Der risikobasierte Ansatz im neuen EU- und Schweizer Datenschutzrecht

Erleichterung und Umsetzungsspielraum für den Verantwortlichen

Fürsprecherin Clara-Ann Gordon, LL.M. (Zürich)

Schweizer Unternehmen haben, bedingt durch das neue EU- und Schweizer Datenschutzrecht, Handlungsbedarf. Sie müssen ihre Datenbearbeitungsprozesse und die entsprechenden Verträge und Datenschutzerklärungen anpassen, ansonsten ihnen hohe Bussen drohen. Es wird jedoch kein Schweizer Unternehmen in jeder Hinsicht alle neuen Bestimmungen einhalten können. Das neue Datenschutzrecht verfolgt und verlangt einen risikobasierten Ansatz bei der Umsetzung der neuen Bestimmungen. Dieser hilft dabei, ein vernünftiges Aufwand-Nutzen-Verhältnis herzustellen. Im Nachfolgenden wird dieser Ansatz näher analysiert.

Im Mai 2018 tritt die neue Datenschutzgrundverordnung (DSGVO) der EU in Kraft. Die schweizerische Datenschutzgesetzgebung befindet sich in Revision, wobei Kompatibilität zwischen DSG und DSGVO angestrebt wird. Die Autorin zeigt die Bedeutung der DSGVO und deren Auswirkungen auf die in der Schweiz mit Bezug zur EU agierenden Unternehmen auf. Sie analysiert Massnahmen zur Erfüllung der neuen Pflichten, namentlich den im Vordergrund stehenden «risikobasierten Ansatz», der den Verantwortlichen Spielraum in der Umsetzung der neuen Bestimmungen ermöglicht und bei der Revision des Datenschutzgesetzes ebenfalls eine zentrale Rolle spielt. Zi.

Le nouveau Règlement européen sur la protection des données (RGPD) entrera en vigueur en mai 2018. La législation suisse en matière de protection des données est elle-même en cours de révision et le législateur tend à assurer la compatibilité entre la LPD et le RGPD. L'auteure souligne l'importance du RGPD et son impact sur les entreprises sises en Suisse qui sont en relation avec l'Union Européenne. Elle analyse les mesures permettant de satisfaire aux nouvelles obligations, en particulier «l'approche basée sur le risque», qui offre aux responsables une marge de manœuvre dans la mise en œuvre des nouvelles dispositions et qui joue également un rôle central dans la révision de la Loi sur la protection des données. P.P.

I Einleitung

A. Direkte Anwendbarkeit der DSGVO auf Schweizer Unternehmen

Schweizer Unternehmen, die eine Niederlassung in der EU haben, unterstehen bei ihren Datenbearbeitungen der Datenschutzgrundverordnung («DSGVO»)[1]. Es fallen aber auch Schweizer Unternehmen, die lediglich Waren und Dienstleistungen an betroffene Personen in der EU anbieten, unter die Bestimmungen der DSGVO, wenn sie in diesem Zusammenhang deren Daten bearbeiten[2]. Dasselbe gilt für diejenigen Datenbearbeiter, die das Verhalten von Personen in der EU beispielsweise mittels des Einsatzes von Cookies beobachten[3].

In diesem Zusammenhang wird auch von dem sogenannten «Marktortprinzip»[4] gesprochen, welches zu einer

1 Art. 3 Abs. 1 DSGVO.
2 Art. 3 Abs. 2 lit. a DSGVO.
3 Art. 3 Abs. 2 lit. b DSGVO.
4 *Bruno Baeriswyl*, in: Ueli Kieser/Kurt Pärli/Ursula Uttinger (Hrsg.), Datenschutztagung 2017, Baustelle Datenschutz – Observation als Brennpunkt, Datenschutzreformen in Europa, 7.

direkten Anwendbarkeit der DSGVO auf sehr viele Schweizer Unternehmen führt[5].

B. Totalrevision DSG – Angleichung an die Bestimmungen der DSGVO

Am 12. Dezember 2016 hat der Bundesrat einen Vorentwurf zur Totalrevision des DSG in die Vernehmlassung gegeben. Die Vernehmlassungsfrist lief am 4. April 2017 ab.

Der Vorentwurf berücksichtigte die europäischen Reformen, ohne dass aber eine klare Linie erkennbar war[6]. Der Vorentwurf wurde von der Schweizer Wirtschaft stark kritisiert, da er sich wohl zu wenig an den Bestimmungen der DSGVO angelehnt hatte und zu viele sogenannte «Swiss Finishes»[7] beinhaltete.

Als nicht EU-Land geniesst die Schweiz bei der Revision ihrer Datenschutzgesetzgebung zwar grosse Souveränität und müsste die Bestimmungen der DSGVO nicht im eigenen Datenschutzrecht umsetzen. Dennoch gilt das Inkrafttreten der DSGVO im Mai 2018 als Schrittmacher, und in der Kritik am Vernehmlassungsvorschlag des Bundesrates stehen die Kompatibilität des DSG zur DSGVO im Vordergrund. Bei der Bedeutung der Auswirkungen der DSGVO auf die Schweiz steht vor allem die «Angemessenheitsentscheidung» der EU-Kommission im Vordergrund. Falls das Schweizer DSG nicht mehr als «angemessen» im Vergleich zur EU gilt, wäre der heute einfache grenzüberschreitende Datenverkehr gefährdet. Zudem gebietet sich aus Sicht der Schweizer Wirtschaft eine Anpassung an die DSGVO, weil gestützt auf das sogenannte «Marktortprinzip» die DSGVO eh direkte Anwendung findet und das DSG deshalb analog zur DSGVO gestaltet werden sollte, um eine Zweigleisigkeit zu vermeiden[8].

Die Kritik wurde (teilweise) berücksichtigt, und am 15. September 2017 wurden der überarbeitete Gesetzesentwurf und die Botschaft veröffentlicht. Der E-DSG lehnt sich nun näher an die Bestimmungen der DSGVO an, ist wirtschaftsfreundlicher und einige (aber lange nicht alle) «Swiss Finishes» wurden entfernt.

Gemäss Mitteilung der staatspolitischen Kommission des Nationalrats vom 12. Januar 2018 wurde beschlossen, die Revision des DSG in zwei Teilen zu behandeln: (1) Anpassungen an Schengen und (2) Totalrevision des DSG. Dadurch können die Anpassungen an Schengen mit Blick auf die Umsetzungsfrist vorab beraten werden. Die Totalrevision des DSG könne sodann «ohne Zeitdruck» angegangen werden[9]. Offen bleibt nun, welche Verzögerungen sich daraus für das Inkrafttreten des revidierten DSG ergeben, welches ursprünglich im Sommer 2018 erwartet wurde[10].

C. Handlungsbedarf der Schweizer Unternehmen

Schweizer Unternehmen bzw. Verantwortliche[11] werden beide, die neuen EU- und Schweizer, Datenschutzbestimmungen einhalten müssen. Diese führen viele neue Rechte für die Datensubjekte bzw. betroffenen Personen[12], aber auch zahlreiche, neue Pflichten für die Verantwortlichen ein. Werden diese neuen Bestimmungen nicht implementiert und eingehalten, drohen neu sehr hohe Bussen. Unter der DSGVO sind es 4% des weltweiten Umsatzes oder € 20 Millionen, je nachdem, welcher Betrag höher ist, oder für geringfügigere Verletzungen 2% des weltweiten Umsatzes oder € 10 Millionen, je nachdem, welcher Betrag höher ist[13]. Unter dem E-DSG sind die Bussen zwar mit CHF 250 000 tiefer, sie werden jedoch der (leitenden) privaten Person auferlegt und nicht dem Unternehmen[14]. Im Blickwinkel dieser Bussen rüsten sich nun die Schweizer Unternehmen und Datenbearbeiter im Hinblick auf die Anwendbarkeit der DSGVO ab dem 25. Mai 2018 auf.

---

5 <https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html>: Die Datenschutz-Grundverordnung der EU und ihre Auswirkungen auf die Schweiz.

6 *Baeriswyl* (Fn. 4) 12.

7 Dies sind Bestimmungen im E-DSG, die über die Bestimmungen der DSGVO hinausgehen und (unnötigerweise) verschärfte Pflichten den Schweizer Datenbearbeitern auferlegen.

8 *Baeriswyl* (Fn. 4) 3 und 4.

9 <https://www.parlament.ch/press-releases/Pages/mm-spk-n-2018-01-12.aspx>.

10 <https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news/kommission-des-nationalrats-beschliesst-etappierung-der-dsg-revi.html>.

11 Gemäss der Terminologie der DSGVO und des E-DSG ist dies die private Person, die allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet.

12 Art. 4 lit. a E-DSG.

13 Art. 83 DSGVO.

14 Art. 54 E-DSG.

D. Breiter Pflichtenkatalog – ist die Einhaltung überhaupt möglich?

Die DSGVO und der E-DSG enthalten einen breiten Pflichtenkatalog[15] für den Verantwortlichen, den dieser erfüllen muss, um datenschutzkonform zu handeln. Angesichts der Fülle dieser neuen Pflichten fragen sich viele Unternehmen, ob sie diese überhaupt erfüllen können. Gerade für KMUs ist die vollständige Umsetzung oft fast nicht möglich.

Um dies etwas abzufedern, haben die DSGVO und auch der E-DSG ein Kriterium eingeführt, wonach der Verantwortliche sich bei der Erfüllung dieser Pflichten an das Risiko für die Rechte und Freiheiten der Betroffenen richten soll. Dies ist der sognannte risikobasierte Ansatz, welcher dem Verantwortlichen eine gewisse Erleichterung und einen Umsetzungsspielraum bringen soll. Nachfolgend wird dieser Ansatz näher untersucht.

II. Der risikobasierte Ansatz in der DSGVO

A. Ausdifferenzierung der datenschutzrechtlichen Pflichten des Verantwortlichen

Die DSGVO geht grundsätzlich von einem risikobasierten Ansatz aus, und dies bedeutet, dass die Pflichten des Verantwortlichen stets unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu beurteilen sind[16].

Angesichts des sehr weiten Anwendungsbereichs der DSGVO und der sehr weitreichenden Massnahmen, die der Verantwortliche vorzunehmen hat, führt der risikobasierte Ansatz zu einer Ausdifferenzierung der datenschutzrechtlichen Pflichten des Verantwortlichen. Dem liegt die Idee zugrunde, dass das datenschutzrechtliche Instrumentarium nur in Abhängigkeit vom Risiko, das von der Datenverarbeitung im Einzelfall für den Betroffenen ausgeht, angewendet werden sollte, um so ein vernünftiges Aufwand-Nutzen-Verhältnis herstellen zu können. Mit strukturierten Risikoprüfungen können die Komplexität handhabbar gemacht und Abwägungsentscheidungen nachvollziehbar getroffen werden[17, 18]. Ein solches risikobasiertes Vorgehen ist bei sogenannten Compliance Management Systemen (CMS) schon heute üblich und zweckmässig.

B. Definition von Risiko in der DSGVO

Im allgemeinen Sprachgebrauch wird der Begriff «Risiko» als ein Umstand beschrieben, der gefährliche oder schädliche Folgen haben kann. In der «ISO 31 000 – Risikomanagement» wird Risiko als «Auswirkung von Unsicherheit auf Ziele» definiert[19].

Die DSGVO enthält zum Risikobegriff im datenschutzrechtlichen Kontext keine spezifische Definition.

C. Welches sind die Risikobereiche?

Der Risikobegriff taucht trotz fehlender Definition dennoch an zahlreichen Stellen in der DSGVO auf. Gemäss Art. 24 in Verbindung mit Art. 32 DSGVO muss bei der Auswahl der technischen und organisatorischen Massnahmen die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt werden. Ferner ist gemäss Art. 33 DSGVO bei der Frage, ob der Verantwortliche bei einer Datenschutzverletzung eine Meldung an die Aufsichtsbehörde abgeben muss, entscheidend, ob die Verletzung zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die DSGVO ordnet zudem die Durchführung von bestimmten, besonderen Massnahmen bei einem «voraussichtlich hohen Risiko» für die persönlichen Rechte und Freiheiten natürlicher Personen an. Beispiele dafür sind die Datenschutz-Folgenabschätzung gemäss Art. 35 DSGVO und die Benachrichtigung des Betroffenen bei Datenschutzverletzungen gemäss Art. 34 DSGVO.

Schliesslich enthalten die Erwägungsgründe einige Beispiele für Datenschutzrisiken. Mögliche Datenschutzrisiken, die aus einer Datenverarbeitung resultieren und zu einem physischen, materiellen oder immateriellen Scha-

[15] Siehe z.B. <https://www.bj.admin.ch/bj/de/home/aktuell/news/2016/ref_2016-12-21.html und https://www.lda.bayern.de/de/datenschutz_eu.html>.

[16] Art. 24 DSGVO.

[17] *Maximilian von Grafenstein:* in Gierschmann/Schlender/Stenzel/Veil (Hrsg.), Kommentar zur Datenschutzgrundverordnung, Art. 2 N 6.

[18] *Winfried Veil:* in Gierschmann/Schlender/Stenzel/Veil (Hrsg.), Kommentar zur Datenschutzgrundverordnung, Art. 24 N 78.

[19] «Effect of uncertainty on objectives», ISO 31000:2009, Risk Management – Principles and guidelines; ISO Guide 73:2009, Risk Management – Vocabulary.

den führen können, sind gemäss Erwägungsgrund 75[20] beispielsweise: Diskriminierung, Identitätsdiebstahl oder finanzieller Verlust. Als Beispiele für Verarbeitungen mit hohem Risiko werden in Erwägungsgrund 89[21] u.a. Verarbeitungen unter Einsatz neuer Technologien und neuartige Verarbeitungen ohne bisherige Durchführung einer Datenschutzfolgeabschätzung genannt.

D. Wie wird der risikobasierte Ansatz in der Praxis angewendet?

Der risikobasierte Ansatz der DSGVO ist für den Verantwortlichen mit einem nicht unerheblichen Aufwand verbunden. Bisher gibt es noch keine Leitlinien zum Risikomanagement von den Aufsichtsbehörden. In der Praxis empfiehlt es sich, anhand der unten aufgeführten Schritte vorzugehen. Hierbei kann der Datenschutzbeauftragte durch seine Erfahrung und Fachkunde eine wichtige Unterstützung sein.

Der risikobasierte Ansatz in der DSGVO führt zu den folgenden Anforderungen an den Verantwortlichen[22]:

- Identifikation der mit der Verarbeitung (einschliesslich Art, Umfang, Umstände, Zwecke) verbundenen Risiken (geschütztes Rechtsgut)
- Risikoanalyse unter Berücksichtigung der Eintrittswahrscheinlichkeit und der Schwere der Folgen
- Einordnung, ob es sich um ein einfaches Risiko oder ein hohes Risiko handelt
- Risikobehandlung durch entsprechende Massnahmen

In einem ersten Schritt muss der Verantwortliche die Risiken der Datenverarbeitung identifizieren. Dabei spielt die Art der Verarbeitung eine Rolle. Diese betrifft entweder die Mittel (z.B. Profiling, automatisierte Verarbeitung, Monitoring, etc.) oder die Verarbeitung bestimmter Arten von Daten (besondere Kategorien wie sensible Daten: Gesundheitsdaten, Gewerkschaftszugehörigkeit, Daten von Kindern, etc.). Wie bereits oben dargelegt, konkretisiert die DSGVO die Schutzgüter nicht. Diese können von den erwähnten Risikokategorien in EG 75 abgeleitet werden[23].

Anschliessend ist eine Risikoanalyse durchzuführen, dafür werden die Eintrittswahrscheinlichkeiten und die möglichen Schäden der identifizierten Risiken evaluiert. Dieser Vorgang ermöglicht auch die Einordnung als einfaches Risiko[24] oder als hohes Risiko[25]. Das Ergebnis aus der Analyse bildet dann z.B. im Rahmen des Art. 32 DSGVO den Massstab für die Wahl der technischen und organisatorischen Massnahmen für die Sicherheit der Verarbeitung.

Im Rahmen der Risikobehandlung kann der Verantwortliche z.B. durch Pseudonymisierung oder Verschlüsselung ein vorhandenes Risiko reduzieren oder er kann – soweit ihm die technischen Möglichkeiten zur Reduktion fehlen – das Risiko durch Outsourcing in Datenzentren mit höheren Standards an einen Dritten übertragen.

III. Risikobasierter Ansatz im E-DSG?

Der E-DSG enthält ebenfalls keine Definitionen der Begriffe «Risiko» und «risikobasierter Ansatz».

Gemäss Botschaft zum E-DSG gilt, dass die Totalrevision sich an sieben Leitlinien orientiert, auf denen die verschiedenen Neuerungen beruhen:

«Eine erste Leitlinie der Revision bildet der risikobasierte Ansatz. Der Revisionsentwurf orientiert sich konsequent an den potenziellen Risiken für die betroffenen Personen, denn die Gefahren für die Privatsphäre der betroffenen Personen hängen weitgehend von den Aktivitäten der verschiedenen Verantwortlichen und Auftragsbearbeiter ab. Dementsprechend sind beispielsweise die Pflichten von Verantwortlichen, deren Aktivitäten mit einem erhöhten Risiko verbunden sind (z.B. Unternehmen, deren Haupttätigkeit in der Datenbearbeitung besteht), strenger als jene von Verantwortlichen, deren Aktivitäten ein geringeres Risiko darstellen (z.B. Datenbearbeitungen, die auf eine Kundendatei ohne besonders schützenswerte Daten beschränkt sind)»[26].

Die Botschaft konkretisiert an diversen Stellen, was «risikobasierter Ansatz» bedeutet: «Die Norm bringt den risikobasierten Ansatz zum Ausdruck. Das Risiko, das mit einer Bearbeitung einhergeht, muss in Beziehung gesetzt werden zu den technischen Möglichkeiten, um dieses zu ver-

[20] <http://www.privacy-regulation.eu/de/erwaegungsgrund-75-DS-GVO.htm>.

[21] <http://www.privacy-regulation.eu/de/erwaegungsgrund-89-DS-GVO.htm>.

[22] Siehe auch <https://www.datenschutzbeauftragter-info.de/der-risikobegriff-in-der-datenschutz-grundverordnung/>.

[23] Beispiele für physische, materielle und immaterielle Schäden sind: Diskriminierung, Identitätsverlust, finanzieller Verlust, Rufschädigung, Verlust von Vertraulichkeit vom Berufsgeheimnis unterliegenden personenbezogenen Daten, Verlust von Rechten und Freiheiten, Vernichtung und Verlust von personenbezogenen Daten, unbefugte Offenlegung.

[24] Z.B. Art. 30 und 33 DSGVO.

[25] Z.B. Art. 34 Abs. 1, 35 Abs. 1 und 36 Abs. 1 DSGVO.

[26] BBl *2017* 6970/6971.

ringern. Je höher das Risiko, je grösser die Eintrittswahrscheinlichkeit und je umfangreicher die Datenbearbeitung ist, umso höher sind die Anforderungen an die technischen Vorkehren, damit sie im Sinne der vorliegenden Bestimmung als angemessen gelten können»[27].

IV. Conclusio: Erleichterungen und Umsetzungsspielraum für den Verantwortlichen

Der risikobasierte Ansatz führt dazu, dass sich der Verantwortliche bei der Umsetzung der neuen Bestimmungen der DSGVO und dem E-DSG am Datenschutzrisiko der betroffenen Person ausrichten muss. Dies führt klar zu einer Erleichterung für den Verantwortlichen, da ihm in der Praxis damit ein gewisser Umsetzungsspielraum eingeräumt wird. Der Verantwortliche wird dabei jedoch aufpassen müssen, dass er bei der Abwägung nicht leichtfertig auf Regeln verzichtet. Dies könnte nämlich zu einer Pflichtverletzung und damit zu hohen Bussen führen.

[27] BBl *2017* 7030.

Entwicklungen im Versicherungs- und Haftpflichtrecht / Le point sur le droit des assurances privées et de la responsabilité civile

Prof. Dr. Walter Fellmann, Rechtsanwalt (Luzern)*

I. Gesetzgebung

A. Haftpflichtrecht

Im Haftpflichtrecht gibt es für das Jahr 2017 über keine neuen Gesetze oder Gesetzesvorhaben zu berichten. Hängig ist die Revision des Verjährungsrechts (Verlängerung Verjährungsfristen). Am 4. September 2017 hat die Kommission für Rechtsfragen des Nationalrats beschlossen, dem Rat zu beantragen, die Vorlage zur Revision des Verjährungsrechts abzuschreiben. Anders entschieden hat die Kommission für Rechtsfragen des Ständerats. Sie hat am 27. Oktober 2017 beschlossen, die Verjährungsrechtsvorlage nicht abzuschreiben. Sie ist überzeugt, dass die Revision auch nach der Gründung des Entschädigungsfonds für Asbestopfer (EFA) weiter erforderlich sei.[1]

B. Privatversicherungsrecht

Der Bundesrat hat an seiner Sitzung vom 28. Juni 2017 die Botschaft für eine Teilrevision des Versicherungsvertragsgesetzes (VVG) verabschiedet. Die zentralen Anliegen der Teilrevision des VVG umfassen folgende Punkte: ein 14-tägiges Widerrufsrecht, Regelung der vorläufigen Deckungszusage, Zulassung der Rückwärtsversicherung unter bestimmten Voraussetzungen, Verlängerung der Verjährungsfrist für Forderungen aus dem Versicherungsvertrag bis auf wenige Ausnahmen von zwei auf fünf Jahre, Einschränkung des Schutzbereichs des VVG bei Grossrisiken bzw. bei professionellen Versicherungsnehmern, Berücksichtigung des elektronischen Geschäftsverkehrs, indem für die meisten Mitteilungen alternativ zur einfachen Schriftlichkeit der Nachweis durch Text ermöglicht wird, Neuregelung der Beendigung des Versicherungsvertrags unter Einführung eines ordentlichen Kündigungsrechts.[2]

* Professor für Privatrecht an der Universität Luzern, Fachanwalt SAV Haftpflicht- und Versicherungsrecht.

[1] <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20130100>.

[2] Botschaft zur Änderung des Versicherungsvertragsgesetzes vom 28. Juni 2017, BBl *2017* 5096 f.; vgl. dazu eingehend HAVE *2017*

Schweizerische Juristen-Zeitung
Revue Suisse de Jurisprudence

1. April 2018, 114. Jahrgang