

Dokument	digma 2017 S. 44
Autor	David Vasella, Jacqueline Sievers
Titel	Der «Swiss Finish» im Vorentwurf des DSG
Seiten	44-49
Publikation	digma - Zeitschrift für Datenrecht und Informationssicherheit
Herausgeber	Bruno Baeriswyl, Beat Rudin, Bernhard M. Hämmerli, Rainer J. Schweizer, Günter Karjoth, David Vasella
ISSN	1424-9944
Verlag	Schulthess Juristische Medien AG

digma 2017 S. 44

Der «Swiss Finish» im Vorentwurf des DSG

Erhebliche Unterschiede zwischen dem Vorentwurf des DSG und der DSGVO in Bezug auf private Datenbearbeiter





David Vasella,
Dr. iur., Rechts-
anwalt, Walder
Wyss AG, Zürich
david.vasella@
walderwyss.com



Jacqueline Sievers,
Dr. iur., LL.M.,
Rechtsanwältin,
Walder Wyss AG,
Zürich
jacqueline.
sievers@
walderwyss.com

Die Datenschutzgesetzgebung wird gegenwärtig auf europäischer und auf schweizerischer Ebene revidiert. Der Vorentwurf des DSG soll dabei nicht nur die ERK-108 und die Schengen-Richtlinie umzusetzen, sondern auch die schweizerische Datenschutzgesetzgebung der DSGVO angleichen. Der Vorentwurf geht mit seinem «Swiss Finish» aber in vielen Punkten über das von der DSGVO Geforderte hinaus. Der Vorentwurf sieht gegenüber der DSGVO weitergehende Informationspflichten vor. Restriktiver sind auch die Regelungen zur Datenbekanntgabe ins Ausland und der Datenschutz-Folgenabschätzung. Der Vorentwurf bringt zudem strengere Meldepflichten für schweizerische Unternehmen und damit einen höheren Administrativaufwand für die Unternehmen wie auch den EDÖB mit sich. Er verpflichtet sodann vielfach (auch) Auftragsbearbeiter, wo die DSGVO nur den Verantwortlichen in die Pflicht nimmt. Bei bestimmten Verletzungen der Datenschutzgesetzgebung – und zwar selbst bei Fahrlässigkeit – werden empfindliche Bussen vorgesehen, die in erster Linie einzelne Personen treffen sollen. Die DSGVO sieht demgegenüber vor allem Unternehmenssanktionen vor. Dieser «Swiss Finish» führt zu Rechtsunsicherheiten, ist in der Sache ungerechtfertigt und für viele Unternehmen problematisch. Daraus resultiert eine Gefährdung der für einen effektiven Datenschutz notwendigen Akzeptanz und Durchsetzung der neuen Regelungen durch die datenbearbeitenden Unternehmen.

Die Revision des DSG strebt u.a. eine «Angleichung» an die DSGVO an. In vielen Punkten geht der Vorentwurf jedoch weit über das hinaus, was die DSGVO verlangt.



Die rasante technische Entwicklung und besonders die Digitalisierung vieler Lebensbereiche erschwert den Überblick über die Datenverwendung. Entsprechend wurden bei der Evaluation des DSG aus den Jahren 2010 und 2011 Vollzugsdefizite festgestellt¹. Die Datenschutzgesetzgebung wird heute demzufolge verbreitet als unzureichend erachtet.

Am 21. Dezember 2016 hat der Bundesrat deshalb mit etwas Verspätung den Vorentwurf eines neuen schweizerischen Datenschutzgesetzes (VE-DSG) veröffentlicht, zusammen mit dem Erläuternden Bericht und weiteren Unterlagen². Bis am 4. April 2017 läuft die Vernehmlassung.

Die Revision des DSG erfolgt nicht isoliert, sondern vor dem Hintergrund einer europäischen Gesetzgebungsrevision. Zunächst ist die Europaratskonvention Nr. 108 (ERK-108)³ zu nennen, deren Revision bis auf redaktionelle Änderungen abgeschlossen ist⁴. Ferner wird im Zuge der EU-Datenschutzreform die geltende Datenschutz-Richtlinie⁵ durch die Datenschutz-Grundverordnung (DSGVO)⁶ ersetzt. Schliesslich wird eine neue Datenschutz-Richtlinie für Polizei und Strafjustiz⁷ eingeführt (Schengen-Richtlinie).

Die ERK-108 steht für die Schweiz seit dem 1. Februar 1998 in Kraft. Die Schweiz wird auch ihre Revision umsetzen. Das Bundesamt für Justiz schlägt sodann vor, die Schengen-Richtlinie nicht nur dort im engen Bereich des Schengen-Acquis umzusetzen (nämlich begrenzt auf Datenbearbeitungen durch Behörden im sachlichen Geltungsbereich der Schengen-Richtlinie), sondern auch für die Datenbearbeitung Privater, soweit sich der Inhalt der Schengen-Richtlinie mit den Anforderungen der ERK-108 decken⁸. Und schliesslich soll das DSG der DSGVO « angeglichen » werden, um die heute von der Europäischen Kommission anerkannte Angemessenheit des schweizerischen Schutzniveaus nicht aufs Spiel zu setzen⁹.

Die DSGVO sieht schärfere Regelungen vor, die im Zuge der DSG-Revision im Sinne einer « Angleichung » an die DSGVO – und an die ERK-108 und die Schengen-Richtlinie – konzeptionell übernommen werden sollen. Der Vorentwurf geht jedoch in zahlreichen Punkten über das hinaus, was die DSGVO verlangt. Der Vorentwurf resultiert dadurch in einem « Swiss Finish », der zu Unklarheiten führt. Er ist aber auch deshalb abzulehnen, weil er Unternehmen im Anwendungsbereich des DSG

¹ Erläuternder Bericht, 8 mit Verweis auf Bericht des Bundesrates vom 9. Dezember 2011 über die Evaluation des Bundesgesetzes über den Datenschutz, BBl 2012 335, und Büro Vatter/Institut für Europarecht, Evaluation des Bundesgesetzes über den Datenschutz – Schlussbericht, Bern 11. März 2011 <<https://www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf>> (letztmals kontrolliert: 1.3.2017).

² <<http://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2016/2016-12-21.html>> (letztmals kontrolliert: 1.3.2017).

³ Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, für die Schweiz in Kraft getreten am 1. Februar 1998, SR 0.235.1.

⁴ Der Entwurf der revidierten ERK-108 kann hier eingesehen werden: <<https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2016/2016-12-21.html>> (Stand: 1.3.2017).

⁵ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, OJ L 281.

⁶ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, OJ L 119.

⁷ Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, OJ L 11/89.

⁸ Erläuternder Bericht, 27 f.

⁹ Erläuternder Bericht, 31 f.

benachteiligt gegenüber Unternehmen, welche nur die DSGVO (und die im Bereich des Datenschutzes weiterhin bestehenden Rechte der Mitgliedstaaten) zu befolgen haben. Besondere praktische Schwierigkeiten ergeben sich ferner für Unternehmen, die sowohl die DSGVO als auch das DSG anzuwenden haben. Das betrifft alle grösseren Unternehmen und Konzerne in der Schweiz¹⁰. Die schweizerische Datenschutzgesetzgebung darf Unternehmen nicht zur Einhaltung eines doppelten Standards zwingen – ihr Compliance-Aufwand ist auch ohne solche Hürden hoch genug.

Übersicht über den Vorentwurf

Bevor im Einzelnen auf den «Swiss Finish» eingegangen wird, sollen die wichtigsten Neuerungen der Revision zusammengefasst werden:

■ **Systematische Änderungen:** Der Aufbau des DSG wird in einigen Punkten angepasst. Das DSG erhält einen neuen 3. Abschnitt «Pflichten des Verantwortlichen und des Auftragsbearbeiters», der der Bestimmungen zusammenfasst, die sich im geltenden DSG im 2. Abschnitt «Allgemeine Datenschutzbestimmungen» und im 3. Abschnitt «Bearbeiten von Personendaten durch private Personen» finden. Neu ist ferner der eigens für das Auskunftsrecht geschaffene 4. Abschnitt «Rechte der betroffenen Person».

digma 2017 S. 44, 45

Ebenfalls neu ist der 9. Abschnitt «Abschluss von Staatsverträgen».

■ **Terminologische Anpassungen:** Viele Änderungen scheinen nur sprachlicher Natur zu sein, wobei nicht immer klar ist, was dadurch gewonnen wird und ob die entsprechenden Änderungen nicht doch auch materiellen Gehalt haben.

■ **Inhaltliche Änderungen bestehender Institute:** An vielen Stellen werden im geltenden DSG bestehende Institute inhaltlich geändert. Einige Beispiele: die Beschränkung des Anwendungsbereichs auf natürliche Personen (Art. 3 lit. b VE-DSG), die (erhebliche) Ausweitung der Informationspflicht (Art. 13 VE-DSG) und des Auskunftsrechts (Art. 20 VE-DSG) oder die Meldepflicht an den EDÖB bei Auslandübermittlungen (Art. 6 Abs. 2 VE-DSG).

■ **Neuschöpfungen:** Der VE-DSG enthält Rechtsinstitute, die dem geltenden schweizerischen Datenschutzrecht zumindest als eigenständiger Regelungsgegenstand unbekannt sind, so etwa die Empfehlungen der guten Praxis (Art. 9 VE-DSG), die Regelung der Daten Verstorbener (Art. 12 VE-DSG), die Regelung der automatisierten Einzelfallentscheidung (Art. 15 VE-DSG), die Datenschutz-Folgenabschätzung (Art. 16 VE-DSG), bestimmte Meldepflichten bei Datenschutzverstössen (Art. 17 VE-DSG), Datenschutz durch Technik und Voreinstellungen (Art. 18 VE-DSG), die Dokumentationspflicht (Art. 19 VE-DSG) und die Weitermeldungspflicht von Berichtigungen, Löschungen, Vernichtungen und Datenschutzverletzungen an die früheren Empfänger der betroffenen Daten (Art. 19 lit. b VE-DSG).

■ **Durchsetzungsbestimmungen:** Der VE-DSG stärkt die Stellung des EDÖB u.a. durch die Verfügungskompetenz, die ihm heute fehlt (vgl. Art. 29 DSG mit Art. 41 ff. VE-DSG).

■ **Der VE-DSG sieht einschneidende Bussen für vorsätzliche oder fahrlässige Verletzungen bestimmter Pflichten vor, leider primär zulasten der für den Verstoss verantwortlichen natürlichen Personen (Art. 50 VE-DSG).**

In der Sache überschüssende Regelungen

Zu weit gehende Informationspflichten

¹⁰ Dazu Bühlmann Lukas/Reinle Michael, Extraterritoriale Wirkung der DSGVO, digma 2017, 8 ff. (in diesem Heft).

Wie die DSGVO hängt auch der Vorentwurf dem Glauben an, der Datenschutz lasse sich durch noch mehr Information verbessern. Das auf diese Weise tatsächlich mehr Transparenz geschaffen wird, widerspricht allerdings der allgemeinen Lebenserfahrung¹¹. Noch längere AGB und Datenschutzerklärungen dürfte betroffene Personen im Gegenteil erst recht davon abhalten, diese zu lesen. In einzelnen Punkten gehen die Informationspflichten gemäss dem Vorentwurf dabei sogar über das hinaus, was die DSGVO fordert:

Trifft der Verantwortliche eine «Entscheidung» – was immer das heisst –, so muss er im Rahmen der Auskunftspflicht über die Tatsache der Entscheidung, ihre Ergebnis, ihr Zustandekommen und ihre Auswirkungen informieren (Art. 20 Abs. 3 VE-DSG). Die DSGVO sieht solch eine Pflicht nur für den Fall automatisierter Entscheidungen vor. Auch die revidierte ERK-108 sieht eine weniger weit gehende Informationspflicht vor (Art. 8 Abs. 1 lit. c ERK-108). Hinter der – strafrechtlich sanktionierten – Informationspflicht des VE-DSG versteckt

Die schweizerische Datenschutzgesetzgebung darf Unternehmen nicht zur Einhaltung eines doppelten Standards zwingen.

sich das konsumentenschützerische Anliegen einer allgemeinen Beratungspflicht der Datenbearbeiter, wie sie höchstens – wenn überhaupt – im Rahmen einer (im Übrigen nicht datenschutzrechtlich begründbaren) Kontrahierungspflicht eine Berechtigung hätte. Der Zweck der Auskunftspflicht sollte sich darauf beschränken, den betroffenen Personen dort «menschliches Gehör»¹² zu verschaffen, wo

digma 2017 S. 44, 46

eine automatisierte Entscheidung tatsächlich eine Persönlichkeitsverletzung mit sich bringt.

Ebenfalls ohne Vorbild in der DSGVO ist die Pflicht, im Fall einer Auftragsbearbeitung aktiv – nicht nur auf Anfrage – über Identität und Kontaktdaten des Auftragsbearbeiters und die betroffenen Daten zu informieren (Art. 13 Abs. 4 VE-DSG). Was damit erreicht werden soll, geht auch aus dem Erläuternden Bericht nicht hervor. Es liegt auf der Hand, dass diese Pflicht für viele Unternehmen, die eine Vielzahl von Auftragsbearbeitern beschäftigen, kaum zu erfüllen ist.

Ein Bereich, bei dem Abweichungen des VE-DSG von der DSGVO festzustellen sind, ist derjenige der Meldepflichten gegenüber dem EDÖB.

Ebenfalls überschüssend ist die Regelung des «Profiling» im Vorentwurf, eines neuen, aber auch in der revidierten ERK-108 verankerten Konzepts, das die Persönlichkeitsprofile ersetzt. Die Legaldefinition des Profilings im Vorentwurf (Art. 3 lit. f VE-DSG) umfasst «jede¹³ Auswertung von Daten und Personendaten (...), um persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen», also auch die manuelle Auswertung. Die DSGVO erfasst als Profiling nur die *automatisierte* Verarbeitung (Art. 4 Nr. 4). Die Regelung des Vorentwurfs ist deshalb schädlich, weil Profiling immer eine Persönlichkeitsverletzung darstellt (Art. 23 Abs. 2 lit. d VE-DSG); eine Rechtsfolge, die höchstens bei der automatisierten Profilierung gerechtfertigt ist.

Zu restriktive Regelung der Bekanntgabe in Länder ohne angemessenen Schutz

Auch bei der Bekanntgabe von Personendaten ins Ausland enthält der VE-DSG Regelungen, die inhaltlich zu Unrecht vom Vorbild der DSGVO abweichen. Das betrifft zunächst die Rechtfertigung der Bekanntgabe in ein Land ohne angemessenen Schutz. Eine Bekanntgabe ist nach dem Vorentwurf u.a. dann erlaubt, wenn sie unmittelbar mit dem Abschluss oder der Abwicklung eines Vertrags mit der betroffenen Person zusammenhängt (Art. 6 Abs. 1 lit. b VE-DSG). Die DSGVO erlaubt

¹¹ Regulierungsfolgenabschätzung (RFA) zur Revision des eidg. Datenschutzgesetzes (DSG). Schlussbericht vom 11. Juli 2016, 28.

¹² So Rosenthal, Rz. 65.

¹³ Hervorhebung durch die Verfasser.



die Bekanntgabe darüber hinaus auch zur Erfüllung eines nicht mit, aber im Interesse der betroffenen Person geschlossenen oder zu schliessenden Vertrags (Art. 49 Abs. 1 lit. c DSGVO). Das ist zweifellos sinnvoll, und es wäre umso wichtiger, wenn private Interessen weiterhin nicht als Rechtfertigung der Bekanntgabe in Betracht kommen. Im Vorentwurf ist das noch so vorgesehen, obwohl die DSGVO die Berufung auf überwiegende private Interessen des Verantwortlichen vorsieht (Art. 49 Abs. 1 DSGVO).

Ferner fällt auf, dass gemäss dem VE-DSG die Ausnahme der Wahrung von Rechtsansprüchen nur greift, wenn ihre Feststellung, Ausübung oder Durchsetzung vor Gericht oder einer Verwaltungsbehörde erfolgen soll (Art. 6 Abs. 1 lit. c Ziff. 2 VE-DSG). Die DSGVO kennt diese Einschränkung nicht (Art. 49 Abs. 1 lit. f DSGVO).

Datenschutz-Folgenabschätzung: Zu niedrige Schwelle

Vor einer Datenbearbeitung ist jeweils zu entscheiden, ob ihr Risikoprofil eine formelle Folgeabschätzung verlangt. Das Institut der Datenschutz-Folgenabschätzung ist dem schweizerischen Recht zumindest als Idee bereits bekannt, und es kann sich de lege lata ggf. auf Art. 7 DSG stützen. Die jetzt in Art. 16 VE-DSG vorgeschlagene Regelung ist insofern nicht unbedingt notwendig. Vor allem aber geht sie über das hinaus, was die europäischen Vorgaben verlangen: Art. 35 Abs. 1 DSGVO verlangt eine formelle Folgeabschätzung nur dann, wenn das Risiko voraussichtlich «hoch» ist. Art. 16 Abs. 1 VE-DSG lässt dagegen bereits ein voraussichtlich «erhöhtes» Risiko genügen. Das ist ein wesentlicher Unterschied, der – gerade mit Blick auf das Sanktionsrisiko – grosse Unklarheit mit sich bringt; denn «erhöht» ist ein Komparativ, dessen Bezugspunkt offen ist: Erhöht im Vergleich zum Normalfall der betreffenden Bearbeitung? Im Verhältnis zum gesellschaftlich akzeptierten Risiko? Im Vergleich zu den vom Verantwortlichen üblicherweise eingegangenen Risiken? Richtigerweise müsste auch der Vorentwurf von einem «hohen» Risiko sprechen.

Unnötige und schädliche Meldepflichten gegenüber dem EDÖB

Ein Bereich, bei dem mehrere Abweichungen des Vorentwurfs von der DSGVO festzustellen sind, ist derjenige der Meldepflichten gegenüber dem EDÖB. Beispielsweise führt der VE-DSG bei der Bekanntgabe von Personendaten in Länder ohne angemessenen Schutz die heute nach Art. 6 Abs. 3 DSG bestehende Pflicht fort, den EDÖB über die Verwendung anerkannter «Garantien» – insbesondere von Datenschutzverträgen und -klauseln – in Kenntnis zu setzen (Art. 5 Abs. 6 VE-DSG). Eine solche Pflicht sieht die DSGVO nicht vor. Ebenso müssen dem EDÖB sämtliche Bekanntgaben von Personendaten ins Ausland gemeldet wer-

digma 2017 S. 44, 47

den, wenn der Empfängerstaat nicht über ein angemessenes Schutzniveau verfügt (was in Zukunft der Bundesrat rechtsverbindlich festlegt; Art. 5 Abs. 2 VE-DSG) und sofern die Bekanntgabe zur Vertragsabwicklung erfolgt, zur Wahrung eines überwiegenden öffentlichen Interesses oder zur Wahrung von Rechtsansprüchen vor Gericht oder einer Verwaltungsbehörde oder zum Schutz des Lebens oder der körperlichen Unversehrtheit (Art. 6 Abs. 2 Vorentwurf). Die DSGVO verlangt eine entsprechende Meldung nur bei der eingeschränkt zulässigen Bekanntgabe zur Wahrung zwingender eigener Interessen des Verantwortlichen (Art. 49 Abs. 1 DSGVO; ein Erlaubnistatbestand, der im Vorentwurf wie im geltenden DSG zu Unrecht fehlt).

Eine weitere überschüssige Meldepflicht findet sich bei der Datenschutz-Folgenabschätzung. Nach Art. 16 Abs. 3 VE-DSG sind dem EDÖB *sämtliche* Folgenabschätzungen zu melden, und zwar auch dann, wenn dabei – bspw. aufgrund ergriffener Sicherheitsmassnahmen – kein oder nur ein niedriges Risiko festgestellt wird. Die DSGVO verlangt die Konsultation der Aufsichtsbehörde demgegenüber nur dann, wenn auch im Ergebnis ein hohes Risiko verbleibt (Art. 36 Abs. 1 DSGVO). Zu lange ist ferner die Frist von drei Monaten für Einwände des EDÖB, die sich durch Einforderung weiterer Informationen durch den EDÖB auf unbestimmte Zeit verlängern kann (Art. 16 Abs. 4 VE-DSG). Das behindert Unternehmen in ihrer



Projektplanung. Realistischer ist die DSGVO, die den Aufsichtsbehörden lediglich acht Wochen (mit einer einmaligen Verlängerungsmöglichkeit von sechs Wochen) einräumt (Art. 36 Abs. 2 DSGVO).

Auch die Meldepflicht gegenüber dem EDÖB bei Datenschutzverletzungen nach Art. 17 Abs. 1 VE-DSG, ein Anwendungsfall der «Breach Notification», geht wesentlich weiter als ihr Gegenstück in der DSGVO. Nach deren Art. 33 Abs. 1 DSGVO sind ggf. «Verletzungen des Schutzes» von Personendaten zu melden, nach der Legaldefinition von Art. 4 Ziff. 12 DSGVO also Verletzungen der Datensicherheit. Nach Art. 17 Abs. 1 VE-DSG sind dagegen unbefugte Datenbearbeitungen zu melden, also nicht nur sicherheitsrelevante Vorfälle, sondern überhaupt *jede* Verletzung, die voraussichtlich zu einem Risiko führt. Das umfasst u.a. auch unverhältnismässige Bearbeitungen, bspw. eine zu späte Löschung. Eine so weit gehende Meldepflicht ist unverhältnismässig und nutzlos, und sie könnte den Grundsatz «nemo tenetur» verletzen, wonach niemand verpflichtet werden darf, sich selbst zu belasten.

All diese Meldepflichten sind nicht geeignet, zum Datenschutz beizutragen. Es liegt auf der Hand, dass der EDÖB mit der Zahl der Meldungen völlig überfordert wäre (zumal der Erläuterungsbericht davon ausgeht, der EDÖB brauche nicht mehr als eine oder zwei zusätzliche Stellen). Im Gegenteil: Übertriebene Meldepflichten wirken kontraproduktiv, weil sie einen Anreiz setzen, die meldepflichtigen Sachverhalte zu umgehen. Das mag bei der Übermittlung ins Ausland zwar schwierig sein. Bei der Folgenabschätzung ist es aber wahrscheinlich, dass Unternehmen in Zweifelsfällen wenig Lust verspüren werden, eine Abschätzung durchzuführen, wenn sie selbst im Falle eines Negativresultat nicht von der Meldung an den EDÖB absehen könnten.

Insbesondere bei den Meldepflichten sollte nicht ausser Acht gelassen werden, dass Unternehmen ein in Art. 13 BV und Art. 28 und 53 ZGB sowie in diversen Vorschriften zum Geheimnisschutz verbrieftes Recht auf Privatsphäre haben, auch wenn das DSG Angaben zu juristischen Personen nicht mehr schützt.

Übertriebene Meldepflichten wirken kontraproduktiv, weil sie einen Anreiz setzen, die meldepflichtigen Sachverhalte zu umgehen.

Überschiessende Pflichten des Auftragsbearbeiters

Ein weiterer Komplex mit einem «Swiss Finish» betrifft die Pflichten der Auftragsbearbeiter. Ihnen obliegt nicht nur eine Mitwirkung bei der datenschutzrechtlichen Compliance der Auftraggeber. Sie sind nach dem Vorentwurf vielmehr Adressaten einer Reihe von Pflichten, die von der Sache her den «Controller» treffen sollten. Das betrifft zum einen die Pflicht zur Durchführung der Datenschutz-Folgenabschätzung, die nach Art. 17 Abs. 1 VE-DSG den Verantwortlichen «oder den Auftraggeber» trifft. Zwar lässt sich diese Bestimmung auch so lesen, dass die Pflicht stets den Verantwortlichen betrifft, sofern sich dieser nicht mit dem Auftragsbearbeiter auf eine andere Regelung verständigt; eine Präzisierung wäre aber notwendig. In der Sache kann die Folgenabschätzung nicht Aufgabe des Auftragsbearbeiters sein, der oftmals nicht über alle dafür erforderlichen Angaben verfügen wird. Die DSGVO nimmt dafür denn auch (nur) den Verantwortlichen in die Pflicht (Art. 35 Abs. 1 ff. DSGVO).

In ähnlicher Weise verpflichtet der VE-DSG nicht nur den Verantwortlichen, sondern auch den Auftragsbearbeiter auf die Massnahmen

digma 2017 S. 44, 48

zum Datenschutz durch Technik und auf geeignete Voreinstellungen (Art. 18 VE-DSG), anders als die DSGVO (Art. 25 Abs. 1 DSGVO). Ein weiteres Beispiel ist die Pflicht, bei der Berichtigung von Daten und in einigen weiteren Fällen die Empfänger der betreffenden Daten zu informieren (Art. 19 lit. b VE-DSG; Art. 19 DSGVO). In all diesen Fällen sollte der Verantwortliche Träger der entsprechenden Pflicht sein. Die Verpflichtung des Auftragsbearbeiters erfolgt dabei in ausreichendem Mass über die allgemeinen Bearbeitungsgrundsätze und die vertragliche Vereinbarung, die der Verantwortliche im eigenen Interesse schliessen wird (und der Bundesrat kann eine



Mitwirkungspflicht gestützt auf Art. 7 Abs. 2 VE-DSG und nach dem Vorbild von Art. 28 Abs. 3 DSGVO ausdrücklich vorschreiben, sollte sich dies als notwendig erweisen).

Der wesentliche Treiber für die Revision ist die technische Entwicklung, die die Einhaltung des Datenschutzes erschwert, und ein gewisses Vollzugsdefizit.

Sanktionsregime

Viel zu reden gibt die vorgeschlagene Sanktionsregelung. Die vorsätzliche Verletzung bestimmter Pflichten, insbesondere der oben dargestellten Informations-, Melde- und Mitwirkungspflichten (Art. 50 VE-DSG) und von bestimmten Pflichten eher formeller Natur (Art. 51 VE-DSG), wird mit Busse bis CHF 500 000 bedroht. Für die fahrlässige Begehung geht der Bussenrahmen bis CHF 250 000. Die Strafe trifft dabei primär die natürlichen Personen; die Unternehmen selbst wären nur subsidiär strafbar, nämlich bei Bussen von höchstens CHF 100 000, wenn die Ermittlung der strafbaren Personen unverhältnismässig aufwendig wäre (Art. 53 VE-DSG). Verwaltungsbussen zulasten der Unternehmen als primäre Sanktionsmittel wurden dagegen verworfen.

Diese Regelung ist nicht nur anders als das in Art. 83 DSGVO vorgesehene Sanktionsregime, das Unternehmensstrafen von bis zu EUR 20 Mio. oder 4% des weltweiten Jahresumsatzes vorsieht (allerdings unter Vorbehalt abweichender Regelungen der Mitgliedstaaten; Art. 84 DSGVO). Sie wirft auch in der Sache einige Fragen auf:

Sind die mit Strafe bedrohten Bestimmungen so präzise formuliert, dass sie zum Straftatbestand erklärt werden können? Diese Frage wird bei vielen, wenn nicht den meisten dieser Bestimmungen eindeutig verneint werden müssen – ein Beispiel ist die Datenschutz-Folgenabschätzung, deren Unterlassung strafbar werden soll, und zwar selbst bei Fahrlässigkeit, obwohl völlig unklar bleibt, wann genau eine Pflicht zu ihrer Durchführung besteht.

Ist es vertretbar, bei Sanktionen primär auf natürliche Personen zu zielen? Dabei ist zu bedenken, dass Datenschutzverletzungen fast immer aufgrund der grossen Unbestimmtheit datenschutzrechtlicher Regelungen begangen werden dürften, und in manchen Fällen sicher auch aufgrund von Schwächen der unternehmensinternen Compliance. Sanktionen gegen einzelne Personen hätten aber nur dann eine Berechtigung, wenn die Ursache der sanktionierten Verletzungen nicht im weiteren Unternehmenskontext zu suchen wäre, sondern in individuellen Entscheidungen einzelner Personen. Das wird beim Datenschutzrecht kaum je der Fall sein. Der Datenschutz kann zudem kein Interesse daran haben, die im Unternehmen für seine Einhaltung besorgten Personen zu kriminalisieren. Die Folge wäre nicht eine Verbesserung des Schutzes betroffener Personen, sondern eine Lähmung der Unternehmen durch immer grösseren bürokratischen Dokumentationsaufwand.

Ist die Sanktionierung natürlicher Personen zur Abschreckung erforderlich? Diese Frage ist klar mit Nein zu beantworten. Die DSGVO ist auf wirksame, abschreckende und verhältnismässige Sanktionen verpflichtet, sieht aber dennoch Unternehmensbussen vor. Die Erfahrung der letzten Monate zeigt ferner, dass die Erwartung hoher Unternehmensbussen genügt, den Datenschutz in Leitungsorganen auf die Agenda zu setzen.

Abschliessende Überlegungen

Der wesentliche Treiber für die Revision des Datenschutzes auf europäischer sowie schweizerischer Ebene ist die technische Entwicklung, die die Einhaltung des Datenschutzes erschwert, und ein gewisses Vollzugsdefizit. Die Lösung dieses Problems liegt aber nicht in der Schaffung einer Compliance-Bürokratie, sondern in der Verbesserung der Akzeptanz des Datenschutzrechts durch die Unternehmen. Die Voraussetzungen dafür sind gut, denn die jüngsten Erfahrungen zeigen, dass Unternehmen und die mit datenschutzrechtlichen Auf-



gaben betrauten Personen durchaus einsehen, dass dem Datenschutz in der heutigen Zeit ein höherer Stellenwert einzuräumen ist. Dafür ist es aber notwendig, dass der schweizerische Gesetzgeber das Augenmass nicht verliert.

Literatur

- Aufgrund der Aktualität der Thematik hat sich die Lehre noch wenig zum VE-DSG geäußert. Hinzuweisen ist aber auf David Rosenthal, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 2017 20. Februar 2017.