach dem Einzelentscheid stattfinden, und in dessen Rahmen verlangt das Schweizer Recht auch, dass die Person sich zu den über sie bearbeiteten Personendaten äussern können muss. Dies wiederum setzt sachlogisch eine Information über solche Entscheide voraus, die ebenfalls in Art. 15 VE DSG statuiert wird; unklar bleibt, wie allgemein die Information sein kann, was aber einen erheblichen Unterschied ausmachen kann.[57] Weiter stellt sich die Frage, ob nicht nur über die Tatsache eines automatisierten Entscheids informiert werden muss, sondern auch über die dazu bearbeiteten Personendaten, da sich die Person dazu ebenfalls äussern können muss; hier sollte darauf hingewiesen werden, dass diese Angaben nur auf Rückfrage zu liefern sind. Alles andere wäre uferlos. Da eine Person aber unabhängig von Art. 15 VE DSG die Möglichkeit hat, sich zu den über sie bearbeiteten Personendaten zu äussern, namentlich auch im Rahmen von Art. 4 Abs. 5 VE DSG, kann dieses Recht aus Art. 15 Abs. 2 VE DSG ohne Verlust gestrichen werden; die DSGVO sieht ein Recht zur Äusserung zu den bearbeiteten Daten in der Regelung zu automatisierten Einzelentscheiden auch nicht vor.[58]

[Rz 60] Aus dem Zusammenhang ergibt sich auch, dass der Entscheid zum Zeitpunkt der Anhörung nicht definitiv sein darf, auch wenn er von der «Maschine» schon gefällt worden ist. Es genügt also im Prinzip, bei automatisierten Einzelentscheiden eine Telefonnummer oder sonstige Kontaktmöglichkeit anzugeben, wo sich eine betroffene Person hinwenden kann, wenn sie sich zum Entscheid äussern möchte. Die Äusserung muss von einer Person zur Kenntnis genommen werden, welche bewirken kann, dass das Unternehmen auf seinen Entscheid zurückkommt; einfach nur entgegennehmen und ablegen wird nicht genügen (ähnliche Regelungen gibt es heute schon in anderen Bereichen, so z.B. Art. 333a Abs. 2 OR).

---

57 Eine allgemeine Klausel, wonach das Unternehmen auch automatisierte Einzelentscheide durchführt, wird allerdings nicht genügen. Es wird mindestens verlangt werden können, dass genügend Angaben geliefert werden, um automatisierte Entscheide als solche erkennen zu können. Die Schwierigkeit besteht allerdings nicht in den ohnehin der betroffenen Person kommunizierten Entscheiden, sondern jenen, die sowieso nicht kommuniziert werden (vgl. das nachfolgend erwähnte Schulbeispiel eines Viren- und E-Mail-Scanners, der jede Mail automatisiert daraufhin prüft, ob sie zugestellt wird; eine Mitteilung an den Absender erfolgt bestenfalls bei Nichtzustellung).

58 Art. 22 DSGVO.

[Rz 61] Anwendungsfälle sind gemäss Erläuterungen Situationen, in welchen ein Computer alleine darüber entscheidet, ob und zu welchen Konditionen ein Vertrag abgeschlossen wird oder Verkehrsbussen, die aufgrund einer Bildaufnahme automatisch verschickt werden.[59] Aber der Anwendungsbereich ist sehr viel breiter und umfasst etwa auch automatisierte Sicherheitskontrollen in Computernetzwerken wie z.B. im Falle von Spam- und Virenscannern, die E-Mails blockieren oder von den anderen separieren, Systeme zur Betrugsbekämpfung, welche z.B. Kreditkarten bei verdächtigen Transaktionen automatisch sperren und letztlich jeden etwas professionelleren Online-Shop, der automatisch Verträge abschliesst. In all diesen Fällen wird neu nicht nur über die Einzelentscheide informiert, sondern auch eine Möglichkeit zum Dialog mit einem Menschen vorgesehen werden müssen. Ausnahmen sieht Art. 15 VE DSG keine vor, die DSGVO hingegen lässt solche zu.[60] Weitere Beispiele sind Glücksspielsysteme, in welchem der Computer (sprich: Der Zufallsgenerator) über den Gewinn des Spielers entscheidet, selbstfahrende Autos oder automatische Börsenhandelssysteme. Sie sind zwar nur dann erfasst, wenn sie Personendaten bearbeiten, doch dies ist in allen drei Fällen ohne Weiteres denkbar.[61] Unklar wiederum ist, inwiefern auch automatisierte Abwicklungssysteme, wie etwa im Internet-Banking, erfasst sind. Ziel der Regelung sind sie sicher nicht, aber aufgrund der weitgefassten Definition und der Tatsache, dass heutzutage schon aus Gründen der Effizienz sehr viele Routineentscheide dem Computer übertragen werden, besteht das Risiko, dass sehr viele Fälle erfasst sind. Besonders hart wird dies die Bundesorgane treffen, da sie hierfür neu eine formelle Gesetzesgrundlage haben müssen (Art. 27 Abs. 2 VE DSG): Ohne eine Gesetzesanpassung wird ein Bundesorgan unter dem neuen DSG somit Computer selbst im Massengeschäft nicht mehr ohne Weiteres zur Effizienzsteigerung einsetzen können[62], was sicherlich nicht im Sinne des Erfinders wäre. Der Vorentwurf sieht solche Anpassungen nicht vor; viele der Anpassungen in anderen Gesetzen beschränken sich auf die Streichung der Erwähnung der Persönlichkeitsprofile.

[Rz 62] Die Erläuterungen zum Vorentwurf sprechen zwar davon, dass die Auswirkungen einer automatisierten Einzelentscheidung einen gewissen Schweregrad erreichen müssen, um erfasst zu sein.[63] Eine beliebige rechtliche Wirkung soll jedoch genügen. Wird in einer Online-Auktion automatisch darüber entschieden, wer den Zuschlag erhält, liegt eine rechtliche Wirkung vor und der Plattformbetreiber wird allen Mitbietern in diesem Fall die Möglichkeit geben müssen, sich zu äussern, auch wenn dies in der Sache völlig unsinnig ist. Noch absurder ist das Beispiel mit den Glückspielen: Sie müssten künftig konsequenterweise datenschutzrechtlich verboten werden, da sie immer rechtliche Wirkungen haben (der Computer entscheidet über die Pflicht zur Auszahlung von Gewinn), ausser der Spieler bleibt anonym oder es wird ihm die Möglichkeit gegeben, mit dem Betreiber darüber zu sprechen, warum er nicht gewonnen hat und warum das falsch ist.

---

59 Erläuterungen VE DSG, S. 59.

60 Art. 22 Abs. 2 Bst. b DSGVO.

61 Man denke an Online-Glückspiele oder Glückspiele, für welche sich eine Person anmelden muss, an selbstfahrende Autos, die über ihre Kameras Bilder von anderen Verkehrsteilnehmern machen, oder Handelssysteme, die es mit einem menschlichen Börsenteilnehmer als Gegenseite zu tun haben.

62 Ein Beispiel sind z.B. die heute bei Krankenkassen im obligatorischen Bereich eingeführten Systeme zur automatisierten Abrechnung.

63 Automatisierte Einzelfallentscheide gibt es überall im Alltag. Auch eine automatische, Badge-basierte Liftsteuerung kann z.B. eine solche sein. So entscheidet im Bürogebäude des Autors dieses Beitrags ein Computer alleine darüber, ob einem Mitarbeiter eine Liftkabine mit einer eingebauten Videokamera oder eine Liftkabine ohne zugeteilt wird, d.h. ob mehr oder weniger gewichtig in die Privatsphäre des Mitarbeiters eingegriffen wird.

[Rz 63] Fristen hierfür für die Anhörung der betroffenen Person sieht Art. 15 VE DSG allerdings keine vor, auch keine spezifische Form. Immerhin muss die Anhörung kostenlos sein.[64] Zu erwähnen ist, dass die Konvention 108 eine derart strenge Regelung nicht verlangt; auch hier geht die Schweiz weiter als nötig.

[Rz 64] Anders als in der DSGVO schaltet der Vorentwurf das Profiling den automatisierten Einzelentscheiden nicht gleich. In der DSGVO ist jedes automatisierte Profiling ein automatisierter Einzelentscheid und als solcher bei hinreichender Auswirkung geregelt; sonst gelten für das Profiling keine besonderen Bestimmungen. In der Schweiz schlägt der Vorentwurf eine breitere Regelung vor, indem auch «menschliches» bzw. manuelles und nicht nur ein maschinelles Profiling erfasst werden soll und daher eine Regelung unabhängig von automatisierten Einzelentscheiden erforderlich wurde. Ob das wirklich sinnvoll ist, ist eine andere Frage.

[Rz 65] Der Vorentwurf geht allerdings auch im Falle der automatisierten Einzelentscheide noch viel weiter als die DSGVO, indem in den Auskunftspflichten ein Verantwortlicher verpflichtet wird, bei *jedem* Entscheid, den er trifft und welchem die Bearbeitung von Personendaten zugrunde liegt, einer betroffenen Person Rechenschaft darüber abzulegen, wie und warum er so entschieden hat und welche Konsequenzen dies für die betroffene Person zusätzlich zu den Daten hat, die er hierzu verwendet hat. Diese Regel in Art. 20 Abs. 3 VE DSG gilt zwar insbesondere für automatisierte Einzelentscheide, aber ausdrücklich nicht nur. Eine solch breite Auskunftspflicht ist völlig überzogen und greift massiv in die Freiheiten der Unternehmen und betroffenen Privatpersonen ein. Stellt eine Person einer Firma eine Werbung für ein Angebot zu und entscheidet sich die Firma, diese Werbung in den Abfall zu werfen, so soll sie der Person für diesen Entscheid auf Nachfrage gemäss Vorentwurf rechenschaftspflichtig bleiben. Doch selbst wenn die Regel auf automatisierte Einzelentscheide beschränkt würde, wäre sie unsinnig: Diesfalls bliebe die Firma für ihren Viren- und Spamfilter rechenschaftspflichtig, um ein Beispiel zu nennen. Sinn macht eine Auskunftspflicht höchstens im Zusammenhang mit automatisierten Einzelentscheiden, die auch Anspruch auf «menschliches Gehör» gewähren, also gewisse Auswirkungen haben. So sieht es auch die DSGVO vor.[65]

[Rz 66] Es sollte zudem klargestellt werden, dass selbst in diesen Fällen nur dann Auskunft zu erteilen ist, wenn spezifisch nach den Zusatzdaten zu einem bestimmten Entscheid gefragt wird. Was nicht zugelassen werden sollte, wäre ein Ersuchen im Sinne von «gebt mir eine Liste aller automatisierten Einzelentscheide, die Ihr in Eurem Unternehmen trefft». Dies würde massiv in die Privatsphäre der Unternehmen eingreifen und dient primär der Ausforschung oder Schikane. Da die betroffene Person im Falle eines automatisierten Einzelentscheids ohnehin konkret auf diesen hingewiesen werden muss, genügt es, die Auskünfte nach Art. 20 Abs. 3 VE DSG auch nur in den Fällen zu gestatten, wo die betroffene Person diesem automatisierten Einzelentscheid unterworfen ist. Da sie ein Anhörungsrecht hat, genügt es, wenn sie die Auskunft vor ihrer konkreten Stellungnahme zum Entscheid erhält; eine Anfrage «auf Vorrat» ist somit nicht nötig.

64 Erläuterungen VE DSG, S. 60.

65 Art. 15 Abs. 1 Bst. h DSGVO.

8. Recht auf Vergessen, Widerspruchsrecht, Weitermeldepflicht

[Rz 67] Trotz erheblicher öffentlicher Diskussionen im Vorfeld der Vorlage[66] soll sich gemäss Vorentwurf am «Recht auf Vergessen» nichts ändern. Das ist völlig richtig so, denn das Schweizer Recht kennt schon heute eine umfassende und ausgewogene Regelung, die einer betroffenen Person erlaubt, sich gegen eine Datenbearbeitung in welcher Weise auch immer auszusprechen. Sie war bisher in Art. 12 DSG enthalten und findet sich nun unverändert in Art. 23 Abs. 2 Bst. b VE DSG.

[Rz 68] Der zivilrechtliche Rechtsschutz ist neu in Art. 25 VE DSG geregelt und entspricht ebenfalls dem heutigen Konzept; wer gegen eine Datenbearbeitung vorgehen will, kann dies vom Zivilgericht verlangen. Das gilt auch für das Recht, eine Berichtigung von Personendaten zu verlangen (bisher Art. 5 DSG, neu Art. 4 Abs. 5 DSG und Art. 25 DSG). Den «Bestreitungsvermerk» gibt es weiterhin. Es wird jetzt aber auch festgehalten, dass die bestrittenen Daten nur noch eingeschränkt bearbeitet werden, was schon bisher möglich war, auch wenn dies nicht ausdrücklich im Gesetz vorgesehen war. Es wird in diesen Fällen eine Interessenabwägung stattfinden müssen; rechtlich handelt es sich um einen Anwendungsfall des Widerspruchs gegen eine Datenbearbeitung, der nur mit einer entsprechenden Rechtfertigung (nach Art. 13 DSG bzw. Art. 24 VE DSG) wie etwa einem überwiegenden privaten Interesse «übergangen» werden kann.

[Rz 69] Neu ist hingegen die Regelung, wonach im Falle einer Berichtigung, Löschung oder Vernichtung von Daten und in weiteren Fällen der Verantwortliche und Auftragsbearbeiter die Dritten, denen sie zuvor die betroffenen Daten zugänglich gemacht haben, diese Berichtungen etc. mitteilen müssen, soweit dies nicht oder nur mit «unverhältnismässigem» Aufwand möglich ist (Art. 19 Bst. b VE DSG). Eine Begrenzung auf Fälle, in denen die betroffene Person ein schützenswertes Interesse hat, fehlt hingegen leider. Es ist nicht einmal erforderlich, dass die Berichtigung, Löschung oder Vernichtung auf einen Vorstoss der betroffenen Person zurückzuführen ist. Das kann zu absurden Verhältnissen führen, denn es gibt viele Gründe, warum Daten berichtigt, gelöscht oder vernichtet werden, ohne dass sich eine Nachinformation bisheriger Empfänger der Daten aufdrängt. Letztere benutzen die Daten möglicherweise gar nicht mehr. Oder eine Löschung erfolgt nicht, weil die Daten datenschutzwidrig bearbeitet wurden oder die betroffene Person dies verlangt hat, sondern weil sie der Inhaber selbst schlicht nicht mehr braucht. Das darf nicht eine Pflicht nach Art. 19 Bst. b VE DSG auslösen, sonst müsste jedes Unternehmen, das seine Archive und dergleichen bereinigt laufend prüfen, wem es die Daten schon einmal mitgeteilt hat und diese darüber informieren. Weil das schon ist im Ansatz unsinnig ist, kann es nicht sein, dass die Nachinformation lediglich wegen dem damit allenfalls verbundenen unverhältnismässigen Aufwand wegfällt. Art. 19 Bst. b VE DSG könnte zum Beispiel so eingeschränkt werden, dass sie nur zum Tragen kommen, wenn eine Person die Nachinformation aus berechtigten Gründen verlangt.

[Rz 70] Die DSGVO kennt eine ähnliche Regelung wie Art. 19 Bst. b VE DSG, doch geht der Vorentwurf auch bezüglich der mitzuteilenden Daten darüber hinaus,[67] als dass auch Verletzungen des Datenschutzes den Empfängern der davon betroffenen Daten mitgeteilt und somit offengelegt werden müssen. Das gilt paradoxerweise selbst dann, wenn die betroffenen Personen selbst darüber nicht informiert werden müssen. Aus der Regel geht auch nicht hervor, ob nur die melde-

66 Vgl. auch Postulat Schwaab 12.3152 und Erläuterungen VE DSG, S. 37.

67 Art. 19 DSGVO.

pflichtigen Datenschutzverletzungen gemeint sind, oder alle, wie es der Wortlaut suggeriert. So oder so ist nicht klar, welchen Sinn diese Pflicht haben soll. Sie ist überdies unverhältnismässig und greift ohne zwingenden Grund in die Privatsphäre der betroffenen Unternehmen ein.

[Rz 71] Man stelle sich zum Beispiel vor, dass in einem Unternehmen ein Mitarbeiter unbefugten Zugriff auf Daten nimmt, die das Unternehmen auch mit seinen Kunden teilt. Der Zugriff wird diesen als Datenschutzverletzung nach Art. 19 Bst. b VE DSG mitgeteilt werden müssen, obwohl er für diese Kunden ohne jede Relevanz ist, den Ruf der Firma aber schädigen wird. Ein anderes Beispiel wäre eine Zeitung, die im Zusammenhang mit der Berichterstattung über eine Person eine sie betreffende Datenschutzverletzung begeht. Nach der Regel von Art. 19 Bst. b VE DSG müsste die Zeitung diese Tatsache, sobald sie sie feststellt, allen Lesern des betroffenen Beitrags mitteilen, was technisch gesehen natürlich ohne Weiteres möglich ist. Tut sie dies nicht, können die betroffenen Mitarbeiter der Zeitung strafrechtlich verfolgt werden. Die Pflicht zur Mitteilung gilt zudem ungeachtet dessen, ob dies die betroffene Person oder andere Dritte in ihren Rechten verletzt.

9. Auch Daten verstorbener Personen geregelt

[Rz 72] Der Vorentwurf enthält mit Art. 12 VE DSG auch Bestimmungen zu Daten verstorbener Personen. Eine Regelung dieser Daten gibt es schon heute, allerdings ist sie erstens in Abs. 1 Abs. 7 VDSG versteckt und zweitens existiert für sie keine Rechtsgrundlage. Ohnehin gilt in der Schweiz der Grundsatz, dass die Persönlichkeit mit dem Tod endet[68], weshalb eine verstorbene Person auch keinen Datenschutz geniesst. Den Datenschutz geniessen allenfalls Personen im Umfeld der verstorbenen Person, die durch die Bearbeitung deren Daten ebenfalls betroffen sind. Die neue Regelung von Art. 12 VE DSG ist daher aus Sicht des Datenschutzes überflüssig. Dass es sie trotzdem gibt und ihr Regelungsgehalt über das bisherige Auskunftsrecht hinaus ausgebaut wird, ist die Folge einer politischen Intervention, welche Regelungen zum «digitalen Tod» in sozialen Medien verlangte.[69]

[Rz 73] Aus der Sicht der Praxis sind solche Zeitgeist-Regelungen unnötig und schädlich, da sie nur aufgrund eines sehr eng begrenzten, zum betreffenden Zeitpunkt gerade öffentlich diskutierten, aber meist nicht wirklich nachhaltig relevanten Anwendungsfalls hinaus verfasst werden. Problematisch sind solche Regelungen, weil sie aufgrund ihrer generell abstrakten Natur unzählige andere, nicht bedachte weitere Anwendungsfälle mitbetreffen und damit unkontrollierte und unüberlegte Nebenwirkungen haben. Das wird auch in diesem Fall so sein, da die Regelung keineswegs nur auf soziale Medien Anwendungen findet, sondern auf alle Unternehmen die Daten von natürlichen Personen bearbeiten.

[Rz 74] Verlangt ein einzelner Erbe, gleich in welcher Beziehung er zur verstorbenen Person steht, dass deren Daten gelöscht werden, soll sich das betroffene Unternehmen zum Beispiel nur auf überwiegende Interessen von Dritten oder der verstorbenen Person selbst berufen können, nicht aber etwa auf eigene überwiegende Interessen oder gesetzliche Pflichten, wie z.B. Aufbewahrungspflichten (Art. 12 Abs. 4 VE DSG). Damit hat der Erbe wesentlich mehr Rechte gegen einen Datenbearbeiter in der Hand als der Erblasser zu Lebzeiten, was keinen Sinn macht. Zudem bleibt

68 Art. 31 Abs. 1 ZGB.

69 Postulat Schwaab 14.3782 und Erläuterungen VE DSG, S. 38.

völlig im Dunkeln, ob und welche Interessen eine tote Person sachlogisch überhaupt haben kann. Konflikte unter den Erben regelt die Bestimmung ebenfalls in keiner Weise – sie sind naturgemäss vorprogrammiert. Interessant wird auch die Frage sein, wie der auskunftspflichtige Verantwortliche prüfen soll, ob eine Person eine faktische Lebensgemeinschaft mit der verstorbenen Person geführt hat.

[Rz 75] Durch die Universalsukzession der Vertragsverhältnisse mit den betreffenden sozialen Medien auf die Erbengemeinschaft und die weiteren Bestimmungen des anwendbaren Vertrags- und Erbrechts sowie der eigenen Persönlichkeitsrechte der Nachfahren wären die wesentlichen Rechtsfragen, die Sache des Gesetzgebers sind, hinreichend geklärt, oder dort zu klären und nicht im DSG. Erforderlich ist daher falls überhaupt nur eine moderate Bestimmung zum Auskunftsrecht; systematisch wäre es sinnvoller, sie mit der Revision des DSG ins ZGB aufzunehmen, wo sie hingehört, so zum Beispiel als neuen Art. 38^{bis} ZGB mit den Nachwirkungen der Ende der Persönlichkeit.

10. Massnahmen zur Sicherstellung des Datenschutzes

[Rz 76] Etliche der Bestimmungen des Vorentwurfs konkretisieren technische und organisatorische Massnahmen, die heute unter Art. 7 Abs. 1 DSG subsumiert werden könnten. Sie dienen der Gewährleistung des Datenschutzes, indem sie direkt oder indirekt auf die Einhaltung der Regelungen hinwirken.

[Rz 77] Die meisten dieser Bestimmungen wurden ins Gesetz genommen, um ein Zeichen zu setzen. Sie sind rechtlich an sich überflüssig, ergeben sie sich doch bereits aus einer korrekten Anwendung des Bearbeitungsgrundsatzes, wonach im Rahmen einer Datenbearbeitung jeweils angemessene (sprich: dem Risiko entsprechende) technische und organisatorische Massnahmen zu treffen sind, um eine unbefugte (sprich: DSG-widrige) Datenbearbeitung zu verhindern.

[Rz 78] Dieser Grundsatz findet sich in Art. 11 VE DSG. Neu wird hierbei der (ungewollte) «Verlust» von Daten als Unterform der unbefugten Bearbeitung im Einklang mit der Praxis der EU gesondert aufgezählt; erfasst war er schon bisher. Es wird allerdings nicht nur dem Bundesrat überlassen, diesen Grundsatz zu konkretisieren. Art. 18 Abs. 1 VE DSG tut dies unter dem Titel «Datenschutz durch Technik» (neudeutsch: «*Privacy by Design*»), wobei im Grunde dasselbe gesagt wird wie in Art. 11 Abs. 1 VE DSG, mit dem einzigen Hinweis, dass die Massnahmen bereits ab dem Zeitpunkt der Planung der Datenbearbeitung zu treffen sind, was aber so oder so gilt, wenn solche Massnahmen im Rahmen einer Datenbearbeitung von Anfang an bestehen müssen.

[Rz 79] Art. 18 Abs. 2 VE DSG schreibt den Grundsatz «datenschutzfreundlicher Voreinstellungen» («*Privacy by Default*») vor, welcher vor allem Anbieter von Online-Diensten und -Apps zwingen soll, die Grundeinstellungen ihrer Dienste so zu programmieren, dass von den im Rahmen eines Dienstes angebotene Datenbearbeitungen standardmässig die am wenigsten weitgehende vorgesehen ist. Die Formulierung im Vorentwurf bringt dies nicht wirklich zum Ausdruck und ist sachlogisch unkorrekt, da es nicht um die Frage geht, ob mehr Daten als für einen bestimmten Verwendungszweck erforderlich bearbeitet werden sollen, sondern zu welchem Verwendungszweck die Daten standardmässig vorgesehen werden soll. Hier ist somit eine Überarbeitung der Formulierung nötig. Ohnehin wäre es aufgrund der Nähe zu Art. 11 VE DSG sinnvoll, die beiden Grundsätze in den Wortlaut von Art. 11 Abs. 1 VE DSG zu integrieren, was mit wenigen Worten möglich wäre.

[Rz 80] Dies gilt im Übrigen auch für die in Art. 19 Bst. a VE DSG aufgeführte Pflicht zur Dokumentation der Datenbearbeitungen, die einerseits eine organisatorische Massnahme im Sinne von Art. 11 VE DSG darstellt und andererseits der Datenschutzaufsicht dient. Unternehmen werden hier gespannt auf die Konkretisierung im Rahmen der Verordnung sein, da je nach Ausgestaltung der Dokumentationspflicht ein erheblicher Aufwand auf sie zukommt. Sinnvoll wäre eine Regelung, die jedenfalls nicht über das von Art. 30 DSGVO vorgeschriebene Verzeichnis der Datenbearbeitungen hinausgeht, und eine Klarstellung, dass nur *regelmässige* Datenbearbeitungen in ein solches Inventar aufgenommen werden müssen, analog der heutigen Regelung von Art. 11a Abs. 3 DSG. Hinzu kommt, dass die meisten Unternehmen auch für die DSGVO nur *strukturierte* Datenbestände bzw. Datenbearbeitungen erfassen werden; eine solche Einschränkung erscheint aus Sicht der Praktikabilität und Möglichkeiten der Governance ebenfalls sinnvoll. Wird die Dokumentationspflicht zu breit oder absolut verstanden, muss jedes Schreiben einer E-Mail oder eines Briefs dokumentiert sein, weil sie jeweils eine Datenbearbeitung darstellen. Das wäre unsinnig. Es stellt sich vor diesem Hintergrund zudem die Frage, ob der gestrichene Begriff der Datensammlung nicht doch weiterhin benutzt werden sollte, um bezüglich gewisser Pflichten unter dem neuen DSG eine sinnvolle Beschränkung zu ermöglichen. Schliesslich wäre zu klären, dass mit Bezug auf die Dokumentation das Rad nicht neu erfunden werden muss und die Bestimmung keine eigenständige Dokumentation für Datenschutzzwecke erfordert, sondern es genügt, dass zum Beispiel auf bestehende Dokumentationen zurückgegriffen werden kann (z.B. ein Betriebshandbuch eines Systems) oder sich die Dokumentation sogar aus dem System selbst ergibt.

[Rz 81] Die in Art. 19 Bst. a VE DSG erwähnte Pflicht soll gemäss den Erläuterungen die Datenbearbeiter auch verpflichten, die Datenschutzverstösse im Sinne von Art. 17 VE DSG zu dokumentieren[70]. Hier kann auf die nachfolgenden Ausführungen zu diesem Thema verwiesen werden (vgl. Rz 93 ff. unten). Angesichts dem breiten Begriffsverständnis von Art. 17 VE DSG erscheint auch diese Dokumentation uferlos und ohne sichtbaren Mehrwert für den Datenschutz; hierbei ist zu beachten, dass diese Pflicht für jedes Unternehmen gilt, sei es noch so klein. Die DSGVO sieht eine solche Dokumentationspflicht zwar auch vor, geht aber von einem sehr viel engeren Verständnis der zu erfassenden Verstösse aus.

[Rz 82] Erstaunlicherweise keinen Eingang in die Vorlage gefunden haben Bestimmungen zum betrieblichen Datenschutzbeauftragten. Richtigerweise wird ein solcher nicht vorgeschrieben. Das war schon bisher nicht der Fall, und auch die DSGVO schreibt ihn für die meisten Betriebe nicht vor. Die Funktion des betrieblichen Datenschutzbeauftragten wäre aber ideal, um den EDÖB in gewissen Bereichen zu entlasten, wenn sichergestellt ist, dass eine solche Stelle über die nötigen Kompetenzen und das nötige Know-how verfügt. Es könnte zum Beispiel analog der bisherigen Regelung in Art. 11a DSG vorgesehen sein, dass die diversen Informations- und Meldepflichten wegfallen, soweit sie überhaupt beibehalten werden sollen, wenn ein Unternehmen selbst über eine solche Stelle verfügt; dies wäre ein erheblicher Anreiz zur Schaffung einer solchen Stelle, was wiederum der Datenschutz-Governance zugutekäme.

70 Erläuterungen VE DSG, S. 65.

11. Datenschutz-Folgenabschätzungen

[Rz 83] Ein neues Instrument zur Sicherstellung des Datenschutzes sind die «Datenschutz-Folgenabschätzungen» (*Privacy Impact Assessments*), welche Art. 16 VE DSG neu in allen Fällen vorschreibt, in welchen eine vorgesehene Datenbearbeitung «voraussichtlich zu einem erhöhten Risiko» für die Persönlichkeit der betroffenen Personen vorsieht. Eine solche Abklärung muss nicht zwingend umfangreich sein, wie die Erfahrung zeigt. Es geht im Wesentlichen darum, zunächst zu dokumentieren, wie die Datenbearbeitung vor sich gehen soll, was dabei schiefgehen bzw. negative Auswirkungen auf die betroffene Person haben kann, und welche Massnahmen zu ihrem Schutz vorgesehen sind, um diese Risiken und Auswirkungen auszugleichen (Abs. 2). Das mag auf einer Seite Platz finden. Das Ergebnis ist dem EDÖB mitzuteilen (Abs. 3), der dann etwaige Einwände innert einer Frist von drei Monaten nach Erhalt aller erforderlichen Informationen anmelden muss (Abs. 4).

[Rz 84] Auch die DSGVO schreibt solche Datenschutz-Folgenabschätzungen vor, und selbst im heutigen Schweizer Recht gibt es sie in den Kantonen teilweise schon[71]. Allerdings ist die im Vorentwurf vorgeschlagene Regelung in verschiedener Hinsicht problematisch. Erstens erscheint die Hürde für die Durchführung einer Abklärung sehr tief angesetzt. «Erhöhte» Risiken werden in der Praxis rasch gegeben sein, womit für fast alle Datenbearbeitungen vorab entsprechende Abklärungen durchgeführt werden müssen, mit den damit verbundenen Aufwänden und massiven Verzögerungen (dazu sogleich). Diesbezüglich beruhigen auch die Erläuterungen nicht, soll es doch schon genügen, dass die Verfügungsfreiheit der betroffenen Person über ihre Daten erheblich eingeschränkt wird oder werden kann[72], was in sehr vielen Fällen der Fall sein wird. Die Bearbeitung von besonders schützenswerten Personendaten oder ein Profiling soll bereits Indiz für ein «erhöhtes» Risiko sein, ebenso die Übermittlung in Drittstaaten ohne angemessenen Datenschutz. Die Strafbewehrung der Bestimmung wird ein ihres dazu beitragen, dass selbst in Fällen, in denen an sich kein erhöhtes Risiko besteht, aus Angst vor Strafbarkeit ein entsprechendes Verfahren durchgeführt wird, inklusive Meldung an den EDÖB. So wäre es bei der jetzigen Ausgangslage nicht erstaunlich, wenn inskünftig jede Übermittlung in die USA, jedes Profiling und jede Bearbeitung von besonders schützenswerten Personendaten zu einer Datenschutz-Folgenabschätzung führt, was völlig übertrieben wäre. Der dafür erforderliche Aufwand für die Wirtschaft (und den EDÖB) wäre enorm, ohne dass für den Datenschutz wirklich etwas gewonnen wäre.

[Rz 85] Die EU verlangt im Gegensatz dazu entsprechende Abklärungen nur bei «hohen» Risiken. Hierbei ist zu berücksichtigen, dass ohnehin jedes Bearbeitungsprojekt geprüft werden muss, denn nur dadurch kann überhaupt ermittelt werden, ob es voraussichtlich zu erhöhten oder hohen Risiken führt. Wesentlich ist, dass die gesetzliche Pflicht zur Erstellung einer formalen, dokumentierten Abklärung auf das beschränkt wird, was wirklich zwingend nötig ist. Die Fälle, in welchen Unternehmen solche formalisierten Abklärungen tatsächlich vornehmen sollen, sollten zudem im Rahmen der Verordnung konkretisiert werden. Eine Ausnahme bietet sich zudem für Fälle an, in welchen das Gesetz ein Unternehmen die Datenbearbeitung vorgibt, auch wenn die konkrete Ausgestaltung natürlich Risiken mit sich bringen kann, die adressiert werden müssen. Solche Fälle sind jedoch nicht im Fokus von Art. 16 VE DSG; die damit verbundenen

71 Vgl. etwa die Vorabkontrolle gemäss § 10 des ZH-IDG, die erforderlich ist, wenn eine Datenbearbeitung «besondere Risiken» mit sich bringt.

72 Erläuterungen VE DSG, S. 61.

fallspezifischen Risiken müssen im Rahmen der jeweiligen Gesetzesvorgaben abgewogen werden und, soweit ein Unternehmen nur die gesetzlichen Vorgaben umsetzt, wird die Datenbearbeitung in der Regel in materieller Hinsicht datenschutzkonform nach Art. 24 Abs. 1 VE DSG gerechtfertigt sein.

[Rz 86] Unpassend erscheint weiter, dass der Vorentwurf die Pflicht zur Abklärung nicht nur dem Verantwortlichen auferlegt, wie dies die DSGVO tut, sondern auch dem Auftragsbearbeiter, obwohl dieser dazu regelmässig nicht in der Lage sein wird und es auch nicht seine Aufgabe ist. Natürlich kann der Verantwortliche eine solche Abklärung an seinen Auftragsbearbeiter delegieren, aber es bleibt schon von der Natur der Sache her eine Pflicht des Verantwortlichen.

[Rz 87] Die Meldepflicht gegenüber dem EDÖB und die ihm eingeräumte Frist zur Bearbeitung ist schliesslich praxisfern und wird die Datenbearbeiter massiv behindern. Ein grosses Pharmaunternehmen aus Basel führt beispielsweise jedes Jahr weit über hundert solche Datenschutz-Folgeabschätzungen durch. Würden sie vom EDÖB ernsthaft geprüft, müsste er alleine für dieses Unternehmen eine eigene Person abstellen. Das wird er nicht und das kann auch nicht sinnvoll sein. Selbst die DSGVO ist weniger streng: Sie verlangt eine Konsultation der Aufsichtsbehörde nur dann, wenn der Verantwortliche zum Schluss kommt, dass trotz der von ihm ergriffenen Schutzmassnahmen ein hohes Risiko der Verletzung der Persönlichkeit der betroffenen Personen verbleibt.[73]

[Rz 88] Die dem EDÖB gewährte Frist zur Beurteilung ist überdies viel zu lange: In der EU muss eine Behörde innert acht Wochen handeln, falls sie sich gegen eine Bearbeitung ausspricht, und die Frist kann nur in komplexen Fällen um sechs Wochen verlängert werden.[74] In der Schweiz soll der EDÖB standardmässig drei Monate Zeit haben, mit der Möglichkeit, durch das Einfordern weiterer Information die Frist jedes Mal von neuem beginnen zu lassen.

[Rz 89] Wird der vorgeschlagene Art. 16 VE DSG tatsächlich so umgesetzt, bedeutet dies für Unternehmen, dass sie bei jedem Projekt, das eine Datenbearbeitung beinhaltet und diese nicht problemlos erscheint, einen Vorlauf von vielen Monaten einplanen müssen, um nach ihrer eigenen Abklärung auch etwaigen Anforderungen des EDÖB gerecht zu werden. Dies wird die Wirtschaft völlig unnötig lähmen und erhebliche Kosten verschlingen. Mag eine Wartezeit in gewissen Projekten noch handhabbar sein, wird sie in anderen Fällen zu erheblichen Schwierigkeiten führen. Man stelle sich zum Beispiel ein ausländisches Gerichtsverfahren oder eine Anfrage einer ausländischen Aufsichtsbehörde vor, für welches bzw. für welche innert Wochen gewisse Unterlagen geliefert werden müssen, die auch Angaben von Mitarbeitern enthalten. Nach der vorgeschlagenen Regelung wäre dies nicht mehr oder nicht sinnvoll möglich. Solche Fälle werden fast immer erhöhte Risiken mit sich bringen, müssten also dem EDÖB vorgelegt werden. Ebenso wird es aber nicht möglich sein, die Monate, die er zur Klärung der möglichen Massnahmen braucht, abzuwarten. Das Unternehmen wird sich entscheiden müssen, dem ausländischen Recht zu folgen und möglicherweise Schweizer Recht zu verletzen bzw. die Konsultation des EDÖB nutzlos werden zu lassen, oder umgekehrt. Dabei sieht die Regelung keine Ausnahmen vor, und dies nicht einmal für den Fall, in welchem alle betroffenen Personen mit der Datenbearbeitung einverstanden sind.

[Rz 90] Auch für den EDÖB wird diese Regelung im Ergebnis nicht angenehm werden. Wird ihm ein Projekt vorgelegt, wird er sich damit zwangsläufig auseinandersetzen müssen, denn tut er es

73 Art. 36 Abs. 1 DSGVO.

74 Art. 36 Abs. 2 DSGVO.

nicht und stellt sich das Projekt später als datenschutzrechtlich problematisch heraus, wird er dafür möglicherweise nicht rechtlich, aber öffentlich und politisch zur Verantwortung gezogen werden, weil er nicht rechtzeitig interveniert hat bzw. keine Einwände äusserte. Dies wird daher auch seinerseits erhebliche Ressourcen binden, über die er aber nicht verfügt bzw. die an anderer Stelle eingespart werden müssen. Sinnvoller wäre, dieses Konsultationsverfahren auf die wirklich heiklen Fälle zu beschränken.

[Rz 91] Zu klären ist weiter die Frage, unter welchen Umständen Datenschutz-Folgenabschätzungen im Rahmen von bestehenden Datenbearbeitungen vorzunehmen bzw. zu wiederholen oder aufzufrischen sind, falls überhaupt. Denn Risiken können sich verändern, die Umstände und Datenbearbeitungen ebenfalls. Der Wortlaut von Art. 16 VE DSG ist diesbezüglich nicht klar, impliziert aber aufgrund von Abs. 1 und 4, dass eine *formalisierte* Abklärung nur jeweils bei der Erstaufnahme einer Datenbearbeitung durchzuführen ist. Dies wäre in der Botschaft in diesem Sinne klarzustellen.

[Rz 92] Im Zusammenhang mit Art. 16 VE DSG sei noch erwähnt, dass diese auf ein Risiko «für die Persönlichkeit oder die Grundrechte» der betroffenen Personen abstellt. Diese Formulierung ist verwirrend. Zwar dient das DSG schon bisher gemäss Art. 1 nicht nur dem Schutz der Persönlichkeit, sondern auch den Grundrechten der betroffenen Personen, doch gilt letzteres nur mit Bezug auf die Datenbearbeitungen durch Behörden im engeren Sinn. Private sind normalerweise nicht zur Wahrung der Grundrechte verpflichtet; in ihrem Bereich dient das DSG – und damit die Datenschutz-Folgenabschätzung – ausschliesslich dem Schutz der Persönlichkeit der betroffenen Personen. Der Verweis auf die «Grundrechte» sollte daher sinnvollerweise überall gestrichen werden. Er hat keinen Mehrwert.

12. Data Breach Notifications

[Rz 93] Was ursprünglich in den USA erfunden wurde, soll es nun auch in der Schweiz geben: *Data Breach Notifications*. Es geht um die Meldung von Datenschutzverstössen, einschliesslich Datenverlust. Eine solche Pflicht bestand bisher nicht, jedenfalls nicht in formalisierter Form. Schon nach heutigem Recht kann es erforderlich sein, im Falle einer Datenschutzverletzung gewisse Sofortmassnahmen wie etwa die Sperrung von abhanden gekommenen Kreditkartendaten auszuführen. Auch die Mitteilung an den EDÖB kann in bestimmten Fällen ratsam sein. Neu soll jedoch *jeder* Datenschutzverstoss dem EDÖB «unverzüglich» gemeldet werden, es sei denn, dieser führe «voraussichtlich nicht zu einem Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person» (Art. 17 Abs. 1 VE DSG).

[Rz 94] Diese Bestimmung ist insofern bemerkenswert, als sie deutlich über die entsprechende Bestimmung der DSGVO hinausgeht, und zwar ohne ersichtlichen Grund. In der EU wird eine Meldung dann erforderlich sein, wenn im Rahmen einer Datenbearbeitung festgestellt wird, dass eine getroffene Sicherheitsmassnahme verletzt wurde (z.B. ein Einbruch in ein Computernetz oder ein Mitarbeiter, der weisungswidrig Daten auf einen privaten Memorystick kopiert) und diese Verletzung zu einem Bruch oder Verlust des Gewahrsams an den Daten führt.

[Rz 95] In der Schweiz soll die Meldepflicht hingegen jede Datenbearbeitung erfassen, die gegen das DSG verstösst, also z.B. eine zweckentfremdete oder unverhältnismässige Nutzung von Daten oder eine Datenbeschaffung, die in nicht transparenter Weise erfolgt. Solche Fälle kommen in jedem Betrieb erfahrungsgemäss jeden Tag vor. Die Ausnahme, in welchem Fall nicht gemeldet

werden muss, ist dabei schon so formuliert, dass sie im Falle einer Datenschutzverletzung nicht gegeben sein kann, stellt doch eine unbefugte Datenbearbeitung immer eine Persönlichkeitsverletzung dar.

[Rz 96] Selbst wenn nur die etwas schwereren Fälle gemeldet werden müssen, wird die Schweizer Regelung ungleich viel mehr Fälle erfassen, als gemäss der DSGVO der Aufsichtsbehörde gemeldet werden müssen. Sachliche Gründe gibt es dafür nicht. Der logische Grund für die Meldepflicht ist das Bedürfnis, der Aufsichtsbehörde die Möglichkeit zu geben, in den Umgang mit einer Datenschutzverletzung aktiv einzugreifen und zum Beispiel die Benachrichtigung der betroffenen Personen zu verlangen (vgl. Abs. 2). Müsste aber tatsächlich wie vorgesehen gemeldet werden und halten sich die Betriebe auch daran, würde der EDÖB jeden Tag mit einer Vielzahl von Meldungen geflutet werden. Die Idee der Regelung wäre durch sie selbst vereitelt.

[Rz 97] Die im Vorentwurf vorgesehene Meldepflicht bringt aber auch die Mitarbeiter in einem Unternehmen in eine Zwickmühle und sorgt für völlig unverhältnismässigen Druck und letztlich eine Angstkultur: Stellt zum Beispiel der interne Datenschutzverantwortliche eine Datenschutzverletzung im eigenen Betrieb fest und könnte sie zu einem Risiko für die betroffenen Personen führen, muss er sie dem EDÖB melden und damit die dafür verantwortlichen Personen «ans Messer» liefern: Je nach Verstoss werden sie dafür strafrechtlich verfolgt werden müssen[75], da der EDÖB seinerseits eine Anzeigepflicht hat (dazu Rz 119 unten). Tut der Datenschutzverantwortliche dies nicht, muss er selbst mit strafrechtlicher Verfolgung rechnen (Art. 50 Abs. 2 Bst. e VE DSG). Dies wird für ihn, der darauf angewiesen ist, dass andere Mitarbeiter mit ihm offen über Datenschutzprobleme sprechen, eine unhaltbare Situation sein. Doch auch dort, wo der Datenschutzverantwortliche selbst für den Datenschutzverstoss (mit-)verantwortlich ist, sind Konflikte vorprogrammiert (Stichwort *nemo tenetur*, vgl. Rz 125 unten).

[Rz 98] Die Meldepflicht ist daher mindestens auf das Niveau der DSGVO zu reduzieren, und selbst diese geht weit. Auch die strafrechtlichen Sanktionen sind zu überdenken bzw. zu prüfen, inwiefern eine Meldung möglicherweise sogar vor Strafe schützt, um einen möglichst offenen Umgang mit solchen Meldungen zu fördern. Sinnvoll erscheint eine Regelung, in welcher zudem nur Fälle gemeldet werden müssen, die eine Vielzahl von Personen betreffen, da sich ein Eingreifen der Aufsichtsbehörde nur dann wirklich rechtfertigt. Versendet ein Spital zum Beispiel einen heiklen Befund versehentlich an den falschen Patienten, ist das zwar eine gewichtige Persönlichkeitsverletzung, aber weshalb es in einem solchen Fall zum Schutz des betroffenen Patienten nötig sein sollte, dass der EDÖB eingeschaltet wird, ist nicht ersichtlich. Eine Pflicht, die betroffene Person direkt zu informieren, wenn es zum Schutz der betroffenen Person erforderlich ist, ist in Abs. 2 bereits vorgesehen.[76]

[Rz 99] Die Meldepflicht sollte zudem in zeitlicher Hinsicht relativiert werden. Statt einer «unverzüglichen» Meldung sollte eine Meldung ohne unnötigen Verzug stattfinden. Denn zwischen dem Erkennen eines Verstosses und dem Zeitpunkt, an welchem genügend Informationen vorliegen, damit sich der EDÖB ein vernünftiges Bild machen kann, vergeht normalerweise einige Zeit. Es bringt gar nichts, dem EDÖB vorab eine Mitteilung machen zu müssen, dass ein Unternehmen

75 So zum Beispiel die Mitarbeiter der Informatik, welche es unterlassen haben, die zum Schutz der Daten notwendigen Massnahmen zu treffen, was bei vorsätzlicher und fahrlässiger Begehung strafbar sein soll (Art. 51 VE DSG).

76 Der zweite Fall («oder der Beauftragte es verlangt») ist irreführend formuliert und überflüssig. Ist es zum Schutz der betroffenen Person nicht erforderlich, gibt es auch keinen Grund, warum der EDÖB eine Information verlangen sollte.

einen Datenschutzverstoss entdeckt hat, aber noch nicht wirklich sagen kann, was passiert ist, warum und welche Massnahmen es trifft. Der EDÖB ist ohnehin in einer viel schlechteren Lage zu beurteilen, was an Massnahmen sinnvollerweise zu ergreifen ist als das betroffene Unternehmen.

[Rz 100] In Abs. 4 wird schliesslich dem Auftragsbearbeiter die Pflicht auferlegt, den Verantwortlichen unverzüglich über eine unbefugte Datenbearbeitung zu informieren, wobei nicht klar wird, ob diese Pflicht nur Verstösse in seinem Verantwortungsbereich betrifft oder auch Verstösse, die der Auftragsbearbeiter seitens des Verantwortlichen wahrnimmt. Sachlogisch muss ersteres gelten. Anders als Abs. 1 sieht Abs. 4 allerdings keine Informationspflicht im Falle von Datenverlust vor. Korrekterweise ist der Hinweis auf den Datenverlust zu streichen, denn wenn ein Datenverlust nicht zugleich eine Datenschutzverletzung darstellt, gibt es in der Sache keinen Grund, diesen melden zu müssen.

13. Auftragsdatenbearbeitung

[Rz 101] Im Bereich der Auftragsdatenbearbeitung, die neu in Art. 7 VE DSG geregelt ist, soll sich mit drei Ausnahmen nicht viel ändern:

[Rz 102] Erstens wird nun ausdrücklich festgehalten, dass sich der Verantwortliche vergewissern muss, dass der Auftraggeber nicht nur in der Lage ist, die Datensicherheit zu gewährleisten, wie dies schon bisher ausdrücklich verlangt wurde, sondern neu auch, dass die Rechte der betroffenen Personen gewährleistet sind (Abs. 2). Was dies genau bedeutet, ist nicht wirklich klar, ist die Gewährleistung der Rechte der betroffenen Personen doch primär die Aufgabe des Verantwortlichen. Handelt es sich wie oft beim Auftragsbearbeiter um eine im Hintergrund agierende Person (wie z.B. ein Outsourcing-Dienstleister), tritt sie gegenüber den betroffenen Personen nicht auf und ist auch nicht deren Ansprechpartner. Richtigerweise müsste also sichergestellt sein, dass der Auftragsbearbeiter das in seinem Bereich Erforderliche tut, damit der *Verantwortliche* die Rechte der betroffenen Personen gewährleisten kann. So wird ein Verantwortlicher prüfen müssen, ob der Auftragsbearbeiter ihm den für einen Auskunftsanspruch erforderlichen Datenzugang gewährleistet oder dass er Datenlöschungen, die der Verantwortliche durchführen muss, ausführen kann.

[Rz 103] Zweitens dürfte der Mindestinhalt der Verträge zwischen Verantwortlichem und Auftragsbearbeiter neu indirekt durch die Verordnung zum DSG konkretisiert werden. Es ist zu vermuten, dass dies analog der Regelung der DSGVO erfolgt. Dies wird bedeuten, dass auf das Inkrafttreten des neuen DSG kurzfristig alle Verträge mit Auftragsbearbeitern überprüft werden müssen. Die Kompetenzdelegation in Abs. 2 ist jedoch problematisch: Sie spricht nicht von einer Konkretisierung der in Art. 7 VE DSG geregelten Grundsätze, sondern von «weiteren» Pflichten, was fallengelassen werden sollte: Es gibt keinen Anlass, dem Bundesrat das Recht einzuräumen, für die Auftragsdatenbearbeitung *weitere* Pflichten vorzusehen, als sie das DSG ohnehin schon vorsieht, und diese gehen schon jetzt zu weit. Eine solche Regelung ist überdies aus rechtsstaatlicher Sicht heikel.

[Rz 104] Drittens wird ein Auftragsbearbeiter weitere Auftragsbearbeiter neu nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen beiziehen dürfen (Abs. 3). Diese Regelung entspricht derjenigen der DSGVO, wobei dort klargestellt wird, dass auch eine generelle Einwilligung möglich ist, die noch keinen Bezug auf die einzelnen Unter-Auftragsbearbeiter nimmt. Zu

denken ist etwa an eine generische Klausel im Vertrag zwischen Verantwortlichem und Auftraggeber, in welchem die Zustimmung pauschal erteilt wird. In der DSGVO wird für diesen Fall verlangt, dass der Verantwortliche vor dem Beizug eines bestimmten Auftragsbearbeiters den Verantwortlichen über diesen informiert und ihm ein Vetorecht gibt. Dies sollte an sich auch für die Schweiz gelten, geht aus der neuen Bestimmung in Abs. 3 aber nicht hervor. Da dieses Vetorecht eine sehr spezielle Regelung darstellt, wäre es angezeigt, darauf hinzuweisen; bisher findet sich ein Hinweis lediglich in den Erläuterungen.[77] Ungenau ist auch der Hinweis auf die Notwendigkeit, dass die Zustimmung schriftlich erfolgt, denn wenn es sich dabei um Schriftlichkeit im Sinne von Art. 13 OR handelt[78], was normalerweise der Fall ist, wenn sich aus dem Gesetz nichts Weiteres ergibt, werden z.B. Online-Verträge mit Cloud- und Internet-Providern nicht mehr möglich sein, da diese regelmässig Unterauftragnehmer haben. Wesentlich kann nicht sein, dass die Zustimmung schriftlich im Sinne des OR erfolgt. Wesentlich ist, dass sie in dokumentierter Weise erfolgt, also ein Nachweis durch Text möglich ist.

[Rz 105] Aus der Regel des Zustimmungsvorbehalts in Abs. 3 ergibt sich implizit im Übrigen auch, dass es weiterhin erlaubt sein wird, dass es genügt, wenn die Verträge mit Unterbeauftragten nur mit dem Auftragsbearbeiter abgeschlossen werden, also keine direkte Vertragsbeziehung zum Verantwortlichen erforderlich ist.[79] Das ist in der Praxis ein wichtiger Aspekt und gilt so unter bestehendem Recht und auch in der EU. In diesen Fällen wird dann der Auftragsbearbeiter die Rolle des Verantwortlichen gegenüber dem Unterbeauftragten übernehmen. Bei diesem Fall zeigt sich auch, wie durchdacht und differenziert die bisherige Terminologie des Schweizer Rechts war: Es unterschied die Rolle der Inhaberschaft der Datensammlung (bzw. neu der Funktion des Verantwortlichen) von jener des Auftraggebers, da ein Auftraggeber nicht zwingend der (in letzter Instanz) Verantwortliche ist.

14. Brisant, aber kreativ: Die «Empfehlungen der guten Praxis»

[Rz 106] Die sicherlich kreativste aber auch rechtsstaatlich «speziellste» Neuerung des Vorentwurfs ist das Konzept der «Empfehlungen der guten Praxis» in Art. 8 und 9 VE-DSG. Die Idee ist in jedem Fall begrüssenswert; sie war auch schon im Vorfeld diskutiert worden und ist auch keine Schweizer Erfindung. Das österreichische Recht kennt sie zum Beispiel schon. Es adressiert das Grundproblem des DSG, das mit seinem Konzept «Prinzipien statt Regeln» zwar sehr flexibel ist und so bestens für die jeweiligen Umstände richtig angewandt werden kann, dadurch aber für den nicht bewanderten Leser zu wenig konkret ist und damit gewisse Rechtsunsicherheiten schafft: Er weiss in der Praxis oft nicht, was genau erlaubt ist und was nicht. Dem wurde bisher mit «Soft Law» begegnet. Neu soll es möglich sein, bestimmte Verhaltensweisen vom EDÖB als datenschutzkonform absegnen zu lassen (Art. 8 Abs. 2 VE DSG). Der EDÖB soll aber auch selbst «Empfehlungen» abgeben, wie sich bestimmte Dinge datenschutzkonform tun lassen (Abs. 1). Diese Empfehlungen sollen keine «*best practice*» sein, sondern lediglich «*good practice*», und in

77 Erläuterungen VE DSG, S. 52.

78 Welche Bestimmung in der Regel eine handschriftliche Unterschrift auf einem festen Träger erfordert.

79 Eine «Zustimmung» braucht es sachlogisch nur in Fällen, in welchen die zustimmende Partei selbst nicht Vertragspartei ist.

Art. 9 Abs. 2 VE DSG wird richtigerweise betont, dass sie in keiner Weise zwingend sind und der Datenschutz auch auf andere Weise eingehalten werden kann.

[Rz 107] Der Clou findet sich aber in Art. 9 Abs. 1 VE DSG, wonach die Einhaltung einer vom EDÖB verfassten oder genehmigten «Empfehlung der guten Praxis» für einen Verantwortlichen bedeutet, dass er die damit konkretisierten Bestimmungen des DSG befolgt hat (warum dies nicht auch für einen Auftragsbearbeiter gelten sollte, ist nicht ersichtlich; dies dürfte ein Versehen sein). Es handelt sich rechtstechnisch um eine Fiktion, die auch für die Gerichte bindend sein wird. Spannend ist dabei, dass in keiner Weise vorgesehen ist, wie oder dass der Erlass oder die Genehmigung einer Empfehlung einer rechtsstaatlichen Kontrolle unterliegen soll. Der EDÖB kann bezüglich seiner eigenen Empfehlungen gemäss Vorentwurf tun und lassen, was er will.

[Rz 108] Die Empfehlungen der guten Praxis qualifizieren nicht als Verfügungen und sind daher auch nicht als solche anfechtbar. Verfügungscharakter wird zwar Genehmigung einer Fremdempfehlung haben: Weist der EDÖB eine beispielsweise von einem Branchenverband vorgelegte Empfehlung als ungenügend ab, wird er auf Verlangen des Verbands eine beschwerdefähige Verfügung ausstellen müssen, gegen die der Verband vorgehen kann. Nach Art. 8 Abs. 2 VE DSG besteht ein Anspruch auf Genehmigung, wenn die vorgelegte Empfehlung mit den Vorschriften des DSG «vereinbar» ist. Sind umgekehrt die betroffenen Personen, deren Daten im Einklang mit einer solchen Empfehlung der guten Praxis bearbeitet werden, mit ihr nicht einverstanden, werden sie sich höchstens indirekt wehren können. Wie das gehen soll, ist aber völlig unklar, denn der Vorentwurf sieht hierzu nichts vor. Es ist in der Tat erstaunlich, dass die damit zusammenhängenden Fragen auch in den Erläuterungen nicht diskutiert werden. Dabei kann die Wirkung einer Empfehlung der guten Praxis massiv sein: Ist sie zu Unrecht genehmigt oder erlassen worden, beraubt sie die betroffenen Personen aufgrund der Fiktion der Gesetzmässigkeit der Datenbearbeitung ihrer gesetzlichen Rechte. Dem Autor ist ein vergleichbares Instrument des Schweizer Rechts bisher nicht bekannt. Hier sind eingehende Überlegungen zum Rechtsschutz erforderlich. Dazu gehört zum Beispiel auch eine Befristung der Empfehlungen der guten Praxis, deren Überarbeitung oder deren gerichtliche Überprüfung. Denkbar ist zum Beispiel ein System analog den Angemessenheitsentscheidungen der Europäischen Kommission, die zwar von den nationalen Gerichten nicht überprüft werden können, die Beurteilung eines Einzelfalls jedoch vorbehalten bleibt. So könnte beispielsweise festgehalten werden, dass die Einhaltung der Empfehlung der guten Praxis nicht eine Fiktion der Datenschutzkonformität zur Folge hat, sondern lediglich eine widerlegbare Vermutung.

[Rz 109] Schon vor diesem Hintergrund dürfte die Regelung, wonach der EDÖB alleine über Ausgestaltung oder Genehmigung einer solchen Empfehlung der guten Praxis bestimmen kann, dazu führen, dass er an solche Empfehlungen einen strengen, übergesetzlichen Massstab anlegen wird. Hinzu kommt, dass dem EDÖB inoffiziell die Rolle des «Beschützers» betroffener Personen und eine solche Empfehlung einen generell abstrakten Charakter haben muss und daher die Berücksichtigung der Umstände im Einzelfall gar nicht möglich ist. Empfehlungen der guten Praxis werden daher zweifellos nicht das Minimum dessen umschreiben, was zur Einhaltung des DSG getan werden muss, sondern letztlich trotz allem eine «beste Praxis» sein, nicht nur eine «gute Praxis». Ihre Gefahr wird darin liegen, dass sie von Gerichten möglicherweise als Richtschnur für die korrekte Umsetzung des DSG herangezogen werden und sie daher bewirken, dass diese das DSG im Ergebnis zu Lasten der Interessen der Datenbearbeiter anwenden, wie dies vom Gesetzgeber an sich nicht beabsichtigt war.

[Rz 110] Weiter stellt sich nebst den bereits angeführten Punkten die Frage, ob es nicht erforderlich ist, ein im Gegensatz zum EDÖB *neutrales*, von ihm unabhängiges Gremium über die Geltung von Empfehlungen der guten Praxis bestimmen zu lassen, wie zum Beispiel eine Kommission, in welcher insbesondere auch Vertreter aus der Praxis einsitzen. Denn Praxiswissen ist gerade in diesem Bereich von zentraler Bedeutung, fehlt dem EDÖB aber erfahrungsgemäss oftmals. Eine solche Vorgehensweise würde den EDÖB zudem personell entlasten und wäre vergleichsweise kostengünstig umzusetzen; dagegen spricht, dass eine solche Kommission ein de facto politisches Gremium wäre, während es vorliegend wichtig ist, Entscheide auf einer Sachebene zu fällen.

[Rz 111] Ein möglicher Ansatz wäre auch, dem EDÖB gar nicht zu gestatten, eigene Empfehlungen der guten Praxis erlassen zu dürfen, sondern nur solche zu genehmigen, die ihm von privater Seite vorgelegt werden. Das Instrument hätte dann stärker den Charakter einer Selbstregulierung. Diese Lösung würde auch dem in breiten Kreisen vorhandene Unbehagen begegnen, dass der EDÖB über seine eigenen Empfehlungen der guten Praxis strengere Anforderungen an ein datenschutzkonformes Verhalten einführt, als das Gesetz es verlangt. In der Vergangenheit wurden seitens des EDÖB immer wieder Regelungen als geltendes Recht vertreten, die klar keine gesetzliche Grundlage haben.[80] Mindestens jedoch sollte der EDÖB verpflichtet werden, die betroffenen Verkehrskreise vor dem Erlass einer Empfehlung der guten Praxis zu konsultieren bzw. eine gerichtliche Überprüfung solcher Empfehlungen durch diese vorgesehen werden, analog dem heute gegen unzulässige öffentliche Behauptungen des EDÖB möglichen Vorgehen gegen Realakte.

15. Aufsicht und Sanktionen: Deutlich härtere Gangart

[Rz 112] Die mit Sicherheit am meisten beachtete neue Regelung des Vorentwurfs sind die Sanktionen, die neu eingeführt werden. Heute kennt das DSG keine nennenswerten Sanktionen; sanktioniert werden gewisse Verhaltensweisen im Zusammenhang mit dem Auskunftsrecht, die vorsätzliche Unterlassung der besonderen Informationspflicht bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen und der Kooperations-, Registrier- und Meldepflichten gegenüber dem EDÖB. Sie führten in der Praxis zu so gut wie keinen Verurteilungen.

[Rz 113] Dass sich dies mit dem Vorentwurf ändern würde, war klar, verlangt doch auch die revidierte Konvention 108 die Einführung von «Administrativsanktionen» im Falle einer Datenbearbeitung, welche die Vorgaben der Konvention verletzt.[81] Vor diesem Hintergrund war erwartet worden, dass der Vorentwurf für Datenschutzverletzungen künftig Verwaltungssanktionen einführt, wie sie auch schon diverse andere Gesetze wie etwa das Fernmeldegesetz oder Kartellgesetzt kennen. Diese sehen Bussen von bis zu zehn Prozent des Jahresumsatzes vor. Die DSGVO setzt ebenfalls hauptsächlich auf Verwaltungssanktionen, die dort bis zu vier Prozent des Jahresumsatzes entsprechen dürfen, allerdings bemessen am weltweiten Umsatz des Unternehmens oder der Unternehmensgruppe, dies je nach Lesart der DSGVO.[82]

---

80 So beispielsweise, dass die Bearbeitung von Persönlichkeitsprofilen eine Einwilligung erfordert. Das Gesetz verlangt nur bei der *Bekanntgabe* von Persönlichkeitsprofilen an Dritten eine Einwilligung *oder* einen anderen Rechtfertigungsgrund.

81 Art. 12bis Abs. 2 Bst. c der revidierten Konvention 108 (Entwurf Stand September 2016).

82 Art. 83 DSGVO.

[Rz 114] Es kam anders: Art. 50 ff. VE DSG setzt primär auf private, strafrechtliche Sanktionen gegen die einzelnen, in eine Verletzung des DSG involvierten Organe und Mitarbeiter. Der Vorentwurf geht somit auch hier über die DSGVO und das, was von der Konvention 108 verlangt wird, hinaus. Der Bussenrahmen beträgt CHF 500'000 für die vorsätzliche Begehung der einzelnen Delikte, erfasst aber mit Bussen von bis zu CHF 250'000 auch fahrlässige Datenschutzverstösse. Ein fahrlässiger Verstoss gegen das DSG kann somit gleich massiv geahndet werden wie die fahrlässige Verletzung des Bankgeheimnisses. Zum Vergleich: Die fahrlässige Verletzung des Amts-, Anwalts- oder Arztgeheimnisses ist nicht strafbar.[83]Immerhin: Anstiftung und Gehilfenschaft sind bei Übertretungen wie hier nicht strafbar.

[Rz 115] Art. 53 VE DSG sieht zwar vor, dass von der Ermittlung der strafbaren Person in einem Betrieb abgesehen werden kann, wenn die Busse CHF 100'000 nicht überschreiten wird; in diesem Falle wird das Unternehmen gebüsst. Der einzelnen Person, die sich durch eine Handlung möglicherweise strafbar macht, wird diese Regelung jedoch kaum den nötigen Komfort geben, da ihre Strafbarkeit von einem entsprechenden Entscheid der ermittelnden Behörde abhängt. 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.[84]

[Rz 116] Der persönliche, strafrechtliche Charakter der Sanktionen ist unverhältnismässig und nicht zielführend. Speziell diejenigen Personen, die wie etwa betriebliche Datenschutzverantwortliche in ihrer Tätigkeit für den Datenschutz an sich geschützt und gestärkt werden sollten, werden durch die Schaffung eines persönlichen Strafbarkeitsrisikos unnötig unter Druck gesetzt und exponiert (vgl. z.B. Rz 97 oben). Mitarbeiter in den Unternehmen werden sich hüten, in strafrechtlich bedrohten Datenschutzfragen selbst Entscheide zu treffen, ohne sich über externen Rechtsrat durch Spezialisten abgesichert zu haben, was zu einer unnötigen Verteuerung der Datenbearbeitung führt und dazu, dass die Möglichkeiten des DSG zur Datenbearbeitung nicht mehr ausgeschöpft werden. Damit aber kommt der vom Gesetzgeber gewollte Ausgleich zwischen den Interessen der betroffenen Personen und der Datenbearbeiter nicht mehr zum Tragen. Die ersten Reaktionen auf den Vorentwurf lassen vermuten, dass die gegenwärtig vorgeschlagenen strafrechtlichen Sanktionen politisch wenig Chancen haben werden.

[Rz 117] Das gilt ganz besonders für die Strafbarkeit von fahrlässigen Verstössen gegen das DSG. Solche Verstösse sind natürlich nicht hinzunehmen, aber eine Kriminalisierung der einzelnen Mitarbeiter ist stossend, zumal die Delikte in den meisten Fällen «nur» in der Verletzung *flankierender* Massnahmen wie etwa eine unterlassene Datenschutz-Folgenabschätzung oder Dokumentation der Datenbearbeitung bestehen, durch welche die betroffenen Personen zunächst nicht wirklich in ihrer Privatsphäre verletzt sind. Pikanterweise sind jene Fälle, in denen die Persönlichkeit einer betroffenen Person tatsächlich verletzt werden, nicht unter Strafe gestellt. Gebüsst wird nicht derjenige, der Personendaten bewusst zweckwidrig oder unverhältnismässig verwendet, sondern derjenige, der vergisst, diese Datenschutzverletzung dem EDÖB zu melden. Das kann nicht sein.

---

83 Art. 320 f. StGB.

84 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, 3. Auflage, Art. 305 StGB, N 20, m.w.H.).

[Rz 118] Einige Stimmen vertreten gar die Ansicht, dass es gar keine Sanktionen braucht, was aus Sicht des Datenschutzes sicherlich stimmt (die Nichteinhaltung einer Verfügung des EDÖB könnte bereits mit der bestehenden Regelung von Art. 292 des Schweizerischen Strafgesetzbuches StGB sanktioniert werden), aber für manche im Widerspruch zum Wortlaut der Konvention 108 steht. Es kann immerhin vertreten werden, dass der Begriff der Administrativsanktion nicht zwingend eine Geldbusse erfordert; auch ein Bearbeitungsverbot könne eine solche sein, wird argumentiert. Allerdings dürften die realpolitischen Chancen, dass das revidierte DSG keine finanziellen Sanktionen enthält, sehr gering sein.

[Rz 119] Wer nach den Gründen der scharfen Regelung im Vorentwurf forscht, dem wird rasch klar, dass sie rein opportunistischer Natur sind: Dem EDÖB soll offenkundig nicht die mit der Sanktionierung von Datenschutzverstössen verbundene (Arbeits-)Last auferlegt werden. Durch eine strafrechtliche Sanktionierung können die Fälle an die Kantone abgeschoben werden.[85] Kommt diese Regelung durch, werden die kantonalen Staatsanwaltschaften künftig auch einen Datenschutzjuristen einstellen müssen, um die betreffenden Fälle zu untersuchen und abzuurteilen. Dies zeigt zugleich, wie ineffizient diese Regelung ist: Zwar ist es denkbar, dass ein Datenschutzverstoss von einer betroffenen Person direkt zur Anzeige gebracht und untersucht wird. Der Regelfall wird jedoch sein, dass ein Fall zunächst vom EDÖB untersucht werden wird (dazu Rz 126 unten). Dieser soll dann im Falle eines strafrechtlich relevanten Verhaltens Anzeige erstatten; Art. 45 VE DSG verpflichtet ihn dazu. Derselbe Fall wird dann von der zuständigen Strafbehörde nochmals untersucht werden müssen. Dies ist auch zwingend erforderlich, da nur so die strafprozessualen Rechte der Beschuldigten gewahrt werden können. Dass sich die Strafbehörden mangels eigener Datenschutzerfahrung wohl auf die Einschätzung des EDÖB abstützen werden, macht die Sache rechtsstaatlich nicht besser.

[Rz 120] Der gewählte Weg der strafrechtlichen Sanktion zwingt auch zur Befassung mit dem strafrechtlichen Bestimmtheitsgebot.[86] Dies dürfte mit ein Grund dafür sein, dass vor allem formelle Pflichten bzw. Massnahmen zur Datenschutz-Governance und –Aufsicht strafrechtlich sanktioniert werden und nicht datenschutzwidrige Datenbearbeitungen selbst. Der gewählte Ansatz ändert jedoch nichts daran, dass viele der sanktionierten Bestimmungen viel zu offen formuliert sind, dass es für den Rechtsunterworfenen schwierig sein wird zu verstehen, was er genau tun darf und was nicht. Dies wird dazu führen, dass er entweder weniger weit geht, als er dies an sich tun können sollte, oder es wird schwierig werden, ihn strafrechtlich zu belangen, weil das DSG das sanktionierte Verhalten zuwenig bestimmt umschreibt.

[Rz 121] Inhaltlich werden die Strafregelungen ebenfalls überarbeitet werden müssen. So sind ein Teil der Delikte nur auf Antrag strafbar, doch ist unklar, wer in solchen Fällen antragsberechtigt sein soll. Beispiele sind die Pflicht zur Dokumentation von Datenbearbeitungen oder die Durchführung einer Datenschutz-Folgenabschätzung (Art. 51 VE DSG). Antragsberechtigt sind jedoch nur Personen, die durch eine solche Unterlassung verletzt werden.[87] Durch die Unterlassung einer Dokumentation oder Folgenabschätzung wird jedoch niemand verletzt, jedenfalls nicht direkt oder höchstens in sehr speziellen Konstellationen. Die Bestimmung bleibt damit toter Buchstabe. Der EDÖB kann ebenfalls nicht sanktionieren, und auch eine etwaige Strafanzeige seinerseits wäre unbeachtlich.

85 Art. 54 VE DSG, welche Bestimmung jedoch überflüssig ist.

86 Art. 1 StGB.

87 Art. 30 Abs. 1 StGB.

[Rz 122] Die Strafbestimmungen in Art. 50 f. VE DSG sind nicht die einzigen, die eingeführt oder angepasst werden sollen:

- Das heute in Art. 35 DSG geregelte «kleine» Berufsgeheimnis, das bisher nur besonders schützenswerte Personendaten und Persönlichkeitsprofile schützte, wird ausgebaut und zu einem allgemeinen Berufsgeheimnis für jeden erweitert, der für die Zwecke seines Berufes geheime Personendaten bearbeiten muss oder solche schlicht zu «kommerziellen Zwecken» bearbeitet. Statt den Verrat nur mit Busse zu sanktionieren, sieht die Norm neu auf Antrag eine Freiheitsstrafe von bis zu drei Jahren oder Geldstrafe vor. Die Bestimmung steht damit dem «grossen» Berufsgeheimnis für Anwälte, Ärzte und Geistliche[88] in nichts mehr nach. Im Gegenteil: Eine Befreiung von der Geheimnispflicht durch eine etwaige Aufsichtsbehörde ist nicht vorgesehen. Die Auswirkungen dieser Anpassung sind noch unklar. Gegenüber Art. 162 StGB grenzt sich die Bestimmung dadurch ab, dass sie nicht nur Geschäftsgeheimnisse, sondern auch «private» Geheimnisse schützt. Weiter kann die Frage gestellt werden, ob die Norm nur dann angewandt werden kann, wenn mindestens implizit zwischen Geheimnisherr und Geheimnisträger eine vertragliche Geheimhaltungspflicht besteht, wie sie Art. 162 StGB verlangt oder zum Beispiel auch das Bankgeheimnis.[89] Soll die Anwendung nicht uferlos werden, wird verlangt werden müssen, dass die Information nicht nur geheim ist, sondern der Geheimnisherr auch eine berechtigte, in einem Vertrag oder sonstigem Verhalten oder Übung begründete Erwartung hat, dass der Geheimnisträger sie auch geheim halten wird. Doch selbst dann hat die Bestimmung einige Sprengkraft, da sie sehr viele Personen, die sich dem gar nicht bewusst sein werden und dies auch nicht erwarten, neu einem strafrechtlich sanktionierten Berufsgeheimnis unterstellt, weil argumentiert wird, dass sie implizit eine Geheimhaltungspflicht haben. So gehen die Erläuterungen offenbar davon aus, dass künftig auch Online-Händler und Betreiber sozialer Netzwerke mit Bezug auf die Daten ihrer Kunden unter diese Regelung fallen und sie etwa zur Anwendung gelangen kann, wenn diese für Marketingzwecke unberechtigterweise verkauft werden.[90] Es wird nicht lange dauern bis argumentiert werden wird, dass eine vorsätzlich datenschutzwidrige Bekanntgabe von nicht jedermann zugänglichen Personendaten in einem Geschäftsbetrieb immer auch eine Verletzung der beruflichen Schweigepflicht darstellt und daher mit bis zu drei Jahren Freiheitsstrafe sanktioniert werden kann. Das erscheint nicht angemessen. Die mit der Anpassung angestrebte Anlehnung an Art. 321 StGB leuchtet nur auf den ersten Blick ein: In den in Art. 321 StGB erfassten Berufen ist es für alle Beteiligten klar, dass Kundendaten grundsätzlich vertraulich zu behandeln sind. Bei einem Online-Shop oder einem sozialen Netzwerk ist das eben nicht der Fall; die beiden Anwendungsvoraussetzungen von Art. 52 VE DSG lösen dieses Problem nicht, da sie beliebig viele Fälle erfassen. Hier wäre entscheidend, dass nur solche Daten der beruflichen Schweigepflicht unterliegen, für welche eine Schweigepflicht unabhängig von Art. 52 VE DSG klar besteht, denn sonst unterliegt so gut wie jeder Berufstätige einer strafrechtlich sanktionierten Schweigepflicht, was unsinnig ist. Es stellt sich die Frage, warum der bisherige Art. 35 DSG nicht einfach beibehalten wird; einen guten Grund für seine Anpassung ist jedenfalls nicht ersichtlich und ein diesbezüglicher Leidensdruck besteht auch nicht wirklich.

88 Art. 321 StGB.

89 Art. 47 BankG.

90 Erläuterungen VE DSG, S. 86.

- Art. 179^{novies} StGB soll ebenfalls ausgeweitet werden und stellt neu jeden auf Antrag unter Strafe, der «unbefugt» Personendaten beschafft, «die nicht für jedermann zugänglich sind». Die Strafandrohung ist mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe deutlich höher als die Bussen, die für sonstige Datenschutzverletzungen vorgesehen sind. Allerdings ist nicht klar, inwiefern die mit der neuen Formulierung zu erfassenden Delikte von den sonstigen Datenschutzverletzungen abgrenzen sollen. Die bisherige Regelung kam nur dann zum Tragen, wenn unbefugt nicht frei zugängliche besonders schützenswerte Personendaten oder Persönlichkeitsprofile aus einer Datensammlung beschafft wurden. Gemeint waren damit allerdings Datendiebstähle aus gesicherten Systemen und Räumen, und nicht eine blosse Verletzung des Datenschutzes, indem eine Person etwa unter Missachtung des Transparenz- oder Verhältnismässigkeitsgrundsatzes Daten erhob, was ja nach Wortlaut ebenfalls erfasst wäre und den Anwendungsbereich der Norm massiv erweitert hätte. Dies scheint trotz einer geringfügigen Anpassung des Wortlauts (neu «für jedermann zugänglich» statt wie heute «frei zugänglich») nicht der Fall zu sein. Die Erläuterungen sprechen jedenfalls lediglich darüber, dass die von der Bestimmung erfassten Datenkategorien erweitert werden sollen.[91] Die «Unbefugtheit» meint somit nicht unbefugt im Sinne einer Verletzung des DSG (wie etwa in Art. 11 VE DSG), sondern ohne Befugnis des für die Daten Verantwortlichen.[92]
- In Art. 179^{decies} StGB neu eingeführt werden soll schliesslich eine Bestimmung zur strafrechtlichen Ahndung des Identitätsmissbrauchs.[93] Er soll dann bestraft werden können, wenn die Identität einer anderen Person dazu verwendet wird, dieser zu schaden oder sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen. Diese Bestimmung erscheint sinnvoll, da gegen ein solches Verhalten bisher meist nur zivilrechtlich vorgegangen werden konnte, was wiederum regelmässig daran scheiterte, dass die Identität des Täters ohne strafprozessuale Mittel nicht ermittelt werden konnte.

[Rz 123] Nebst Strafbestimmungen sollen auch die Rechte des EDÖB erweitert werden. Das bisherige System der Sachverhaltsabklärungen, Empfehlungen und Klagen vor Bundesverwaltungsgericht wird, obwohl es gut funktioniert, abgeschafft. Neu soll der EDÖB die Kompetenz erhalten, gegen Datenbearbeiter verwaltungsverfahrensrechtliche Untersuchungen durchzuführen (Art. 41 VE DSG) und gegen diese Verfügungen zu erlassen, sei es in Form von vorsorglichen Massnahmen (Art. 42 VE DSG), sei es, um eine Datenbearbeitung anzupassen, sie zu stoppen, einschliesslich der Bekanntgabe ins Ausland, oder um Daten zu vernichten (Art. 43 VE DSG). Der EDÖB soll offenbar sogar die Kompetenz erhalten, gegen eine Bekanntgabe ins Ausland selbst dann vorzugehen, wenn sie nicht gegen das DSG, sondern gegen ein anderes Gesetz verstösst; was dies bedeuten soll, wird aber nicht näher erläutert.[94]

[Rz 124] Problematisch ist in diesem Zusammenhang, dass Beschwerden gegen vorsorgliche Massnahmen *per se* keine aufschiebende Wirkung haben sollen (Art. 44 Abs. 3 VE DSG). Hierbei ist zu berücksichtigen, dass eine vorsorglich verfügte Einstellung oder Anpassung einer Datenbearbeitung gerade im Bereich der automatisierten Datenbearbeitung massive Kosten bzw. Schäden zur Folge haben kann, die der EDÖB regelmässig nicht einschätzen können wird. Solange der Staat bzw. der EDÖB für diese nicht aufkommt, muss ein Unternehmen die Möglichkeit haben, sich

91 Erläuterungen VE DSG, S. 93.

92 David Rosenthal, Handkommentar DSG, Zürich 2008, Art. 179^{novies} StGB, N 17.

93 Diese Bestimmung geht zurück auf die Motion Comte 14.3288.

94 Erläuterungen VE DSG, S. 80, mit Verweis auf Art. 12 Abs. 2 des Entwurfs der revidierten Konvention 108.

vor einer unabhängigen Instanz gegen ein unverhältnismässiges Vorpreschen des EDÖB wehren zu können. Das bisherige System, dass der EDÖB solche Massnahmen vom Bundesverwaltungsgericht beantragen musste, hat sich bestens bewährt (und gezeigt, dass der EDÖB gewisse vorsorgliche Massnahmen auch unberechtigt verlangt hat[95]).

[Rz 125] Das Verfahren richtet sich neu nach dem Verwaltungsverfahrensgesetz. Gemäss Vorentwurf soll der EDÖB das Recht haben, ohne Vorankündigung Hausdurchsuchungen durchzuführen und sich Zugang zu allen notwendigen Daten und Information zu verschaffen, muss das untersuchte Unternehmen aber vorgängig erfolglos zur Mitwirkung angehalten haben (Art. 41 Abs. 3 VE DSG). Wie das im Einzelnen vor sich gehen soll, bleibt unklar. Nicht wirklich diskutiert sind auch so heikle Fragen wie der Grundsatz *nemo tenetur* – das Recht zu Vorwürfen gegen die eigene Person zu Schweigen bzw. sich nicht selbst belasten zu müssen –, die sich angesichts der Pflicht zur Meldung von Datenschutzverstössen und den strafrechtlichen Konsequenzen akzentuiert stellen.

[Rz 126] Der EDÖB kann jederzeit ein Verfahren eröffnen, wenn Anzeichen bestehen, dass gegen das DSG verstossen wird; es muss nicht mehr eine grössere Zahl von Personen betroffen sein. Eine Pflicht zur Untersuchung besteht allerdings nicht, auch nicht im Falle einer Anzeige einer betroffenen Person. Immerhin muss der EDÖB diese über sein Vorgehen und das Ergebnis einer allfälligen Untersuchung informieren (Art. 41 Abs. 5 VE DSG); Partei ist sie nicht (Art. 44 Abs. 2 VE DSG), aber es steht ihr selbstverständlich offen, gestützt auf das ihr mitgeteilte Ergebnis (und weiteren Informationen, die sie über ein Gesuch nach Öffentlichkeitsgesetz erhält) gegen den Verantwortlichen zivilrechtlich vorzugehen. Diese neuen Bestimmungen sind aufgrund der Vorgaben der revidierten Konvention 108 und der politischen Stimmung erwartet worden. Viele Beobachter gehen jedoch auch davon aus, dass die Neuerungen dem Datenschutz nicht dienen werden: Zwar erhält der EDÖB mehr und schärfere Instrumente zur Aufsicht in die Hand, doch damit verbunden wird ebenso der Aufwand, den er für die entsprechenden Verfahren betreiben muss, deutlich steigen. Da jedenfalls bei der heutigen politischen Grosswetterlage nicht davon auszugehen ist, dass ihm hierfür mehr Mittel zur Verfügung stehen werden, wird er im Ergebnis weniger Fälle durchführen können. Immerhin soll ihm weiterhin das Recht zustehen, auch ausserhalb eines formellen Untersuchungsverfahrens zu überprüfen, ob ein Unternehmen (oder eine Behörde) die Datenschutzvorschriften einhält (Art. 41 Abs. 4 VE DSG). Obwohl in diesen Fällen kein Zwang zur Kooperation besteht, ist ein Widerstand seitens der betroffenen Unternehmen kaum zu erwarten.

16. Und wo bleiben die Übergangsregelungen?

[Rz 127] Schon bei der letzten Revision des DSG im Jahre 2008 stellten sich hinsichtlich der Übergangsregelungen etliche Fragen. Angesichts der noch sehr viel zahlreicheren Neuerungen, die der Vorentwurf vorsieht, erstaunt es daher, dass die Übergangsbestimmungen in Art. 59 VE DSG so mager ausgefallen sind.

95 So im Fall Moneyhouse im Sommer 2012, in welchem eine superprovisorische Sperrung des Dienstes kurze Zeit danach wieder aufgehoben wurde (vgl. https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-45545.html).

[Rz 128] Zwei Jahre Zeit wird gewährt für die Erstellung der Dokumentation der zum Zeitpunkt des Inkrafttretens des revidierten DSG bereits bestehenden Datenbearbeitungen, zur diesbezüglichen Einführung des «*Privacy by Default*» und «*Privacy by Design*» und eines Verfahrens zur Datenschutz-Folgenabschätzung. Warum selbiges zum Beispiel nicht auch für ein Verfahren zur Meldung von Datenschutzverstössen gelten soll, bleibt unklar. Es fehlen auch Übergangsregelung für andere wichtige Punkte wie zum Beispiel die neuen Informations- und Auskunftspflichten, automatisierten Einzelentscheiden und Verträge mit Auftragsbearbeitern.

[Rz 129] Die einfachste Lösung wird daher sein, für die Umsetzung des revidierten DSG eine generelle Umsetzungsfrist von zwei Jahren vorzusehen. Zwar steht die Schweiz unter einem gewissen Druck der EU, ihr Datenschutzrecht anzupassen. Entscheidend wird jedoch sein, dass das Parlament das DSG revidiert, und nicht, wann genau es in Kraft tritt. Überdies hat die EU für die DSGVO ebenfalls eine Umsetzungsfrist von zwei Jahren vorgesehen, und zwar für alle Bestimmungen.

17. Abgrenzung zur DSGVO

[Rz 130] Viele Schweizer Unternehmen sehen sich heute nicht nur mit den Anforderungen eines revidierten DSG konfrontiert, sondern werden auch in den Geltungsbereich der DSGVO fallen. Dies ist nach Art. 3 DSGVO zum Beispiel dann der Fall, wenn sie Daten von Personen in der EU bearbeiten, weil sie diesen dort Produkte oder Dienstleistungen anbieten oder weil sie deren Verhalten analysieren, oder wenn sie deren Daten durch einen Auftragsbearbeiter in der EU (z.B. einen Cloud-Provider) bearbeiten lassen. Damit unterstehen diese Unternehmen zugleich auch der Aufsicht der nationalen EU-Datenschutzbehörden, die zwar nach Art. 55 Abs. 1 DSGVO nur jeweils für ihr «Hoheitsgebiet» zuständig sind, dieser Begriff aber gemäss den Erwägungen der DSGVO extraterritorial zu interpretieren ist.[96] Dies bedeutet für viele Schweizer Unternehmen, die Daten von Personen in der EU bearbeiten, dass sie inskünftig sowohl der Datenschutzaufsicht der Schweiz als auch aller von der Datenbearbeitung betroffenen Mitgliedstaaten der EU (und des EWR) unterstehen.[97] Dies wird zu einer massiven administrativen Zusatzbelastung für Schweizer Unternehmen führen, und überdies zu zahlreichen Rechtsunsicherheiten, da die DSGVO mit Bezug auf ihre Geltung für Unternehmen ausserhalb des Territoriums der EU unsorgfältig redigiert und nicht durchdacht ist.[98] Die Aufsichtstätigkeit der nationalen Datenschutzbehörden der EU-Mitgliedsstaaten auf Schweizer Hoheitsgebiet stellt wiederum die Schweizer Souveränität in Frage und birgt auch für daran mitwirkende Schweizer Unternehmen ein Risiko der Strafbarkeit nach Art. 271 StGB. Die Situation ist also mit anderen Worten konfus und verfahren.

[Rz 131] Vor diesem Hintergrund besteht dringender Abstimmungsbedarf zwischen der offiziellen Schweiz und der EU. Informelle Kontakte diesbezüglich bestehen bereits, und auch die Politik hat den Handlungsbedarf bereits erkannt. Eine Motion «Gegen Doppelspurigkeiten im

96 Erwägung 122 DSGVO.

97 Das Konzept des *One-Stop-Shop* gemäss Art. 56 DSGVO steht für Unternehmen ausserhalb der EU nicht zur Verfügung (vgl. dazu die «Guidelines for identifying a controller or processor's lead supervisory authority» der Artikel-29-Datenschutz-Arbeitsgruppe, WP 244, S. 7).

98 So ist zum Beispiel nicht klar, ob sich ein Schweizer Unternehmen auf Schweizer Recht zur Rechtfertigung einer Datenbearbeitung im Sinne von Art. 6 Abs. 1 Bst. c DSGVO berufen kann; gemäss Art. 6 Abs. 3 DSGVO scheint dies nicht der Fall zu sein, was jedoch zu unbilligen Ergebnissen führt.

Datenschutz»[99] wurde bereits im September 2016 eingereicht und vom Bundesrat zur Annahme empfohlen[100]; der Nationalrat ist dem im Dezember 2016 bereits gefolgt. Im besten Fall kommen die Behörden der beiden Rechtsordnungen überein, dass die (verwaltungsrechtliche) Aufsicht auf dem jeweiligen Hoheitsgebiet alleine Sache der jeweils nationalen Behörde ist, die sie nach ihrem eigenen Recht umsetzt. In diesem Fall wären aufsichtsrechtlich für Datenbearbeitungen durch Unternehmen in der Schweiz einzig der EDÖB zuständig, der sie nach DSG beurteilen würde. Auch die Informations- und Genehmigungspflichten würden für diese Unternehmen nur gegenüber ihm gelten; Schweizer Unternehmen müssten beispielsweise eine Datenschutzverletzung nur ihm und nicht auch allen betroffenen Datenschutzaufsichtsbehörden der jeweiligen EU-Mitgliedsstaaten mitteilen, und zwar nach den Vorgaben des DSG, nicht der DSGVO. Der Informationsfluss zwischen dem EDÖB und den Datenschutzbehörden der EU wäre über die im Vorentwurf ebenfalls vorgesehenen Bestimmungen zur Amtshilfe sichergestellt. Der zivilrechtliche Rechtsschutz bliebe jedoch unberührt, d.h. ein betroffener EU-Bürger könnte auch gegen ein Schweizer Unternehmen gestützt auf DSGVO vorgehen.[101] Dieser Rechtsschutz spielt in der Praxis jedoch eine untergeordnete Rolle.

[Rz 132] Es bleibt zu hoffen, dass die Bundesverwaltung die Gespräche mit der EU möglichst rasch auch offiziell aufnimmt. Zwar gibt es vereinzelt Stimmen, die der Ansicht sind, ein solches Vorgehen habe ohnehin keine Chance, weil die Schweiz gegenüber der EU keine Forderungen stellen könne. Die Realität in der EU zeigt jedoch, dass die EU ebenso an einer Abstimmung mit der Schweiz interessiert ist wie umgekehrt, da mit der Datenschutzaufsicht auch erhebliche Kosten verbunden sind. Kann die Datenschutzaufsicht über Unternehmen mit Sitz in der Schweiz faktisch an den EDÖB «delegiert» werden, kommt dies den einzelnen nationalen Aufsichtsbehörden entgegen, jedenfalls solange die Schweiz über vergleichbare Datenschutzregelungen verfügt und sie ihre Rechte bei Bedarf auf dem Weg der Amtshilfe durchsetzen können, was beides der Fall ist oder noch sein wird. Umgekehrt ist es politisch undenkbar, dass die Schweiz es zulässt, dass EU-Datenschutzbehörden eigene Zwangsmassnahmen nach eigenem EU-Recht durch den EDÖB auf Schweizer Territorium vollziehen lassen oder sogar direkt gegen Unternehmen in der Schweiz durchsetzen.[102] Die britische Regierung wird im Rahmen des BREXIT ähnliche Gespräche führen. Art. 50 Bst. a DSGVO sieht die Kompetenz zur Entwicklung solcher Mechanismen der internationalen Zusammenarbeit zur wirksamen Durchsetzung des Datenschutzes für die Europäische Kommission und die nationalen Aufsichtsbehörden im Übrigen bereits vor.

---

99 Motion Fiala 16.3752.

100 Wenngleich die Begründung des Bundesrats inhaltlich fehlerhaft ist, da sie die Erwägung 122 der DSGVO übersieht. Der Bundesrat geht noch davon aus, dass die EU-Aufsichtsbehörden keine Zuständigkeit für Aktivitäten auf dem Territorium der Schweiz beanspruchen, was falsch ist.

101 Bereits der heutige Art. 139 des Bundesgesetzes über das Internationale Privatrecht (IPRG) gibt einer betroffenen Person weitreichende Wahlrechte mit Bezug auf das Datenschutzrecht, welches auf ihren Fall anwendbar sein soll. Die extraterritoriale Anwendbarkeit, welche Art. 3 Abs. 2 DSGVO neu vorsieht, kennt die Schweiz damit schon lange. Es stellt sich freilich die Frage, ob es sinnvoll wäre, im Zuge der Revision des DSG auch hier gewisse Einschränkungen vorzunehmen und beispielsweise festzuhalten, dass ein ausländischer Erfolgsort (und damit die Anwendbarkeit von ausländischem Datenschutzrecht) nicht allen damit begründet werden kann, dass die Daten im betreffenden Land gespeichert werden. Dies würde beitragen, dass auf Schweizer Unternehmen nicht schon deshalb die DSGVO zur Anwendung kommen könnte, weil sie einen Cloud-Provider in der EU benutzen.

102 Die im Vorentwurf vorgeschlagene Amtshilfebestimmung in Art. 47 VE DSG bleibt diesbezüglich vage. Eine direkte Durchsetzung wäre eine Verletzung von Art. 271 StGB.

18. Schlussbemerkungen

[Rz 133] Im Vorentwurf für ein totalrevidiertes DSG steckt wesentlich mehr verborgen, als es auf den ersten Blick den Anschein macht. Positiv zu vermerken ist, dass die Schweiz der bewährten Tradition, mit Prinzipien statt ausformulierten Regeln zu arbeiten, treu bleiben will. Die Bestimmungen des allgemeinen Teils und des Teils für die Bearbeitung durch Privatpersonen beansprucht neu zwar 25 statt bisher 15 Artikel, doch ist das Gesetzeswerk dennoch erfreulich schlank und kein Vergleich zu den 99, teils furchtbar kompliziert und langwierig verfassten Artikeln der DSGVO.

[Rz 134] Der Vorentwurf erweckt zudem den Eindruck, dass das Bundesamt für Justiz im Datenschutz keine Revolution, sondern eine Evolution suchte mit dem primären Ziel, die Revision der Konvention 108 des Europarats nachzuvollziehen und die Adäquanz der Schweiz im Verhältnis zur EU weiterhin sicherzustellen[103]. Unsinnige Bestimmungen der DSGVO wie etwa jene der Datenportabilität[104] wurden daher zum Glück (vorerst) nicht übernommen, und auch sonst zeigt der Vorentwurf eine gesunde Distanz zur Rechtsetzung in der EU. Denn manches, was diese in der DSGVO umgesetzt hat, ist nicht wirklich durchdacht, und im Bereich der Datenbearbeitung durch Private ist die Schweiz jedenfalls nicht verpflichtet, die Regelungen der DSGVO zu übernehmen. Daher soll bei der Auslegung des DSG richtigerweise nicht einfach die Auslegung der DSGVO herangezogen werden.

[Rz 135] Bei näherer Betrachtung zeigt der Vorentwurf allerdings gewichtige Schwächen, die eine deutliche Überarbeitung erfordern werden. Dies erstaunt etwas, zumal die Vorlage im Rahmen der Ämterkonsultation intensiv kommentiert worden ist, was wohl der Grund für die mehrmonatige Verzögerung des Vorentwurfs ist. Trotz allem macht er einen unausgegorenen, praxisfremden Eindruck. Es entsteht der Anschein, dass mehr Zeit darin investiert worden ist, dem EDÖB genug Spielraum zu verschaffen als die Frage der Praktikabilität und der Auswirkungen auf die Unternehmen zu prüfen, die die neuen Vorgaben umzusetzen haben werden.

[Rz 136] Einige der Mängel sind in diesem Beitrag angesprochen. In etlichen Punkten geht der Vorentwurf zudem ohne guten Grund über die Anforderungen der DSGVO hinaus, auch wenn dies womöglich lediglich Versehen sind oder mit dem heutigen DSG zusammenhängt[105]. Ein solches «Swiss Finish» sollte es aber so oder so nicht geben. Die Wirtschaft wird durch parallele Anwendbarkeit von DSG und DSGVO ohnehin schwer belastet werden. Es sollte ihr daher die Compliance nicht mit einem DSG, das teilweise über die DSGVO hinausgeht, noch schwerer und kostspieliger gemacht werden, als sie in diesem Bereich ohnehin sein wird. In diesen Bereichen wird die Vorlage bei der Erarbeitung der Botschaft hoffentlich zurückgebunden werden.

[Rz 137] Auch wenn ein «Swiss Finish» aus politischen Gründen kaum Chancen haben wird, kommt auf die Schweizer Wirtschaft mit dem revidierten DSG einiges an Mehrarbeit zu. Das betrifft sowohl die Datenschutz-Governance, also die betriebsinternen Massnahmen zur Sicherstellung des Datenschutzes, als auch die Interaktion mit den betroffenen Personen, namentlich was die neuen und stark erweiterten Informations- und Auskunftspflichten betrifft. Dies wird

103 Erläuterungen VE DSG, S. 5 und 32.

104 Art. 20 DSGVO.

105 Dass z.B. auch manuelles Profiling erfasst wird, dürfte darin begründet sein, dass der Begriff den heutigen Begriff des Persönlichkeitsprofils ablöst, das ebenfalls manuell oder automatisiert entstehen kann.

insbesondere auch KMU treffen, die bisher kaum in diesen Bereich investiert haben und die dafür erforderlichen Prozesse und Dokumentationen erst noch schaffen müssen.

[Rz 138] Ob die Revision die Datenschutz-Aufsicht und die Durchsetzung des DSG ebenfalls stärken werden, ist hingegen eine andere Frage. Auf dem Papier wird der EDÖB durch die Verfügungskompetenz und die ausgebauten Untersuchungsmöglichkeiten zweifellos mehr Rechte haben. Die neuen Verfahren werden sein Wirken allerdings auch sehr viel komplizierter machen und von ihm mehr Aufwand abverlangen. Da jedoch bezweifelt werden darf, dass ihm die Politik mehr Mittel in die Hand geben wird, kann es durchaus sein, dass die Datenschutzaufsicht im Ergebnis künftig weniger bewerkstelligen kann, als sie es heute tut. Ob das im Sinne des Erfinders ist, ist allerdings eine andere Frage. Vom revidierten DSG werden vor allem die Datenschutzspezialisten, Sicherheitsexperten und Anwälte profitieren – jedenfalls jene, die sich angesichts der Strafbestimmungen noch trauen, in diesem Minenfeld zu beraten.

David Rosenthal, Lic. iur., Konsulent, Homburger AG, Zürich, Lehrbeauftragter ETH Zürich und Universität Basel; der Autor dankt Barbara Kaiser und Djamila Batache für die Unterstützung und insbesondere die sehr fruchtbaren Diskussionen zum Begriff der «Ausdrücklichkeit» einer Einwilligung.