Beilage 3:

Wichtigste neue Regelungen des Bundesgesetzes über den Datenschutz (Datenschutzgesetz, DSG), Totalrevision

Das neue Schweizer Datenschutzrecht bringt zahlreiche Neuerungen mit sich, von denen die wichtigsten nachfolgend erläutert werden.

1. Anwendungsbereich: Auswirkungsprinzip, Vertretung und keine Daten juristischer Personen

Im neuen Datenschutzgesetz (nDSG) bestimmt sich der räumliche Geltungsbereich neu explizit nach dem sogenannten **Auswirkungsprinzip.** Das heisst, das Gesetz wird auch für Unternehmen mit Sitz im Ausland anwendbar sein, wenn diese Personendaten bearbeiten und sich diese Datenbearbeitung in der Schweiz auswirkt. Für die zivil- und strafrechtliche Durchsetzung bleiben aber die bisherigen Grundsätze bestehen.

Neu können Unternehmen ohne Sitz in der Schweiz zudem dazu verpflichtet sein, eine **Vertretung in der Schweiz** zu bezeichnen, wenn sie Personendaten von Personen in der Schweiz bearbeiten. Diese Pflicht wird ausgelöst, wenn die Datenbearbeitung im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen (sogenannte Angebotsausrichtung) oder der Verhaltensbeobachtung dieser Personen steht. Zudem muss es sich um eine umfangreiche und regelmässige Bearbeitung handeln, die ein hohes Risiko für die Persönlichkeit der betroffenen Personen mit sich bringt.

Nicht mehr anwendbar ist das nDSG künftig auf **Daten juristischer Personen.** Damit wird diese Schweizer Besonderheit erfreulicherweise abgeschafft. Die Auswirkungen in der Praxis sollten aber nicht überschätzt werden, erfolgt doch beispielsweise auch im B2B-Verkehr regelmässig eine Bearbeitung von Daten natürlicher Personen (zum Beispiel der Ansprechpartner).

2. Neue besonders schützenswerte Personendaten

Die Definition der besonders schützenswerten Personendaten wurde gegenüber dem geltenden Bundesgesetz über den Datenschutz (DSG) erweitert und umfasst künftig auch Daten über die **Ethnie, genetische Daten sowie biometrische Daten, die eine natürliche Person eindeutig identifizieren.** Die einzelnen Kategorien führten zu vielen Diskussionen (zum Beispiel Streichung gewerkschaftlicher Daten und Massnahmen der sozialen Hilfe) und waren teilweise bis zum Schluss umstritten (zum Beispiel Einschränkung der genetischen Daten). Die Kategorie der «Persönlichkeitsprofile», für welche bisher die gleich strengen erhöhten Anforderungen galten wie für besonders schützenswerte Personendaten, wird ferner im nDSG nicht enthalten sein (vgl. aber die Regelung zum Profiling unten).

3. Regelung des Profilings

Das revidierte DSG enthält neu eine Legaldefinition des Profilings, die derjenigen der Datenschutz-Grundverordnung der EU (DSGVO) entspricht und im bisherigen DSG nicht enthalten war.
Als **Profiling** gilt demnach:

> *«[…] jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen*.»

Für private Verantwortliche wird eine Einwilligung oder andere Rechtfertigung für ein Profiling (mit hohem Risiko) somit nur bei einer persönlichkeitsverletzenden Datenbearbeitung erforderlich sein. Je nach Art und Umfang des Profilings kann dies allerdings relativ rasch der Fall sein, wodurch eine

Einwilligung oder ein anderer Rechtfertigungsgrund erforderlich sein wird. Da beim Rechtfertigungsgrund des überwiegenden Interesses häufig grosse Unsicherheiten bestehen, dürfte auch künftig nicht selten das Einholen einer Einwilligung zu empfehlen sein. Muss von einem «Profiling mit hohem Risiko» ausgegangen werden, dann genügt zudem nur eine ausdrückliche Einwilligung als (eventuell erforderliche) Rechtfertigung.

Das **Profiling mit hohem Risiko** war einer der Hauptstreitpunkte, an dem die DSG-Revision beinahe noch gescheitert wäre. Das Vorliegen eines Profilings mit hohem Risiko ist neben der Ausdrücklichkeit einer Einwilligung auch für den Rechtfertigungsgrund der Bonitätsprüfung relevant (siehe unten). Im revidierten DSG gilt als Profiling mit hohem Risiko:

«*Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt*.»

4. Erweiterte Informationspflicht

Die Informationspflicht wird gegenüber dem bisherigen Recht stark ausgebaut. Das nDSG enthält aber bedauerlicherweise keine abschliessende Liste aller Pflichtinformationen, die der betroffenen Person bei der Beschaffung mitgeteilt werden müssen. Es ist daher im Einzelfall zu prüfen, welche Angaben erforderlich sind, wobei eine Orientierung am Katalog der DSGVO der EU in Frage kommen könnte.

Mindestens mitzuteilen sind jedenfalls folgende **Pflichtangaben:**

- die **Identität** und die Kontaktdaten des Verantwortlichen
- die **Bearbeitungszwecke**
- bei einer Bekanntgabe von Daten: die **Empfänger** oder die Kategorien von Empfängern
- bei indirekter Datenerhebung (das heisst, wenn Daten nicht bei der betroffenen Person selbst erhoben werden) zusätzlich: die **Kategorien der bearbeiteten Personendaten**
- die Durchführung **automatisierter Einzelentscheidungen,** das heisst einer Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für die betroffene Person mit einer Rechtsfolge verbunden ist oder die betroffene Person erheblich beeinträchtigt

Im nDSG wird im Übrigen nicht geregelt, auf welche Art und Weise die Information gegenüber der betroffenen Person zu erfolgen hat. Es gilt somit zwar kein gesetzliches Formerfordernis zu beachten, es ist aber eine «angemessene» Form zu wählen, welche dem Zweck einer transparenten Datenbearbeitung gerecht wird. Eine **Datenschutzerklärung** auf der Website wird dabei aber auch nicht in jedem Fall ausreichen.

5. Ausbau der Betroffenenrechte

Im nDSG wird nicht nur die Informationspflicht erweitert, sondern es werden auch die Rechte der Betroffenen weiter ausgebaut. Neu wird ähnlich wie in der DSGVO ein **Recht der betroffenen Person auf Datenherausgabe und -übertragung** statuiert. Betroffene Personen werden verlangen können, dass die von ihnen bekanntgegebenen Daten in einem gängigen elektronischen Format herausgegeben oder an andere Anbieter übermittelt werden.

Darüber hinaus hat die betroffene Position bei automatisierten Einzelentscheidungen (siehe Punkt 4 – Erweiterte Informationspflicht) ein **Widerspruchsrecht,** wonach sie ihre Position hierzu darlegen darf und verlangen kann, dass die automatisierte Einzelentscheidung von einer natürlichen Person überprüft wird.

- **Auskunftsrecht** – das Recht, zu wissen, welche Daten ein Unternehmen sammelt und verarbeitet (siehe Punkt 4 – Erweiterte Informationspflicht)

- **Recht auf Sperrung/Einschränkung** – das Recht, Daten sperren zu lassen, wenn sie nicht für den festgehaltenen Bearbeitungszweck, zum Beispiel zur Vertragserfüllung, vorgesehen sind; gilt ebenso bei Bekanntgabe an Dritte
- **Recht auf Berichtigung** – das Recht, zu verlangen, dass Daten berichtigt werden, wenn die gesammelten Informationen nicht aktuellen Tatsachen entsprechen
- **Recht auf Löschung/Vernichtung** – das Recht, zu verlangen, dass die Daten nach Beendigung des Nutzungszweckes, zum Beispiel bei Vertragsende, gelöscht werden

6. Regelungen für konzerninterne Weitergabe von Personendaten – Konzernprivileg?

So gelten für den konzerninternen Datenaustausch unter dem nDSG zwar Ausnahmen von der Informationspflicht und dem Auskunftsrecht, trotzdem kann eine konzerninterne Weitergabe auch künftig persönlichkeitsverletzend und in diesem Fall nur bei Vorliegen eines Rechtfertigungsgrunds zulässig sein. Dabei gilt der besondere Rechtfertigungsgrund für die konzerninterne Bearbeitung nur, wenn die betreffenden Daten und die Art ihrer Bearbeitung «für den wirtschaftlichen Wettbewerb» relevant und erforderlich sind. Auch konzerninterne Bearbeitungen müssen deshalb stets im Einzelfall sorgfältig auf ihre Rechtmässigkeit geprüft werden.

7. Rechtfertigungsgrund der Bonitätsprüfung

Für die Durchführung einer Bonitätsprüfung werden in Art. 30 Abs. 2 lit. c nDSG besondere, strengere Voraussetzungen für die Annahme eines überwiegenden Interesses statuiert. Eine Bonitätsprüfung ist demnach gerechtfertigt, wenn:

- keine besonders schützenswerten Personendaten bearbeitet werden und es sich um kein Profiling mit hohem Risiko handelt
- die Daten Dritten nur bekanntgegeben werden, wenn diese die Daten für den Abschluss oder die Abwicklung eines Vertrags mit der betroffenen Person benötigen
- die Daten nicht älter als zehn Jahre sind
- die betroffene Person volljährig ist

8. Verzeichnis sämtlicher Datenbearbeitungen

Künftig wird – wie unter der DSGVO – auch nach Schweizer Recht ein Verzeichnis sämtlicher Datenbearbeitungen zu führen sein («Verzeichnis der Bearbeitungstätigkeiten»). Das Führen eines Datenbearbeitungsverzeichnisses wird für die meisten Unternehmen mutmasslich zum grössten Aufwand bei der Umsetzung führen, falls nicht bereits entsprechende Massnahmen für die DSGVO-Compliance getroffen wurden. Der **grosse Aufwand** folgt daraus, dass sämtliche Datenbearbeitungen des gesamten Unternehmens erfasst und genaue Angaben dazu gemacht sowie laufend aktualisiert werden müssen. Der Mindestinhalt dieses Bearbeitungsverzeichnisses ist gesetzlich sowohl für den Verantwortlichen als auch den Auftragsbearbeiter vorgegeben.

Das Bearbeitungsverzeichnis des Verantwortlichen muss folgende **Mindestangaben** enthalten:

- die Identität des Verantwortlichen
- den Bearbeitungszweck
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten
- die Kategorien der Empfängerinnen und Empfänger
- «wenn möglich» die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer
- «wenn möglich» eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit (geeignete technische und organisatorische Massnahmen, die es ermöglichen, Verletzungen der Datensicherheit zu vermeiden)
- falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien, durch die ein geeigneter Datenschutz gewährleistet wird

9. Weitere neue Pflichten des Verantwortlichen

Ebenfalls neu aufgenommen wurden verschiedene weitere Pflichten, die mit der Bearbeitung von Personendaten einhergehen:

- **Data-Breach-Notification:** Verletzungen der Datensicherheit (zum Beispiel Datenverluste), die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen, sind unverzüglich dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und gegebenenfalls der betroffenen Person zu melden.

- **Datenschutz-Folgenabschätzungen:** Wenn eine beabsichtigte Datenbearbeitung ein hohes Risiko einer Verletzung der Persönlichkeit oder der Grundrechte einer betroffenen Person mit sich bringt, ist der Verantwortliche dazu verpflichtet, die Risiken einer solchen Bearbeitung in einer Datenschutz-Folgenabschätzung zu analysieren. Das nDSG geht davon aus, dass insbesondere bei der Verwendung neuer Technologien und einer umfangreichen Bearbeitung besonders schützenswerter Personendaten oder bei der systematischen Überwachung umfangreicher öffentlicher Bereiche von einem hohen Risiko ausgegangen werden muss.

- **Privacy-by-Design und Privacy-by-Default:** Wie in der DSGVO sind auch im nDSG explizit die Grundsätze des «Datenschutzes durch Technik» und des «Datenschutzes durch datenschutzfreundliche Voreinstellungen» verankert. Bei der Verarbeitung von Personendaten müssen «ab der Planung» angemessene technische und organisatorische Massnahmen getroffen werden, welche die Umsetzung von Datenschutzgrundsätzen (zum Beispiel Datenminimierung) in diesen Systemen sicherstellen (Privacy-by-Design). Auch die Voreinstellungen, beispielsweise bei Apps oder Websites, sind so auszugestalten, «dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist» (Privacy-by-Default).

10. Verschärfung der Sanktionen und Ausbau der Befugnisse des EDÖB

Das nDSG sieht strafrechtliche Sanktionen in Form einer **Busse von bis zu CHF 250’000** vor. Darüber hinaus kann der EDÖB ein verwaltungsrechtliches Untersuchungsverfahren eröffnen und Verfügungen erlassen. Auch wenn der EDÖB selbst keine Sanktionen anordnen kann, drohen auch bei Missachtung einer Anordnung des EDÖB, also beispielsweise bei der Weiterbearbeitung von Daten trotz Verbot, Strafsanktionen in der gleichen Höhe. Zuständig für die Durchsetzung der strafrechtlichen Sanktionen werden die kantonalen Strafverfolgungsbehörden sein. Möglich sind schliesslich weiterhin auch zivilrechtliche Klagen auf Beseitigung, Unterlassung oder Schadenersatz.

Im Gesetzgebungsverfahren wurde zum Ausdruck gebracht, dass die strafrechtlichen Sanktionen hauptsächlich auf **Leitungspersonen** und nicht auf die ausführenden Mitarbeitenden abzielen. Zugleich wurde aber nicht gänzlich ausgeschlossen, dass es auch Fälle geben kann, in welchen die Sanktion Mitarbeitenden ohne Leitungsfunktion auferlegt werden könnte. Bei Widerhandlungen, bei denen höchstens eine Busse von CHF 50’000 in Betracht kommt und der Aufwand zur Ermittlung der strafbaren Person innerhalb des Geschäftsbetriebs unverhältnismässig wäre, kann schliesslich auch das Unternehmen anstelle der natürlichen Person zur Zahlung der Busse verurteilt werden.

Ausblick

Mit der Annahme des Schlussabstimmungstexts durch beide Räte steht somit fest, welchen Vorschriften die Datenbearbeitungen der Unternehmen in der Schweiz künftig entsprechen müssen. Auf wann der Bundesrat das revidierte DSG in Kraft setzen wird, ist allerdings noch unklar. Bis der Bundesrat das Datum des Inkrafttretens mitteilt, wird aber noch das Ablaufen der Referendumsfrist (14. Januar 2021) abzuwarten sein. Das konkrete Datum hat insbesondere deshalb grosse Bedeutung, weil im **nDSG keine Übergangsfristen** vorgesehen sind. Vor diesem Hintergrund empfiehlt sich, die entsprechenden Compliance-Projekte rasch voranzutreiben oder allerspätestens jetzt zu lancieren

Quelle: Auszug aus Newsletter Anwaltskanzlei Meyerlustenberger Lachenal (MLL), 19. Oktober 2020