BRANDI
RECHTSANWÄLTE

REVISION DES DATENSCHUTZGESETZES IN DER SCHWEIZ

Informationen zum Datenschutz I März 2021

Einleitung

Da die Schweiz nicht Mitgliedstaat der EU ist, sind Unternehmen in der Schweiz nicht in gleicher Weise wie europäische Unternehmen von dem Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) umfasst. Die Verordnung kann nach Art. 3 Abs. 2 DSGVO aber auch auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der EU befinden, Anwendung finden, wenn die Datenverarbeitung durch einen nicht in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeiter erfolgt. Voraussetzung hierfür ist, dass die Datenverarbeitung im Zusammenhang damit steht, Betroffenen in der EU Waren oder Dienstleistungen anzubieten oder das Verhalten von Betroffenen in der EU zu beobachten.

Durch die nationalen Gesetze in der Schweiz werden sowohl zentrale Grundgedanken aus dem europäischen Datenschutzrecht übernommen als auch eigene Regelungen aufgestellt. Das Schweizer Parlament hat am 25.09.2020 die Revision des schweizerischen Datenschutzgesetzes (Bundesgesetz über den Datenschutz, DSG) verabschiedet. Der Text ist auf der Internetseite des Schweizer Parlaments abrufbar. Da für die Geltung des neuen Datenschutzgesetzes maßgebend ist, ob eine Datenverarbeitung sich in der Schweiz auswirkt – unabhängig davon, ob sie in der Schweiz oder im Ausland veranlasst wird – können auch deutsche Unternehmen von dem Gesetz betroffen sein.

Wir haben dies zum Anlass genommen, uns gemeinsam mit Julia Bhend von der Rechtsanwaltskanzlei Probst Partner AG vertieft mit der Revision des Datenschutzgesetzes in der Schweiz auseinanderzusetzen. Wir informieren außerdem über die Auswirkungen des Gesetzes für deutsche Unternehmen und wesentliche Unterschiede der schweizerischen Regelungen zu dem in Deutschland geltenden Datenschutzrecht.

Die Probst Partner AG ist, wie BRANDI, Mitglied von PangeaNet, einem Zusammenschluss unabhängiger Rechtsanwaltskanzleien aus über 25 Ländern. Teil des Netzwerks ist eine Praxisgruppe für Datenschutz- und IT-Recht, bestehend aus Experten der beiden Rechtsgebiete aus den verschiedenen Kanzleien. Sowohl Julia Bhend als auch die Mitglieder des Datenschutzteams von BRANDI sind Teil dieser Praxisgruppe, innerhalb derer ein regelmäßiger Austausch über aktuelle Themen stattfindet.

Revision des Datenschutzgesetzes in der Schweiz – ein Überblick

Nach langer Beratung wurde im letzten Herbst das totalrevidierte Datenschutzgesetz („nDSG“) verabschiedet. Ziel der Revision war, die Gesetzgebung auf Bundesebene an das revidierte Übereinkommen SEV 108 des Europarats und die Richtlinie der Europäischen Union 2016/60 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts als Teil des Schengen-Acquis anzupassen, damit die Schweiz als Nicht-EU- aber Schengen-Mitglied ihren Schengen-Verpflichtungen nachkommen kann. Das nDSG sollte sich zudem der DSGVO „annähern“, um die weitere Anerkennung der Angemessenheit des schweizerischen Datenschutzniveaus durch die Europäische Kommission zu erreichen. Das nDSG ist zwar in vielen Aspekten inspiriert von der DSGVO. Sie ist aber keine Kopie und weicht in manchen Punkten von dieser ab.

Die **grundlegenden Prinzipien und das Regelungskonzept des schweizerischen Datenschutzrechts bleiben unverändert**. Das bedeutet, dass sich die Art und Weise, wie personenbezogene Daten im Unternehmen bearbeitet werden, durch die Revision nicht grundlegend ändert. Wie bis anhin ist für die Bearbeitung von Personendaten durch private Unternehmen **keine Einwilligung und kein anderer Rechtfertigungsgrund erforderlich**, solange die Bearbeitungsgrundsätze (Transparenz, Zweckbindung, Verhältnismässigkeit und Datensicherheit) eingehalten werden, die betroffene Person der Bearbeitung nicht widersprochen hat und Dritten keine besonders schützenswerten Personendaten mitgeteilt werden. Diesbezüglich liegt auch künftig ein **wesentlicher Unterschied zwischen dem Schweizer Datenschutzkonzept und der DSGVO**, welche für jede Datenbearbeitung eine Rechtsgrundlage verlangt.

Die grössten Auswirkungen wird das revidierte Datenschutzgesetz auf Unternehmen haben, welche die Vorschriften der DSGVO in ihrem Unternehmen (noch) nicht implementiert haben. Mit weniger Aufwand dürfen Unternehmen rechnen, die ihre Datenbearbeitungsprozesse bereits an die DSGVO angepasst haben. Gleichwohl werden gewisse Anpassungen an das Schweizer Recht erforderlich sein.

Das neue Recht tritt voraussichtlich im Jahr 2022 in Kraft. Infolge **fehlender Übergangsfrist** nach dem Inkrafttreten des Gesetzes müssen Unternehmen rechtzeitig Massnahmen zur Umsetzung des neuen Datenschutzgesetzes ergreifen.

Im Folgenden werden einzelne Neuerungen des totalrevidierten Datenschutzgesetzes vorgestellt:

1. Geltungsbereich

Das nDSG regelt die Bearbeitung von Personendaten durch Private und durch Bundesorgane. Für die Datenbearbeitungen durch die Kantone und Gemeinden gelten weiterhin die jeweiligen kantonalen und kommunalen Datenschutzgesetze.

Das nDSG knüpft bezüglich des **räumlichen Geltungsbereichs** neu ausdrücklich an das sog. **Auswirkungsprinzip** an. Massgebend für die Unterstellung ist, ob sich eine Datenbearbeitung in der Schweiz auswirkt, ungeachtet dessen, ob sie im Ausland veranlasst bzw. durchgeführt wird (Art. 3 nDSG). Wie eine Datenbearbeitung ausgestaltet sein muss, um sich in der Schweiz „auszuwirken", ist noch nicht geklärt.

Das revidierte Datenschutzgesetz beschränkt neu seinen Geltungsbereich auf Daten natürlicher Personen (Art. 2 Abs. 1 nDSG). **Daten juristischer Personen** – bislang eine Besonderheit des Schweizer Rechts – werden also durch das nDSG **nicht mehr geschützt**.

Das revidierte Datenschutzgesetz erweitert den Umfang von besonders schützenswerten Personendaten (Art. 5 lit. c nDSG) um **genetische Daten** und **biometrische Daten**, die eine natürliche Person eindeutig identifizieren.

2. Profiling

In den parlamentarischen Beratungen war die Regelung des sog. „Profiling" bis zuletzt umstritten. Als Profiling wird nach Art. 5 lit. f nDSG jede Art der **automatisierten Bearbeitung von Personendaten definiert, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte einer Person 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. Das nDSG sieht keine allgemeine Pflicht zum Einholen einer Einwilligung im Falle von Profiling vor.

Der Begriff des Profiling weicht vom bisher verwendeten Begriff der Persönlichkeitsprofile ab; wesentliche Änderungen sind damit allerdings nicht verbunden. Lediglich für ein Profiling durch ein Bundesorgan und ein Profiling mit hohem Risiko ist die **ausdrückliche Einwilligung** der betroffenen Person erforderlich (Art. 6 Abs. 7 nDSG).

Unter **Profiling mit hohem Risiko** ist ein Profiling zu verstehen, 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 Person erlaubt.

3. Auftragsdatenbearbeitung

Die Bearbeitung von Personendaten kann wie unter geltendem Recht vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter („Processor") übertragen werden (Art. 9 nDSG). Anders als die DSGVO sieht das Schweizer Recht keine ausführlichen Anforderungen für **Verträge zur Auftragsbearbeitung** vor. Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten. Neu ist die Übertragung der Bearbeitung auf einen Dritten (sog. **Unterauftragnehmer) nur mit vorgängiger Genehmigung** des Verantwortlichen zulässig.

4. Erhöhung der Transparenz

Die Informationspflichten des Verantwortlichen (insb. in Form von Datenschutzerklärungen) werden erweitert. Er muss den betroffenen Personen diejenigen Informationen mitteilen, die erforderlich sind, damit sie ihre Rechte nach dem nDSG geltend machen können und eine transparente Datenbearbeitung gewährleistet ist. Mindestens hat er ihnen **die Identität und die Kontaktdaten des Verantwortlichen, den Bearbeitungszweck sowie gegebenenfalls die Empfänger oder die Kategorien von Empfängern, denen Personendaten bekanntgegeben werden**, mitzuteilen. Werden Personendaten ins Ausland bekanntgegeben, sind zudem das **Empfängerland** und gegebenenfalls die **Garantien zum Schutz der Personendaten** mitzuteilen.

Die Informationspflicht knüpft an die „Beschaffung" an. Das heisst, dass nach Inkrafttreten des nDSG **keine erneute Informationspflicht nach dem neuen Gesetz besteht für Bestandesdaten, über die der Verantwortliche im Zeitpunkt des Inkrafttretens des nDSG bereits verfügt**.

Neu hat der Verantwortliche die betroffene Person über eine Entscheidung **zu informieren, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht** und für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt (Art. 21 nDSG). Der Verantwortliche gibt der betroffenen Person auf Antrag die Möglichkeit, ihren Standpunkt darzulegen. Zudem kann die betroffene Person **verlangen, dass die automatisierte Einzelentscheidung von einer natürlichen Person überprüft** wird. Dies gilt nicht, wenn die automatisierte Einzelentscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht und ihrem Begehren stattgegeben wird oder die betroffene Person ausdrücklich eingewilligt hat, dass die Entscheidung automatisiert erfolgt.

Die bisherige Pflicht zur Registrierung von Datensammlungen **entfällt**. Dafür sind sowohl die Verantwortlichen als auch die Auftragsbearbeiter neu verpflichtet, ein **Verzeichnis ihrer Bearbeitungstätigkeiten** zu führen (Art. 12 nDSG). Das Gesetz schreibt dessen Mindestinhalt vor. **Ausnahmen** von dieser Pflicht gelten für Unternehmen, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen und deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt. Die Ausnahmen werden in der Verordnung (die noch nicht vorliegt) noch spezifiziert werden.

5. Datenschutz-Folgenabschätzung

Auch das Schweizer Recht führt das Instrument der Datenschutz-Folgenabschätzung ein. Der Verantwortliche muss eine solche erstellen, wenn eine Bearbeitung ein **hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen** mit sich bringen kann (Art. 22 Abs. 1 nDSG). Das hohe Risiko ergibt sich – insbesondere bei Verwendung neuer Technologien – aus Art, Umfang, Umständen und Zweck der Bearbeitung. Dies ist gemäss Gesetz namentlich der Fall bei der **umfangreichen Bearbeitung besonders schützenswerter Personendaten oder wenn systematisch umfangreiche öffentliche Bereiche überwacht** werden.

Unter bestimmten Voraussetzungen kann der Verantwortliche von der Erstellung einer Datenschutz-Folgenabschätzung absehen (vgl. dazu Art. 22 Abs. 4 und Abs. 5 nDSG). Die wichtigste Ausnahme besteht für alle Datenbearbeitungen, zu denen die Verantwortlichen aufgrund gesetzlicher Bestimmungen verpflichtet sind.

Ergibt sich aus der Datenschutz-Folgenabschätzung, dass die geplante Bearbeitung trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat, so muss der Verantwortliche vorgängig die **Stellungnahme des EDÖB** einholen. Dieser hat bis zu drei Monate Zeit, um Einwände gegen die geplante Bearbeitung zu erheben und dem Verantwortlichen Massnahmen vorzuschlagen. Wenn sich der Verantwortliche nicht an diese Vorschläge hält, kann der EDÖB weitere Anordnungen treffen.

In der Praxis wird es selten zum Einbezug des EDÖB kommen. Es ist zu erwarten, dass die Datenschutz-Folgenabschätzungen regelmässig so lange angepasst werden, bis kein hohes Risiko für die betroffenen Personen mehr besteht.

6. Bezeichnung eines Schweizer Vertreters für ausländische Unternehmen

Private Verantwortliche mit Sitz oder Wohnsitz im Ausland müssen eine Vertretung in der Schweiz bezeichnen, wenn sie Daten von Personen in der Schweiz bearbeiten und die Datenbearbeitung die folgenden Voraussetzungen erfüllt: Die Bearbeitung steht im Zusammenhang mit dem Angebot von Waren und Dienstleistungen oder der Beobachtung des Verhaltens von Personen in der Schweiz; es handelt sich um eine umfangreiche und regelmässige Bearbeitung und die Bearbeitung bringt ein hohes Risiko für die Persönlichkeit der betroffenen Personen mit sich (Art. 14 nDSG).

Name und Adresse des Vertreters müssen vom Verantwortlichen – zum Beispiel in Datenschutzerklärungen – veröffentlicht werden.

Die Vertretung muss das Verzeichnis der Bearbeitungstätigkeiten führen und dient als Anlaufstelle für die betroffenen Personen zur Ausübung ihrer Rechte und für den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten („EDÖB").

7. Datenexporte ins Ausland

Die Anforderungen für die Übermittlung von Personendaten ins Ausland bleiben im Wesentlichen unverändert. Übermittlungen von Personendaten in Länder mit einer angemessenen Datenschutzgesetzgebung, namentlich in die Länder der EU, des EWR und ins Vereinigte Königreich, können künftig ohne besondere Massnahmen erfolgen, da nun auch der Schutz von Daten juristischer Personen wegfällt, den die wenigsten Länder kannten.

Die bisherige **Meldepflicht beim EDÖB** bei der Verwendung von vertraglichen Garantien fällt weg, wenn vom EDÖB vorgängig genehmigte oder anerkannte Standarddatenschutzklauseln verwendet werden.

8. Meldepflicht bei der Verletzung der Datensicherheit

Künftig muss der Verantwortliche **jede mögliche Verletzung der Datensicherheit dem EDÖB so rasch als möglich melden, sofern diese zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt** (Art. 24 nDSG).

Gleichzeitig hat der Verantwortliche – sofern kein Ausnahmetatbestand nach Art. 25 Abs. 5 nDSG erfüllt ist – **die betroffenen Personen zu informieren**, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.

Stellt der **Auftragsbearbeiter** eine Verletzung der Datensicherheit fest, muss er dies dem Verantwortlichen so rasch als möglich melden (also nicht direkt dem EDÖB oder den betroffenen Personen).

9. Betroffenenrechte

Das revidierte Datenschutzgesetz führt ein **Recht auf Datenportabilität** ein, das von der DSGVO bekannt ist. Demnach kann jede Person vom Verantwortlichen die Herausgabe ihrer Personendaten in einem gängigen elektronischen Format verlangen, wenn der Verantwortliche die Daten automatisiert bearbeitet und die Daten mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person bearbeitet werden (Art. 28 nDSG).

10. Durchsetzung des neuen Datenschutzgesetzes

Die Kompetenzen des EDÖB und die Sanktionen für die Verletzung von Datenschutzpflichten werden ausgebaut. Unter dem nDSG ist der EDÖB befugt, v**on Amtes wegen oder auf Anzeige hin** eine Untersuchung gegen ein Bundesorgan oder eine private Person zu eröffnen, wenn genügend Anzeichen dafür bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte (Art. 49 nDSG). Das Vorliegen eines „Systemfehlers" ist dafür nicht mehr erforderlich.

Stellt der EDÖB eine Verletzung von Datenschutzvorschriften fest, **kann er Unternehmen gestützt auf Art. 51 nDSG dazu verpflichten, dass die Bearbeitung ganz oder teilweise angepasst, unterbrochen oder abgebrochen wird** und die Personendaten ganz oder teilweise gelöscht oder vernichtet werden. Er kann unter gegebenen Umständen die **Bekanntgabe ins Ausland untersagen**. Weitere Anordnungen sind im Rahmen von Art. 51 Abs. 3-5 nDSG möglich. Akzeptiert der Adressat diese verbindlichen Anordnungen nicht, muss er sie beim Bundesverwaltungsgericht anfechten.

Weiterhin stehen auch **zivilrechtliche Rechtsbehelfe** zur Durchsetzung der datenschutzrechtlichen Ansprüche zur Verfügung. In diesem Zusammenhang bringt das revidierte Gesetz wesentliche **Kostenerleichterungen für die betroffenen Personen** mit sich: Einerseits kann die beklagte Partei von der klagenden Partei bei zivilrechtlichen Klagen aus dem nDSG keine Sicherstellung der Parteientschädigung mehr verlangen. Andererseits werden den Parteien weder im Schlichtungsverfahren noch im Entscheidverfahren Gerichtskosten auferlegt. Durch diese Neuerungen wird das **klägerische Kostenrisiko** erheblich gesenkt und die zivilrechtliche Durchsetzung bzw. die gerichtliche Beurteilung von Streitigkeiten aus dem nDSG dürfte mit Inkrafttreten des revidierten Datenschutzgesetzes attraktiver werden. Gleichwohl bleibt eine erhebliche prozessuale Hürde durch die **unveränderte Beweislastverteilung** bestehen, hat der Kläger doch den Beweis für die Persönlichkeitsverletzung zu führen und zudem die Beweislast für die Kausalität zwischen dieser und dem Verhalten des Beklagten zu tragen.

Die Strafbestimmungen wurden im nDSG stark ausgebaut. Strafbar sind **die vorsätzliche Verletzung** von spezifischen Pflichten: die vorsätzliche Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten (Antragsdelikt, Art. 60 nDSG), die vorsätzliche Verletzung von Sorgfaltspflichten bei der Bekanntgabe von Personendaten ins Ausland, der Beauftragung eines Auftragsbearbeiters und bei der Einhaltung der Mindestanforderungen an die Datensicherheit (Antragsdelikt, Art. 61 nDSG), die vorsätzliche Verletzung der beruflichen Schweigepflicht (Antragsdelikt, Art. 62 nDSG) oder die vorsätzliche Missachtung von Verfügungen (Art. 63 nDSG). Für ein solches Fehlverhalten sieht das nDSG **Bussen in der Höhe von maximal CHF 250'000** vor (bisher bis CHF 10'000). Dies sieht im Vergleich zum Bussenrahmen der DSGVO nach wenig aus. Die Strafbestimmungen des Schweizer Rechts **richten sich jedoch gegen die verantwortlichen natürlichen Personen**, während die Bussen gemäss der DSGVO die jeweiligen Unternehmen treffen. Nach Schweizer Recht kann statt der **natürlichen Person das Unternehmen bestraft werden**, wenn sich die verantwortliche natürliche Person innerhalb des Unternehmens nur mit einem unverhältnismässigen Untersuchungsaufwand ermitteln lässt und eine Busse von höchstens CHF 50'000 in Betracht fällt.

Unterschiede zum Datenschutzrecht in Deutschland und Auswirkungen auf deutsche Unternehmen

Das revidierte schweizerische Datenschutzgesetz nähert sich in vielen Punkten der DSGVO an, sodass zwischen dem schweizerischen und dem deutschen Datenschutzrecht insgesamt viele Gemeinsamkeiten bestehen. Es existieren jedoch auch einige Abweichungen.

Deutsche Unternehmen sollten zunächst den räumlichen Geltungsbereich des schweizerischen Datenschutzgesetzes beachten. Das Gesetz gilt für Sachverhalte, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden. Wird von einem deutschen Unternehmen eine Datenverarbeitung veranlasst oder durchgeführt, die sich in der Schweiz auswirkt, gilt demnach das Schweizer

DSG. Es empfiehlt sich insofern, die weiteren Entwicklungen hinsichtlich des bisher ungeklärten Begriffs der „Auswirkung“ im Blick zu behalten, um das geltende Recht im Einzelfall möglichst sicher bestimmen zu können.

Ein wesentlicher Unterschied zwischen dem schweizerischen Datenschutzgesetz und der DSGVO ist, dass ersteres grundsätzlich keine Rechtsgrundlage für eine Datenverarbeitung verlangt, solange die Grundsätze der Datenverarbeitung (Transparenz, Zweckbindung, Verhältnismäßigkeit und Datensicherheit) eingehalten werden, die betroffene Person der Verarbeitung nicht widersprochen hat und Dritten keine besonders schützenswerten Personendaten mitgeteilt werden. Insofern sind die Anforderungen lockerer als die der DSGVO. Soweit ein Unternehmen jedoch unter den Anwendungsbereich der DSGVO fällt, muss es deren Anforderungen dennoch beachten und kann sich nicht lediglich auf die in der Schweiz geltende weniger strenge Regelung berufen.

Entsprechendes gilt für Fälle der Auftragsverarbeitung. Für diese sieht das schweizerische Recht im Gegensatz zur DSGVO keine ausführlichen Anforderungen an Vereinbarungen zur Auftragsverarbeitung vor. Die Anforderungen an eine entsprechende Vereinbarung sind insofern geringer. Soweit Unternehmen jedoch unter den Anwendungsbereich der DSGVO fallen, müssen sie die strengeren Anforderungen einhalten. Dies gilt zum Beispiel für deutsche oder andere europäische Unternehmen, die entweder als Verantwortlicher oder als Auftragsverarbeiter in einem Auftragsverarbeitungsverhältnis mit einem schweizerischen Unternehmen stehen. Die Anforderungen finden aber auch auf schweizerische Unternehmen Anwendung, soweit diese unter Art. 3 Abs. 2 DSGVO fallen, weil sie in der EU Waren oder Dienstleistungen anbieten oder das Verhalten betroffener Personen in der EU beobachten.

Hinsichtlich der Meldepflichten im Falle von Datenschutzverletzungen sollten Unternehmen die verschiedenen Zuständigkeiten beachten. Im Anwendungsbereich der DSGVO ist eine Datenschutzverletzung der zuständigen Aufsichtsbehörde zu melden, wenn die Datenschutzverletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (Art. 33 Abs. 1 S. 1 DSGVO). Ist das Risiko voraussichtlich besonders hoch, hat der Verantwortliche grundsätzlich die betroffene Person über die Verletzung zu benachrichtigen (Art. 34 Abs. 1 DSGVO). Im Anwendungsbereich des nDSG hat der Verantwortliche Verletzungen der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen, dem EDÖB zu melden (Art. 24 Abs. 1 nDSG). Die betroffene Person ist grundsätzlich dann zu informieren, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt (Art. 24 Abs. 4 nDSG).

Private Verantwortliche mit Sitz oder Wohnsitz im Ausland müssen außerdem beachten, dass sie eine Vertretung in der Schweiz benennen müssen, wenn sie personenbezogene Daten von Personen in der Schweiz verarbeiten und die Datenverarbeitung die Voraussetzungen des Art. 14 Abs. 1 nDSG erfüllt.

Die Annäherung des schweizerischen Datenschutzgesetzes an die DSGVO soll unter anderem bewirken, dass die EU die Schweiz auch zukünftig als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt, damit die grenzüberschreitende Datenübermittlung auch künftig möglich bleibt. Angesichts der Orientierung an der DSGVO und der Stärkung des Schutzes personenbezogener Daten durch die neuen Regelungen ist zunächst davon auszugehen, dass für Datenübermittlungen in die Schweiz auch nach Inkrafttreten des nDSG von einem der EU vergleichbaren Schutzniveau in der Schweiz ausgegangen werden kann und der Angemessenheitsbeschluss der Europäischen Kommission für die Schweiz weiterhin bestehen bleibt.

Fazit

Die Revision des Schweizer Datenschutzgesetzes betrifft nicht nur Unternehmen in der Schweiz, sondern unter Umständen auch deutsche und andere europäische sowie außereuropäische Unternehmen, deren Datenverarbeitungen sich in der Schweiz auswirken. Unternehmen sollten insofern genau prüfen, welche Datenschutzbestimmungen für sie im Einzelfall anwendbar sind. In Zweifelsfällen ist der Datenschutzbeauftragte hinzuzuziehen.

Für Datenübermittlungen in die Schweiz ist angesichts der neuen Regelungen zunächst weiterhin von einem der EU vergleichbaren Datenschutzniveau in der Schweiz auszugehen. Insofern ergeben sich aus der Revision keine Änderungen.

Julia Bhend / Johanna Schmale

Kontakt:

Probst Partner AG
Rechtsanwälte | Attorneys at law
Bahnhofplatz 18, CH-8401 Winterthur
Kreuzstrasse 26, CH-8008 Zürich

www.probstpartner.ch

Julia Bhend
lic. iur., Rechtsanwältin

T +41 52 269 14 00
M julia.bhend@probstpartner.ch

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 890
F +49 521 96535 - 113
M johanna.schmale@brandi.net