

NEWS

NEUES DATENSCHUTZGESETZ FÜR DIE SCHWEIZ

Ein wichtiges Ziel der Revision war, ein mit der Datenschutzgrundverordnung der EU („DSGVO“) gleichwertiges Schutzniveau sicherzustellen. Dies ist notwendig, damit die Schweiz weiterhin die Vorzüge des gegenwärtig bestehenden Angemessenheitsbeschlusses der EU-Kommission nutzen kann. Bestünde kein mit der EU gleichwertiges Schutzniveau, könnten Personendaten aus dem europäischen Wirtschaftsraum („EWR“) nur noch mit zusätzlichen Sicherheitsvorkehrungen in die Schweiz übermittelt werden. Es ist noch unklar, wann die EU-Kommission den Beschluss über die Angemessenheit des nDSG fällen wird.

WAS ÄNDERT SICH?

Die Revision führt zu keinen grundlegend anderen Anforderungen an den Umgang mit Personendaten. Unverändert bleibt, dass Datenbearbeitungen für private Unternehmen grundsätzlich zulässig sind und ein Rechtfertigungsgrund (wie z.B. die Einwilligung der betroffenen Person) nur in Ausnahmefällen (namentlich bei einem Eingriff in die Persönlichkeitsrechte) erforderlich ist. Dennoch sind zahlreiche Neuerungen zu beachten. Nachfolgend wird eine Übersicht von wichtigen Änderungen vorgelegt, welche für eine Vielzahl von Unternehmen bedeutsam sind. Ferner führt das nDSG zu Änderungen bei der Bearbeitung von Personendaten durch Bundesorgane. Diese werden vorliegend nicht dargestellt.

VERZEICHNIS DER BEARBEITUNGSTÄTIGKEITEN

Neu wird bei der Bearbeitung von Personendaten vorausgesetzt, dass der Verantwortliche (d.h. die natürliche oder juristische Person, die über den Zweck und die Mittel der Datenbearbeitung entscheidet) ein Verzeichnis der Bearbeitungstätigkeiten führt. Die gleiche Pflicht gilt für Auftragsbearbeiter, die Personendaten im Auftrag des Verantwortlichen bearbeiten. Der Mindestinhalt dieser Verzeichnisse ist gesetzlich vorgeschrieben und umfasst z.B. die Identität des Verantwortlichen,

Das Schweizer Parlament hat am 25. September 2020 das revidierte Datenschutzgesetz („nDSG“) verabschiedet. Wann das neue Gesetz in Kraft treten wird, ist offen – voraussichtlich frühestens in der zweiten Jahreshälfte 2021. Da das nDSG keine Übergangsfristen vorsieht, empfiehlt sich, rechtzeitig mit den Vorbereitungen zu beginnen.

den Bearbeitungszweck, die Kategorien betroffener Personen sowie die Kategorien bearbeiteter Personendaten. Der Bundesrat kann Ausnahmen für KMU mit weniger als 250 Mitarbeitern vorsehen, deren Bearbeitung von Personendaten höchstens ein geringes Risiko von Persönlichkeitsverletzungen mit sich bringt. Der Entwurf der Verordnung, in welcher diese Ausnahmen geregelt werden, liegt allerdings noch nicht vor. Deshalb ist noch nicht absehbar, in welchem Ausmass Unternehmen tatsächlich von dieser administrativen Verpflichtung befreit werden. Ohnehin ist die Einhaltung der datenschutzrechtlichen Vorschriften ohne eine rudimentäre Übersicht über die Bearbeitungen nur schwer möglich.

ERWEITERTE INFORMATIONSPLICHT

Das nDSG sieht ausdrücklich eine Informationspflicht bei der Beschaffung von Personendaten vor. Den betroffenen Personen müssen ausreichend Informationen zur Verfügung gestellt werden, damit die Transparenz der Datenbearbeitung sowie die Verwirklichung der Rechte der betroffenen Personen gewährleistet sind. Dies umfasst mindestens die Identität und die Kontaktdaten des Verantwortlichen sowie den Bearbeitungszweck, zu dem die Personendaten beschafft werden. Werden die Personendaten an Dritte bekannt gegeben oder ins Ausland übermittelt, sind weitere Angaben vorgeschrieben. Die vorsätzliche Verletzung dieser Pflicht kann strafrechtliche Folgen auslösen.

MELDEPFLICHT BEI VERLETZUNGEN DER DATENSICHERHEIT

Führt eine Verletzung der Datensicherheit zu einem hohen Risiko für die betroffene Person (z.B. Persönlichkeitsrechtsverletzungen), ist künftig dem eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten („EDÖB“) eine Meldung zu machen. Eine Verletzung der Datensicherheit liegt insbesondere vor, wenn Personendaten

unbeabsichtigt verlorengehen, vernichtet oder verändert oder für Unbefugte zugänglich werden. Das Gesetz legt keine feste Frist für diese Meldung fest, schreibt aber immerhin vor, dass die Meldung so rasch als möglich zu erfolgen hat. Gesetzlich vorgeschrieben ist der Mindestinhalt der Meldung: Zu melden sind namentlich die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen.

DATENSCHUTZ-FOLGENABSCHÄTZUNG

Der Verantwortliche hat eine sog. Datenschutz-Folgenabschätzung («DS-FA») zu erstellen, wenn eine geplante Bearbeitung ein hohes Risiko für Persönlichkeits- oder Grundrechtsverletzungen mit sich bringen kann. Ein hohes Risiko besteht insbesondere bei der Verwendung neuer Technologien, wenn besonders schützenswerte Personendaten (wie z.B. Gesundheitsdaten) umfangreich bearbeitet werden (z.B. bei einem medizinischen Forschungsprojekt) oder wenn systematisch umfangreiche öffentliche Bereiche überwacht werden (z.B. eine Bahnhofshalle). Die DS-FA muss neben der Beschreibung der geplanten Bearbeitung eine Bewertung der Risiken sowie die geplanten Schutzmassnahmen enthalten. Verbleibt bei der geplanten Bearbeitung trotz der Schutzmassnahmen ein hohes Risiko, so ist sie dem EDÖB vorzulegen. Falls der EDÖB Einwände gegen die geplante Bearbeitung erhebt, schlägt er dem Verantwortlichen geeignete Schutzmassnahmen vor. Da der EDÖB für seine Rückmeldung zwei Monate (bei komplexen Bearbeitungen gar drei Monate) Zeit hat, empfiehlt sich, eine allfällige DS-FA frühzeitig in Angriff zu nehmen.

VERTRETUNG IN DER SCHWEIZ

Das nDSG sieht unter gewissen Voraussetzungen eine Pflicht für ausländische Unternehmen vor, eine Vertretung in der Schweiz zu bestellen. Die Vertretung dient als Anlaufstelle für die betroffenen Personen und den EDÖB. Die Pflicht besteht jedoch nur, wenn mehrere Anforderungen kumulativ erfüllt sind: Das ausländische Unternehmen muss seine Tätigkeit auf die Schweiz ausrichten und in diesem Zusammenhang regelmässig und in grossem Umfang Personendaten bearbeiten. Gleichzeitig muss durch die Bearbeitung ein hohes Risiko für Persönlichkeitsrechtsverletzungen bestehen. Diese Anforderungen (und die damit verbundene Pflicht zur Vertreterbestellung) werden nur in Einzelfällen erfüllt sein.

RECHTE DER BETROFFENEN PERSON

Das nDSG sieht zusätzliche Rechte für die betroffenen Personen vor. Zu erwähnen sind namentlich das Recht auf Datenherausgabe und -übertragung (sog. Datenportabilität) sowie die Informations-

pflicht bei automatisierten Einzelentscheidungen. Das Recht auf Datenportabilität erlaubt es der betroffenen Person, vom Verantwortlichen kostenlos die Herausgabe ihrer Personendaten (die sie dem Verantwortlichen bekannt gegeben hat) in einem gängigen (maschinenlesbaren) Format zu verlangen. Ebenso kann die betroffene Person verlangen, dass die Personendaten an einen anderen Verantwortlichen übertragen werden. Vorausgesetzt ist, dass der Verantwortliche die Daten automatisiert (d.h. nicht analog) bearbeitet und die Personendaten in unmittelbarem Zusammenhang mit einem Vertrag mit der betroffenen Person oder gestützt auf die Einwilligung der betroffenen Person bearbeitet werden. Mögliche Anwendungsbereiche dieser Bestimmung sind z.B. der Wechsel der Bank oder des Versicherungsanbieters. Die betroffene Person kann verlangen, dass die vorhandenen Personendaten direkt dem neuen Dienstleister weitergegeben werden. Für das Unternehmen bedeutet dieses Recht, dass die technischen Voraussetzungen zur Erfüllung dieses Rechts geschaffen werden müssen.

Weiter wird eine Informationspflicht für Entscheidungen geschaffen, die ausschliesslich auf einer automatisierten Bearbeitung von Personendaten beruhen. Der Verantwortliche hat die betroffene Person zu informieren, wenn die Entscheidung die betroffene Person erheblich beeinträchtigen kann oder die Entscheidung „mit einer Rechtsfolge verbunden ist“. Eine derartige Rechtsfolge liegt namentlich im Abschluss oder der Kündigung eines Vertrags. Es ist zu erwarten, dass der EDÖB Richtlinien oder Merkblätter zur Erläuterung dieser unbestimmten Rechtsbegriffe veröffentlichen wird. Bis diese vorliegen, empfiehlt es sich, im Zweifelsfall die betroffenen Personen zu informieren.

DURCHSETZUNG UND SANKTIONEN

Um die Einhaltung der datenschutzrechtlichen Pflichten sicherzustellen, wurden die strafrechtlichen Sanktionen merklich ausgebaut. Verletzungen von Datenschutzbestimmungen können künftig mit Bussen bis zu CHF 250'000 bestraft werden (gegenüber vorher CHF 10'000). Die strafrechtliche Verantwortlichkeit richtet sich gegen die natürliche Person, welche die Verletzung begeht. Ebenfalls strafbar machen können sich die leitenden Organe von Unternehmen, die es vorsätzlich oder fahrlässig in Verletzung einer Rechtspflicht unterlassen, die Widerhandlung zu unterbinden. Gegebenenfalls kann die Busse auch der juristischen Person auferlegt werden. Die Strafverfolgung obliegt den Kantonen.

Gleichzeitig erhält der EDÖB erhält neue Kompetenzen. Sein Einflussbereich ist nicht mehr

auf wenige Themenbereiche beschränkt, sondern er kann bei sämtlichen Datenschutzverletzungen tätig werden. Zusätzlich kann der EDÖB künftig verbindliche Verfügungen erlassen und den Verantwortlichen befehlen, dass eine Datenbearbeitung angepasst oder eingestellt wird und die betroffenen Personendaten zu löschen sind. Die vorsätzliche Missachtung solcher Verfügungen können strafrechtlich verfolgt werden.

WAS IST ZU TUN?

Der Handlungsbedarf zur Umsetzung des nDSG wird regelmässig merklich geringer sein, wenn ein Unternehmen bereits die Anforderungen der DSGVO umgesetzt hat. Für diesen Fall können die bestehende internen Datenschutz-Rahmenbedingungen an die Besonderheiten des nDSG angepasst werden, was nur punktuelle Änderungen erfordert. Ausländische Unternehmen haben zu prüfen, ob eine Vertretung in der Schweiz zu bestellen ist.

Wurden noch keine entsprechenden Rahmenbedingungen erarbeitet (oder steht ohnehin eine periodische Überprüfung an), ist in einem ersten Schritt zu prüfen, welche Personendaten im Unternehmen auf welche Weise bearbeitet werden (sog. „Data Mapping“). Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbar natürliche Person beziehen. Unter den Begriff fallen also z.B. Informationen über Mitarbeiter, Kunden und Kontaktpersonen bei Lieferanten sowie Besucher der Website. Im Gegensatz zum geltenden Datenschutzgesetz sind Personendaten juristischer Per-

sonen künftig nicht mehr durch das nDSG erfasst. Die Ergebnisse des Data Mapping sind in einer Übersicht (dem Verzeichnis der Bearbeitungstätigkeiten) darzustellen, periodisch zu überprüfen und gegebenenfalls anzupassen. Gestützt auf die Übersicht ist weiter zu prüfen, ob sämtliche benötigten Dokumente erstellt und die erforderlichen Prozesse dokumentiert sind. Zu prüfen sind mindestens die folgenden Aspekte:

- Auftragsbearbeiter, die vom Verantwortlichen mit der Bearbeitung von Personendaten betraut wurden (bestehen schriftliche Verträge, und erfüllen diese die Anforderungen des nDSG?).
- Datentransfers ins Ausland (erfolgen Transfers in Länder ohne ausreichendes Schutzniveau nur mit angemessenen Schutzmassnahmen?).
- Datenschutzerklärung (werden sämtliche Bearbeitungen von Personendaten abgedeckt und erfüllt diese Information die Mindestanforderung des nDSG?).
- Besteht ein Prozess zur Erfüllung der Meldepflicht bei Verletzungen der Datensicherheit?
- Besteht ein Prozess zur Durchführung von Datenschutz-Folgeabschätzungen?
- Ist sichergestellt, dass Anfragen von betroffenen Personen rechtzeitig und vollständig bearbeitet werden können?



CHRISTOPH GASSER
Rechtsanwalt, Dr. iur.,
LL.M. University of Michigan
Nebenamtlicher Richter am
Bundespatentgericht
Partner | Zürich



THIERRY BURNENS
Rechtsanwalt, M.A. HSG, CIPP/E
Associate | Zürich



STEPHANIE VOLZ
Rechtsanwalt, Dr. iur.
Associate | Zürich

BIANCHISCHWALD GMBH
mail@bianchischwald.ch
bianchischwald.ch

GENÈ
5, rue Jacques-Balmat
Postfach 5839
CH-1211 Genf 11
T +41 58 220 36 00
F +41 58 220 36 01

ZÜRICH
St. Annagasse 9
Postfach 1162
CH-8021 Zürich
T +41 58 220 37 00
F +41 58 220 37 01

LAUSANNE
12, avenue des Toises
Postfach 5410
CH-1002 Lausanne
T +41 58 220 36 70
F +41 58 220 36 71

BERN
Elfenstrasse 19
Postfach 1208
3000 Bern 16
T +41 58 220 37 70
F +41 58 220 37 71