DIE TOTALREVISION DES DATENSCHUTZGESETZES: ÜBERBLICK ÜBER DIE WICHTIGSTEN NEUERUNGEN

MLaw Simone Küng, Rechtsanwältin

Am 25. September 2020 hat das Schweizer Parlament dem Entwurf zur Totalrevision des Datenschutzgesetzes (DSG) verabschiedet. Es wird voraussichtlich am 1. September 2023 in Kraft treten. Da das revidierte Datenschutzgesetz keine Übergangsfrist für die neu in Kraft tretenden Regelungen vorsieht, sollten die Anpassungen frühzeitig umgesetzt werden. Insgesamt beinhaltet das revidierte Datenschutzgesetz eine Verschärfung der bisherigen Bestimmungen. Zurückzuführen ist die Revision insbesondere auf internationale Abkommen mit der EU. Nachdem das Schutzniveau des schweizerischen Datenschutzgesetzes erheblich tiefer war, als dasjenige der EU, drohte die Schweiz als nicht angemessen regulierter Drittstaat qualifiziert zu werden, was erhebliche Schwierigkeiten im internationalen Datenaustausch mit sich gebracht hätte. Dies erklärt sodann auch die auffallende Angleichung des Schweizer Datenschutzrechts an die Datenschutzgrundverordnung (DSGVO) der EU.

I. RÄUMLICHER GELTUNGSBEREICH

Mit der Einführung des neuen Datenschutzgesetzes kommt analog zum Kartellrecht und zur Datenschutzgrundverordnung (DSGVO) das *Auswirkungsprinzip* zum Tragen (Art. 3 revDSG). Demnach unterliegen auch Unternehmen mit ausländischem Sitz dem schweizerischen Datenschutzgesetz, wenn sich die Datenbearbeitung von Personendaten auf die Schweiz auswirkt. Wann sich eine Datenbearbeitung auf die Schweiz «auswirkt», ist im neuen Gesetz nicht definiert. Es dürften allerdings analoge Kriterien zur DSGVO herangezogen werden, womit das Angebot von Waren oder Dienstleistungen an Personen in der Schweiz ausreicht, damit das neue Datenschutzrecht der Schweiz greift. Liefert bspw. ein ausländisches Unternehmen seine Produkte auch in die Schweiz, so dürfte die Bearbeitung der Personendaten des Schweizer Kunden dem neuen Datenschutzgesetz unterstehen.

Unterliegt die Datenbearbeitung eines ausländischen Unternehmens dem schweizerischen Datenschutzrecht, so kann das Unternehmen unter Umständen dazu verpflichtet werden, eine Vertretung in der Schweiz zu bezeichnen, wie dies bereits die DSGVO für Drittstaaten analog vorsieht.

II. DATEN JURISTISCHER PERSONEN UND BESONDERS SCHÜTZENSWERTE PERSONENDATEN

Die Bestimmungen des Datenschutzgesetzes sind grundsätzlich nur auf die Bearbeitung von Personendaten anwendbar, sofern mittels den erfassten Daten ein Bezug oder eine Aussage zu einer bestimmten, individualisierbaren Person enthalten ist. Bisher gehörten hierzu auch Daten über juristische Personen. Mit der Revision des Datenschutzgesetzes fällt die Bearbeitung von *Daten über juristische Personen* nicht mehr unter dessen Anwendungsbereich (Art. 5 lit. a revDSG). Dies betrifft allerdings nur Daten über die juristische Person an sich. Auf die Daten über natürliche Personen eines Unternehmens (wie bspw. deren Mitarbeiter), kommt aber nach wie vor das Datenschutzrecht zur Anwendung.

Die aktuelle Fassung des Datenschutzgesetzes qualifiziert die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen *als besonders schützenswerte Personendaten* (Art. 3 lit. c DSG). Neu gelten auch Daten zur Ethnie sowie genetische und biometrische Daten als besonders schützenswert (Art. 5 lit. c revDSG). Für besonders schützenswerte Personendaten gelten insbesondere erhöhte Anforderungen an die Einwilligung der betroffenen Personen zu deren Bearbeitung.

III. BETROFFENENRECHTE

Mit Art. 6 Abs. 4 revDSG wird die Pflicht zur Vernichtung oder Anonymisierung der Personendaten eingeführt. Sobald diese zum Zweck der Datenbearbeitung nicht mehr erforderlich sind, müssen sie vernichtet oder zumindest anonymisiert werden. Dies bedingt wiederum, dass vorab eine Aufbewahrungsdauer für die erhobenen Personendaten festgelegt wird.

In Art. 25 revDSG findet sich neuerdings das Auskunftsrecht, welches heute noch in Art. 8 DSG geregelt ist. Nach wie vor sollen Betroffene hierüber Auskunft über die sie betreffenden Datenbearbeitungen erhalten. Unter bestimmten Umständen kann das Auskunftsrecht aber eingeschränkt werden, wenn überwiegende Interessen vorliegen (Art. 26 revDSG).

Im Weiteren erhalten betroffene Personen ein Recht auf Datenherausgabe und -übertragung («Datenportabilität», Art. 28 revDSG) sowie ein Widerspruchsrecht. Das Recht auf Datenherausgabe und -übertragung ist insofern beschränkt, als die Rechteausübung stets verhältnismässig sein muss und die Herausgabe der Daten in einem gängigen elektronischen Format erfolgen darf. Das Widerspruchsrecht hingegen nimmt Bezug auf automatisierte Einzelentscheidungen (Profiling). Die betroffene Person kann verlangen, dass das Profiling von einer natürlichen Person wiedererwägt wird (vgl. die Ausführungen zum Profiling).

Neu wurde das Berichtigungsrecht unter Art. 28 Abs. 1 revDSG bei den Rechtsansprüchen Betroffener geregelt, welches sich bisher ohnehin vom Grundsatz der Richtigkeit der Daten ableiten liess.

IV. PROFILING («AUTOMATISIERTE EINZELENTSCHEIDE»)

Unter «Profiling» wird eine ausschliesslich automatisierte Entscheidfindung verstanden. Typisches Beispiel sind insbesondere Onlineshops, die das Surfverhalten ihrer Nutzer analysieren und diesen dann Kaufempfehlungen präsentieren. Neu unterscheidet das revidierte Datenschutzgesetz zwischen (gewöhnlichem) Profiling und «Profiling mit hohem Risiko». Gemäss Art. 5 lit. g revDSG liegt ein hohes Risiko vor, wenn die Persönlichkeit oder die Grundrechte der betroffenen Person besonders gefährdet sind, indem das Profiling zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

Eine ausdrückliche Einwilligung durch die betroffene Person ist für das Profiling nach wie vor nicht erforderlich. Es gilt allerdings weiterhin, dass bei einer persönlichkeitsverletzenden Datenbearbeitung eine Einwilligung oder ein Rechtfertigungsgrund für die Datenbearbeitung bzw. das Profiling erforderlich ist. Liegt ein «Profiling mit hohem Risiko» vor, so muss die Einwilligung eine ausdrückliche sein.

Betroffene können u.U. verlangen, dass die automatisierte Entscheidfindung durch eine natürliche Person überprüft wird. Als klassisches Beispiel dürfte hier die Bonitätsprüfung dienen (bspw. bei der Vergabe eines Leasingvertrages). Sollte die Bonitätsprüfung negativ ausfallen, kann die betroffene Person eine Überprüfung durch eine natürliche Person verlangen, sofern sie vorgängig nicht ausdrücklich einer vollständig automatisierten Entscheid-findung zugestimmt hat. Bezüglich einer allfälligen Bonitätsprüfung ist ergänzend anzumerken, dass deren Durchführung unter dem revidierten Datenschutzgesetz nur noch unter strengen Voraussetzungen zulässig ist (Art. 30 Abs. 2 lit. c revDSG).

V. PFLICHTEN FÜR DATENSCHUTZVERANTWORTLICHE IM EINZELNEN

1) INFORMATIONSPFLICHT

Neu greift eine verschärfte Informationspflicht (Art. 19 revDSG). Demnach müssen betroffene Personen i.S. der Transparenz vorab über die beabsichtigte Datenbearbeitung informiert werden. Die Informationspflicht umfasst im Wesentlichen Angaben über die Bearbeitungszwecke, die verantwortliche Person der Datenbearbeitung (sofern eine solche ernannte wurde) sowie über die Empfänger bei Übermittlung von Daten und auch über eine etwaige Übermittlung ins Ausland (inkl. Information über die Rechtsgrundlage für Exporte in unsichere Länder). Zudem wird wohl über eine allfällige automatisierte Entscheidung oder andere Profiling-Massnahmen zu informieren sein. Diese Informationspflicht dürften die Verantwortlichen durch die Publikation / Abgabe einer rechtsgenüglichen Datenschutzerklärung nachkommen.

2) DATENVERARBEITUNGSVERZEICHNIS

Neu sind Verantwortliche verpflichtet, ein Verzeichnis über die Datenbearbeitungstätigkeiten zu führen (Art. 12 revDSG), was einen erheblichen Aufwand mit sich bringen kann. Hingegen dürfte der Bundesrat für KMUs Erleichterungen zum Datenverarbeitungsverzeichnis vorsehen (Art. 12 Abs. 5 revDSG). Das Datenverarbeitungs-verzeichnis soll einen Überblick über die wichtigsten unternehmensinternen Datenverarbeitungsprozesse beinhalten und muss regelmässig aktualisiert werden. Die notwendigen Mindestangaben sind in Art. 12 Abs. 2 revDSG aufgeführt.

3) DATENSCHUTZFOLGEABSCHÄTZUNG («DSFA»)

Soll unternehmensintern eine neue Datenbearbeitung eingeführt werden, besteht neuerdings eine Pflicht zur Vornahme von Datenschutz-Folgenabschätzungen (kurz: «DSFA»), sofern die fragliche Datenbearbeitung ein hohes Risiko für die betroffene Person mit sich bringen kann (Art. 20 Abs. 1 revDSG). Sie muss insbesondere Erwägungen über die Risiken der geplanten Datenbearbeitungen beinhalten, sowie allfällige Massnahmen vorsehen, mit welchen diesen begegnet werden kann. Führt die DSFA zum Ergebnis, dass die Datenbearbeitung ein hohes Risiko für die betroffenen Personen mit sich bringt, so besteht eine vorgängige Konsultationspflicht beim EDÖB (Art. 21 Abs. 1 revDSG, wobei Ausnahmen bestehen, wenn ein unternehmensinterner Datenschutzberater vorgängig konsultiert wurde).

4) «PRIVACY BY DESIGN» UND «PRIVACY BY DEFAULT»

Unter «privacy by design» (vgl. Art. 7 revDSG) ist die Pflicht zur Gewährleistung eines rechtsgenüglichen Datenschutzes in der Gestaltung von Systemen zu verstehen. Dies bedeutet, dass alle zumutbaren technischen und organisatorischen Möglichkeiten ausgeschöpft werden müssen, um die aufbewahrten Personendaten i.S. von Art. 6 revDSG zu schützen. «privacy by design» ergänzt Art. 7 DSG, welcher neu in Art. 8 revDSG geregelt ist und auf die Datensicherheit im engeren Sinne Bezug nimmt.

«privacy by default» (vgl. Art. 7 Abs. 3 revDSG) verpflichtet Verantwortliche im Weiteren, den Datenschutz durch Voreinstellungen zu gewährleisten. Sollte also ein Verantwortlicher mehrere Möglichkeiten der Datenbearbeitung vorsehen und die Auswahl hierüber den betroffenen Personen überlassen, so haben die Voreinstellungen grundsätzlich eine möglichst geringfügige Datenbearbeitung vorzusehen. Die betroffene Person kann dann selbstverständlich auch in eine weitergehende Datenbearbeitung einwilligen.

5) AUFTRAGSBEARBEITUNG

Gemäss Art. 5 lit. k revDSG gilt als Auftragsbearbeiter, wer im Auftrag eines Verantwortlichen Personendaten bearbeitet. Erforderlich ist, dass der Auftragszweck in der Bearbeitung von Personendaten liegt (bspw. externe Lohnbuchhaltung). Ist die Datenbearbeitung lediglich ein Mittel zur Auftragserfüllung, so liegt keine Auftragsbearbeitung vor.

Wird ein Auftragsbearbeiter eingesetzt, muss der Verantwortliche dafür sorgen, dass der Auftragsbearbeiter die Daten nur so bearbeitet, wie der Verantwortliche selbst dazu berechtigt wäre (Art. 9 revDSG). Der Auftragsbearbeiter darf die Daten also nicht zu seinem eigenen Zweck bearbeiten. Der Verantwortliche ist mithin nicht nur für die eigene Datenbearbeitung, sondern auch für diejenige des Auftragsbearbeiters in der Pflicht. Um sich rechtsgenüglich abzusichern, ist der Abschluss einer Auftragsbearbeitungsvereinbarung ratsam. Neu ist sodann, dass die Weitergabe der Daten an einen Subunternehmer eine vorgängige Genehmigung durch den Verantwortlichen erfordert.

6) MELDEPFLICHT: DATA BREACH

Liegt eine Datenschutzverletzung vor (bspw. Datenverluste oder wenn Daten Unbefugten offengelegt / zugänglich gemacht wurden), hat der Verantwortlich diese dem EDÖB unverzüglich zu melden, sofern diese voraussichtlich ein grosses Risiko für die Persönlichkeit oder die Grundrechte der Betroffenen birgt (Art. 22 revDSG). Die Verletzung der Datensicherheit muss der betroffenen Person im Übrigen nur mitgeteilt werden, sofern dies zu ihrem Schutz erforderlich ist oder vom EDÖB verlangt wird. Im Unterschied zur DSGVO sieht das revDSG keine starre 72-Stunden-Meldefrist und keine Protokollierungspflicht vor.

7) BERUFSGEHEIMNIS

Für geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile sieht das aktuelle Datenschutzgesetz bereits eine berufliche Schweigepflicht vor (Art. 35 DSG). Neuerdings gilt die berufliche Schweigepflicht für sämtliche geheimen Personendaten, von denen jemand bei der Ausübung eines Berufes Kenntnis erlangt hat, der die Kenntnis solcher Daten erfordert (Art. 62 revDSG). Damit wurde de facto eine Schweigepflicht für alle Berufstätigen eingeführt. Der Verstoss gegen das Berufsgeheimnis kann mit Busse bis zu CHF 250’000.00 geahndet werden.

VI. DATENTRANSFER INS AUSLAND

Werden Daten ins Ausland übermittelt, so muss entsprechend darüber informiert werden (Art. 19 Abs. 4 revDSG; vgl. die Ausführungen zu den Informationspflichten). Im Rahmen der Datenschutzerklärung muss im Weiteren bekannt gegeben werden, gestützt auf welcher Grundlage der Datenexport stattfindet. Der Bundesrat legt diesbezüglich verbindlich fest, welche Länder einen angemessenen Datenschutz gewährleisten. Erachtet der Bundesrat das Datenschutzniveau im betroffenen Land als angemessen, ist die Datenübermittlung ohne besondere Vorkehrungen zulässig (Art. 16 Abs. 1 revDSG). Handelt es sich hingegen um einen unsicheren Drittstaat, müssen weitere Massnahmen ergriffen werden (wie bspw. die Verwendung bestimmter Datenschutzklauseln), damit eine datenkonforme Übermittlung der Daten ins Ausland erfolgen kann (Art. 16 Abs. 2 und Art. 17 revDSG). Insbesondere nachdem auch das EDÖB in seiner Stellungnahme vom 8. September 2020 festgehalten hat, dass die Swiss-US Privacy Shield Zertifizierung keine ausreichende Garantie für einen Datentransfer in die USA gewährleiste, sind vertragliche Garantien bei Datentransfers in die USA genau zu prüfen.

VII. KOMPETENZEN EDÖB UND SANKTIONEN

Mit dem revidierten Datenschutzgesetz wurden die Kompetenzen des EDÖB (Eidgenössischer Daten- und Öffentlichkeitsberater) ausgebaut. Bisher konnte dieser lediglich Empfehlungen aussprechen. Neu ist er berechtigt, verbindliche Verfügungen zu erlassen und Massnahmen anordnen (Art. 50 und 51 revDSG). Die Kompetenz, fehlbare Verantwortliche zu büssen, obliegt allerdings allein den kantonalen Strafverfolgungsbehörden (Art. 65 Abs. 1 revDSG). Die Maximalbusse liegt neu bei CHF 250’000.00 (Art. 60, 61 und 63 revDSG) und richtet sich gegen die verantwortliche natürliche Person (und damit nicht gegen das Unternehmen).

22. Januar 2021 / MLaw Simone Küng