Rolf H. Weber
Prof. Dr. iur., em. Prof. an der Universität Zürich Rechtsanwalt
Konsulent
Telefon +41 58 258 10 00
rolf.weber@bratschi.ch

Neue Compliance-Anforderungen im Datenschutzbereich

Das neue, im Jahre 2022 in Kraft tretende totalrevidierte Datenschutzgesetz wird den Compliance-Aufwand der Unternehmen erhöhen, insbesondere wegen der erweiterten Informationspflichten und der strengeren Datensicherheitsvorschriften. Überlegungen zur Umsetzung der konkreten Massnahmen sind schon jetzt empfehlenswert.

1. Einleitung

Das Datenschutzrechtsumfeld ist im Fluss. Im Anschluss an die seit Ende Mai 2018 in Kraft stehende Datenschutz-Grundverordnung der Europäischen Union (EU) hat auch das Schweizer Parlament nach einem langjährigen Gesetzgebungsprozess am 25. September 2020 das totalrevidierte Datenschutzgesetz (DSG) verabschiedet. Die Referendumsfrist ist am 14. Januar 2021 unbenutzt verstrichen; mit dem Inkrafttreten des neuen DSG ist 2022 zu rechnen.

Zwar spricht die politische Diskussion von einer «totalen» Revision des DSG, doch sind die neuen Bestimmungen nicht so innovativ, wie man auf den ersten Blick denken könnte; gerade konzeptionell ist das Datenschutzrecht nicht stark verändert worden. Diese Einschätzung ändert aber nichts an der Tatsache, dass die Compliance-Verantwortlichen in Unternehmen vor verschiedenen neuen Herausforderungen stehen, weil der Datenschutz über die gesellschafts- und kartellrechtlichen Bereiche hinaus zu einem wichtigen Compliance-Thema geworden ist.

2. Punktuelle Neuerungen bei den Datenbearbeitungsgrundsätzen

Angesichts der Digitalisierung aller Lebensbereiche gewinnen die Daten, gerade für Unternehmen, eine immer grössere Bedeutung. In den Anwendungsbereich des DSG fallen Personendaten von natürlichen Personen (künftig nicht mehr von juristischen Personen). Personendaten liegen vor, wenn die Information sich auf eine bestimmte oder zumindest bestimmbare natürliche Person bezieht; die weit auszulegende Bestimmbarkeit lässt sich durch Anonymisierung und Pseudonymisierung von Daten ausschliessen. An der Abgrenzung zwischen Personen- und Sachdaten ändert

sich mit dem neuen DSG kaum etwas; auch die Datenbearbeitungsgrundsätze (Verhältnismässigkeit, Erkennbarkeit bzw. Transparenz, Zweckbindung) haben keine wesentlichen Änderungen erfahren. Drei Themen sind aus Compliance-Sicht aber erwähnenswert:

- Neue Anforderungen können sich aus der Regulierung des bisher nicht (unmittelbar) adressierten Phänomens des Profilings (mit hohem Risiko) ergeben. Ein Profiling besteht in einer automatisierten Datenbearbeitung zur Beurteilung persönlicher Aspekte einer natürlichen Person; Datenverknüpfungen können ein hohes Risiko mit sich bringen (Art. 5 lit. f und g DSG). Verletzt ein solches Profiling mit hohem Risiko einen Datenbearbeitungsgrundsatz und vermag sich der Verantwortliche nicht auf einen Rechtfertigungsgrund des DSG abzustützen, muss die Einwilligung der betroffenen Person ausdrücklich erfolgen (Art. 6 Abs. 7 lit. b DSG).
- Im Falle der Vornahme automatisierter Entscheidungen ist die betroffene Person zu informieren und ihr die Möglichkeit zu geben, den eigenen Standpunkt darzulegen bzw. es ist ihr das Recht einzuräumen, die Entscheidung überprüfen zu lassen (Art. 21 DSG). Zudem verfügt die betroffene Person über ein Auskunftsrecht betreffend (i) das Vorliegen einer automatisierten Einzelentscheidung sowie (ii) die Logik, auf der die Entscheidung beruht (Art. 25 Abs. 2 lit. f DSG).
- Neu eingeführt hat das DSG ausserdem die Pflicht zur Erstellung eines Verzeichnisses der Bearbeitungstätigkeit. Diese Inventarpflicht, welche für Verantwortliche und Auftragsbearbeiter gilt, kann im Lichte des gesetzlich angeordneten Mindestinhalts eines solchen Verzeichnisses (Art. 12 Abs. 2 und 3 DSG) herausfordernd und aufwendig sein.

3. Erweiterung der Datensicherheitsvorgaben

Selbst wenn sich dies dem neuen DSG nicht unmittelbar entnehmen lässt, lösen einzelne Vorschriften, die sich mit dem Thema der Datensicherheit beschäftigen, künftig wohl den grössten Handlungsbedarf aus. Der Verantwortliche und der Auftragsbearbeiter sind verpflichtet, durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten (Art. 8 Abs. 1 DSG). Der Bundesrat hat die Möglichkeit, konkretisierende Bestimmungen über die Mindestanforderungen in der noch auszuarbeitenden Datenschutz-Verordnung zu erlassen. Informationstechnologisch geht es darum, Massnahmen zu implementieren, um die Resilienz der Systeme sicherzustellen. Zum entsprechenden Schutzkonzept gehören der Informationsaustausch auf allen Ebenen (strategisch, taktisch und operativ/technisch) sowie die Einrichtung von Prozessen, um Fehlerquellen zu entdecken («detection») und um angemessen auf Schwachstellen zu reagieren («reaction»), insbesondere im Anschluss an eine Cyber-Attacke. Beaufsichtigte Unternehmen (z.B. Banken, Versicherungen) sind gestützt auf sektorspezifische Regulierungen schon heute gehalten, ein «Business Continuity Management» und eine «Desaster-Recovery-Planung» einzurichten; solche Prozesse dürften künftig auch für nichtüberwachte Unternehmen relevant werden.

Neu hat das Konzept «Privacy by Design», das im internationalen Kontext entwickelt worden ist, Eingang in das DSG gefunden. Gemäss Art. 7 DSG ist der Datenschutz (auch) durch Technik und

datenschutzfreundliche Voreinstellungen zu gewährleisten, d.h. die Datenbearbeitung ist technisch und organisatorisch so auszugestalten, dass die Datenbearbeitungsgrundsätze (Art. 6 DSG) eingehalten werden können. Die Massnahmen müssen dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, angemessen sein. Die Datensicherheit bezieht sich auf den Schutz von Daten vor dem ungewollten Verlust, der ungewollten Löschung, Vernichtung, Veränderung oder Offenlegung oder anderem Zugänglichmachen gegenüber Unbefugten (Art. 5 lit. h DSG).

In einer sehr detaillierten Bestimmung (Art. 22 DSG) wird zulasten des Verantwortlichen die Pflicht festgelegt, eine Datenschutz-Folgenabschätzung vorzunehmen, wenn die Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Die Folgenabschätzung muss eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken sowie Massnahmen zum Persönlichkeitsschutz enthalten. Im Ausland sind bereits Modelle für datenschutzrechtliche «Stresstests» hinsichtlich der Risikobewertung bei Folgenabschätzungen entwickelt worden. Zu konkretisieren sind dabei die verschiedenen Risikokategorien sowie die prozedurale Risikobewertung in Mikro- und Makro-Stresstests.

Neu eingeführt hat das DSG auch eine Pflicht zur Meldung im Falle von Verletzungen der Datensicherheit. Der Verantwortliche hat eine solche Verletzung, wenn sie zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, «so rasch als möglich» dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu melden, und zwar unter Angabe der Art der Verletzung, deren Folgen sowie der ergriffenen oder vorgesehenen Massnahmen (Art. 24 DSG). Die betroffenen Personen sind zu informieren, wenn dies zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt. Unter Compliance-Gesichtspunkten sind diejenigen Vorkehren rechtzeitig zu treffen, die als angebracht erscheinen, um die Meldung einer Verletzung der Datensicherheit umgehend vornehmen zu können; nach Eintritt eines negativen Ereignisses bleibt regelmässig keine Zeit, entsprechende Überlegungen anzustellen. Die Meldepflicht gilt in jedem Fall der rechtswidrigen Datenbearbeitung, aber auch etwa bei einer versehentlichen Zerstörung oder Veränderung von Daten. Im Falle einer «Datenpanne» sind also die Risiken abzuschätzen und angemessen zu dokumentieren. Empfehlenswert sind z.B. die Festlegung definierter Rollen und Verantwortlichkeiten, die Schulung der entsprechenden Mitarbeitenden, die Klassifizierung und Priorisierung der zu treffenden Massnahmen sowie die umfassende Dokumentierung der Handlungsempfehlungen und des Monitorings.

Bei der Ausgestaltung des Datensicherheitskonzepts ist auf die branchenüblichen Rahmenbedingungen gemäss den «Best Practices» abzustellen; Leitlinien finden sich in den Publikationen internationaler Berufsverbände der IT-Branche.

4. Outsourcing und grenzüberschreitender Datenverkehr

Im Falle eines Outsourcings bzw. der Nutzung von Cloud-Dienstleistungen hat der Verantwortliche die betroffenen Personen darüber zu informieren, in welchem Rahmen die IT-Auslagerung erfolgt (z.B. Kategorien von Empfängern, denen Personendaten bekannt gegeben werden) und wie sich die Individualrechte nach dem DSG geltend machen lassen. Gemäss den Erläuterungen des EDÖB zum Cloud-Computing gilt als Grundregel: «Je vertraulicher, geheimer, wichtiger» (weil geschäftskritisch) oder «sensitiver» (weil besonders schützenswert) die Daten sind, umso eher ist von einer Auslagerung der Daten in die Cloud, insbesondere eine ausländische Cloud, abzusehen, und desto strikter und umfassender müssen die (Datenschutz-)Sicherheitsvorkehren und deren Kontrolle sein. In der Praxis lässt sich immerhin nicht übersehen, dass (technologisch fortgeschrittene) Cloud-Anbieter zuweilen eine höhere Datensicherheit gewährleisten als (nicht IT-affine) Unternehmen; in einer solchen Situation vermag die Nutzung von Cloud-Dienstleistungen gar ein Erfordernis der datenschutzrechtlichen Vorgaben an die Datensicherheit zu sein.

Eine Auftragsdatenbearbeitung setzt eine vertragliche Grundlage voraus, die es dem Cloud-Anbieter «nur» erlaubt, die Daten so zu bearbeiten, wie das outsourcende Unternehmen es selbst tun dürfte. Vertragsmuster für ein Outsourcing sind verbreitet verfügbar. Der Verantwortliche muss sich zudem vergewissern, dass der Cloud-Anbieter in der Lage ist, die Datensicherheit zu gewährleisten (Art. 9 Abs. 2 DSG). Will der Cloud-Anbieter die Bearbeitung an einen Dritten (Substituten oder Unterakkordanten) übertragen, hat er vorgängig eine Genehmigung einzuholen (Art. 9 Abs. 3 DSG).

Nutzt ein Unternehmen die Cloud-Dienstleistungen eines ausländischen Anbieters, gibt es Daten ins Ausland bekannt und muss deshalb die besonderen Vorgaben von Art. 16/17 DSG beachten. Inhaltlich weicht das neue Recht nicht wesentlich von den bisherigen Regelungen ab, doch ist deren Verletzung künftig mit Busse bedroht (Art. 61 lit. b DSG). Ausschlaggebend für die Zulässigkeit des grenzüberschreitenden Datenverkehrs ist ein angemessener Schutz der Daten im Ausland. Anstelle des EDÖB ist neu ausdrücklich der Bundesrat für die Beurteilung der Angemessenheit der ausländischen Gesetzgebung zuständig (Art. 16 Abs. 1 DSG). Fehlt es an einem entsprechenden Angemessenheitsentscheid, ist die Bekanntgabe zulässig, wenn ein geeigneter Datenschutz durch besondere Garantien, etwa durch Standarddatenschutzklauseln, welche der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat, gewährleistet wird (Art. 16 Abs. 2 lit. d DSG). Eine Bekanntgabe von Daten ins Ausland ist weiter zulässig, wenn die ausdrückliche Einwilligung der betroffenen Person vorliegt (Art 17 DSG).

Im Verhältnis zwischen der Schweiz und den EU-Ländern hat bisher ein Angemessenheitsentscheid vorgelegen. Derzeit prüft die EU-Kommission das Schutzniveau des neuen DSG; mit der entsprechenden Einschätzung ist in Kürze zu rechnen. Anders ist die Situation mit Bezug auf den Datenverkehr zwischen der Schweiz und den USA. Der Europäische Gerichtshof konnte mit dem Entscheid vom 16. Juli 2020 (Schrems II) nur den EU-US-Privacy Shield für ungültig erklären und dieses Urteil ist in der Schweiz nicht direkt anwendbar; indessen hat der EDÖB im September 2020

verlauten lassen, dass eine Neubeurteilung auch in der Schweiz vorgenommen werden müsse und dass deshalb der «Verweis auf einen angemessenen Datenschutz unter bestimmten Bedingungen» für die USA in der Länderliste zu streichen sei. Aus diesem Grunde können sich Schweizer Unternehmen nun nicht mehr auf den Privacy Shield abstützen. Im Datenverkehr mit den USA sind vielmehr Standardvertragsklauseln zu verwenden, wenn auch in angepasster bzw. verbesserter Form unter Berücksichtigung der Vorgaben aus dem Schrems II-Urteil. Die EU-Kommission hat am 12. November 2020 einen neuen Entwurf für Standardvertragsklauseln publiziert; dieses «Muster» vermag auch den Schweizer Unternehmen zu dienen. Ein nicht unerheblicher Handlungsbedarf ist insoweit also offensichtlich; verschiedene Elemente im Datenverkehr mit den USA, vom Data Mapping über die Transfermechanismen bis zur rechtlichen Beurteilung, sind vertieft zu analysieren.

5. Ausblick

Sofern Unternehmen nicht schon 2018 wegen der DSGVO die datenschutzrechtliche Compliance verbessert haben, wird dieses Erfordernis im Jahre 2022 aufleben. Besondere Beachtung ist der Erhöhung der Datensicherheit zu schenken; verfeinerte Prozesse zu deren Schutz und ausreichende Vorkehren, um auf eintretende Probleme zu reagieren, sind unabdingbar. Zugleich ist die interdisziplinäre Zusammenarbeit zwischen den Technikern und den Rechtskundigen auszubauen.

Weiterführende Unterlagen, verfügbar bei Bratschi AG:

- Adrian Bieri/Julian Powell, Die Totalrevision des Bundesgesetzes über den Datenschutz, Jusletter 16. November 2020
- Adrian Bieri/Julian Powell, Informationspflicht nach dem totalrevidierten Datenschutzgesetz, AJP 2020, 1533 ff.
- Rolf H. Weber/Simon Henseler, Daten-Governance und Cloud Banking im neuen Datenschutzrechtsumfeld, SZW 2020, 604 ff.
- Rolf H. Weber, Datenexport in die USA – Neue Welt nach Schrems II?, EuZ 2021, 24 ff.

Basel
Lange Gasse 15
Postfach
CH-4052 Basel
T +41 58 258 19 00
F +41 58 258 19 99
basel@bratschi.ch

Bern
Bollwerk 15
Postfach
CH-3001 Bern
T +41 58 258 16 00
F +41 58 258 16 99
bern@bratschi.ch

Genf
Rue du Général-Dufour 20
1204 Genf
T +41 58 258 13 00
F +41 58 258 17 99
geneva@bratschi.ch

Lausanne
Avenue Mon-Repos 14
Postfach 5507
CH-1002 Lausanne
T +41 58 258 17 00
T +41 58 258 17 99
lausanne@bratschi.ch

St. Gallen
Vadianstrasse 44
Postfach 262
CH-9001 St. Gallen
T +41 58 258 14 00
F +41 58 258 14 99
stgallen@bratschi.ch

Zug
Gubelstrasse 11
Postfach 7106
CH-6302 Zug
T +41 58 258 18 00
F +41 58 258 18 99
zug@bratschi.ch

Zürich
Bahnhofstrasse 70
Postfach
CH-8021 Zürich
T +41 58 258 10 00
F +41 58 258 10 99
zuerich@bratschi.ch