Das neue Schweizer Datenschutzgesetz – Die wichtigsten Neuerungen für Unternehmen

Autorin
Daniela Fábián Masoch,
Attorney at Law, Privacy Expert CIPP E/CIPM/FIP and ISMS 27001 Lead Auditor

FABIAN PRIVACY LEGAL
www.privacylegal.ch

9. Oktober 2020

Inhaltsverzeichnis

Das Schweizer Parlament hat am 25. September 2020 das revidierte Datenschutzgesetz (DSG-neu) verabschiedet.[1] Über das Inkrafttreten entscheidet der Bundesrat nach Ablauf der 100-tägigen Referendumsfrist. Dieser Artikel fasst die wichtigsten Neuerungen für Unternehmen zusammen.[2]

At a Glance

- Die Grundkonzeption der «Erlaubnis der Datenbearbeitung mit Verbotsvorbehalt» (d.h. Verbot, wenn die Datenbearbeitung zu einer «widerrechtlichen Persönlichkeitsverletzung führt») bleibt bestehen. Eine Einwilligung für die Bearbeitung von Personendaten ist, auch bei Profiling und der Bearbeitung von besonders schützenswerten Daten, nach wie vor grundsätzlich nicht erforderlich. Auch die Grundsätze der Datenbearbeitung bleiben weitgehend unverändert.
- Juristische Personen fallen aus dem Schutzbereich heraus. Nur noch natürliche Personen unterstehen dem Schutz des DSG-neu.
- Der Geltungsbereich des DSG-neu erstreckt sich auf Sachverhalte, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden.
- Die Begriffe «Inhaber der Datensammlung», «Persönlichkeitsprofile», und «Datensammlung» wurden gestrichen, dafür die Begriffe «Profiling», «Profiling mit hohem Risiko» und «Verletzung der Datensicherheit» eingeführt. Genetische und biometrische Daten sowie Daten über die Zugehörigkeit zu einer Ethnie gehören neu zu den besonders schützenswerten Daten.
- Die Konzepte «Privacy by Design» und «Privacy by Default» sind, wie auch schon in der EU-Datenschutz-Grundverordnung (DSGVO), nun im Gesetz verankert.
- Für die Datensicherheit sind sowohl der Verantwortliche als auch der Auftragsbearbeiter verantwortlich. Ein risikobasierter Ansatz wird eingeführt.
- Die Datenbearbeitung durch Auftragsbearbeiter bleibt im Wesentlichen gleich. Neu darf der Auftragsbearbeiter einen Unterauftragnehmer für die Bearbeitung der Daten nur nach vorgängiger Genehmigung des Verantwortlichen beiziehen.
- Die Ernennung einer Datenschutzberaterin oder eines Datenschutzberaters bleibt freiwillig. Vorteile einer Ernennung können sich im Zusammenhang mit der Datenschutz-Folgenabschätzung ergeben.
- Neu müssen der Verantwortliche und der Auftragsbearbeiter ein Verzeichnis ihrer Bearbeitungstätigkeiten führen. Dieses Verzeichnis muss dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) nicht gemeldet werden (bisher musste der Inhaber von Datensammlungen seine Sammlungen grundsätzlich beim EDÖB anmelden).
- Unternehmen mit Sitz im Ausland, die Personendaten von Personen in der Schweiz bearbeiten, müssen künftig einen Vertreter in der Schweiz bezeichnen.
- Die Voraussetzungen für die Bekanntgabe von Personendaten ins Ausland bleiben im Wesentlichen gleich. Neu stellt der Bundesrat verbindlich fest, ob die Gesetzgebung eines Staates oder das internationale Organ einen angemessenen Schutz gewährleistet.
- Die Informationspflicht ist neu auf das Beschaffen jeglicher Personendaten ausgedehnt worden (bisher nur bei der Beschaffung von besonders schützenswerten Daten und Persönlichkeitsprofilen) und umfasst auch automatisierte Einzelentscheidungen.
- Der Verantwortliche muss neu bei Datenbearbeitungen mit voraussichtlich hohem Risiko für die betroffene Person eine Datenschutz-Folgenabschätzung durchführen.
- Der Verantwortliche muss künftig Verletzungen der Datensicherheit dem EDÖB melden.

[1] Schlussabstimmungstext DSG
[2] Auf die spezifischen Bestimmungen zur Datenbearbeitung durch Bundesorgane wird hier nicht eingegangen.

- Betroffene Personen haben neu ein Recht auf Datenherausgabe oder -übertragung (Datenportabilität).
- Der EDÖB erhält erweiterte Kompetenzen und kann neu eine Reihe von Verwaltungsmassnahmen verfügen.
- Die Strafbestimmungen wurden mit Bussen bis zu 250 000 Franken für private Personen (also nicht Unternehmen!) erheblich verschärft, allerdings nur für Verstösse in bestimmten Bereichen, insbesondere der Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten sowie von Sorgfaltspflichten betreffend Anforderungen an die Datenbekanntgabe ins Ausland, Beiziehung eines Auftragsbearbeiters und für Nichteinhaltung der Mindestanforderungen an die Datensicherheit. Bussen bedingen eine vorsätzliche Handlung und werden in den meisten Fällen nur auf Antrag verhängt.

Die wichtigsten Neuerungen

1. Zweck und Geltungsbereich[3]

Das DSG-neu bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden. Nach geltendem Gesetz fallen auch juristische Personen unter den Schutzzweck. Mit der Streichung der juristischen Personen aus dem Schutzbereich gleicht sich das DSG-neu der DSGVO an, welche ebenfalls nur den Schutz natürlicher Personen bezweckt.

Das DSG-neu regelt nun auch den räumlichen Geltungsbereich. Nach Art. 3 gilt das Gesetz für Sachverhalte, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden.

2. Begriffe[4]

Diverse Begriffe werden an die DSGVO angeglichen.

Der Begriff der «*Personendaten*» wird eingeschränkt auf «alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.» Als «*betroffene Person*» gelten künftig nur noch natürliche Personen, über die Personendaten bearbeitet werden.

Für die Bestimmbarkeit wird dabei weiterhin von einem «relativen Ansatz» ausgegangen. Gemäss *Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz*[5] reicht, wie auch nach geltendem Recht, die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, nicht aus, um anzunehmen, eine Person sei bestimmbar. Bereits in seiner Botschaft zum DSG von 1988[6] hielt der Bundesrat fest, dass keine Bestimmbarkeit vorliegt, wenn «der Aufwand für die Bestimmung der betroffenen Personen derart gross ist, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird». «Vielmehr muss die Gesamtheit der Mittel betrachtet werden, die vernünftigerweise eingesetzt werden können, um eine Person zu identifizieren. Ob der Einsatz dieser Mittel vernünftig ist, muss mit Blick auf die Umstände, etwa den zeitlichen und finanziellen Aufwand für die Identifizierung, beurteilt werden. Dabei sind die zum Zeitpunkt der Bearbeitung verfügbaren Technologien und deren Weiterentwicklung zu berücksichtigen. Das Gesetz gilt nicht für anonymisierte Daten, wenn eine Re-identifizierung durch Dritte unmöglich ist (die Daten wurden vollständig und endgültig anonymisiert) oder wenn

[3] Art. 1-4 DSG-neu
[4] Art. 5 DSG-neu
[5] BBl 2017 7019
[6] BBl 1988 II 444

dies nur mit einem hohen Aufwand möglich wäre, den kein Interessent auf sich nehmen würde. Das gilt ebenfalls für pseudonymisierte Daten». [7]

- Der Begriff «besonders schützenswerte Personendaten» ist um «*Daten über die Zugehörigkeit zu einer Ethnie*», «*genetische Daten*» und «*biometrische Daten, die eine natürliche Person eindeutig identifizieren*» erweitert worden. Während bei den biometrischen Daten klargestellt wurde, dass diese eine natürliche Person eindeutig identifizieren müssen, wurde dieser Zusatz bei den genetischen Daten im Differenzbereinigungsverfahren wieder gestrichen.
- Die Begriffe «Inhaber der Datensammlung», «Persönlichkeitsprofile», und «Datensammlung» wurden gestrichen. Neu werden folgende Begriffe eingeführt:
  - «*Verantwortlicher*»: private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet.
  - «*Auftragsbearbeiter*»: private Person oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.
  - «*Profiling*»: 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, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.
  - «*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.
  - «*Verletzung der Datensicherheit*»: eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

3. Grundsätze für die Datenbearbeitung

Die Grundsätze der Datenbearbeitung bleiben materiell weitgehend unverändert.

- Neu wird in Art. 6 Abs. 4 ausdrücklich geregelt, dass die Daten vernichtet oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind. Die Erfüllung dieser Verpflichtung setzt voraus, dass der Verantwortliche im Vorfeld Aufbewahrungsfristen bestimmt.
- Der Begriff «Persönlichkeitsprofil» wird durch «*Profiling*» ersetzt (siehe die Beschreibung unter «Begriffe»). Die Terminologie des Profilings war der eigentliche Knackpunkt, bei dem die Räte bis zuletzt uneinig waren und der auch in den Medien heftig diskutiert wurde. Schliesslich hat sich die Einigungskonferenz dem Antrag des Ständerates angeschlossen und die Einführung des «*Profiling mit hohem Risiko*» beschlossen (was mit dem heutigen Konzept des Persönlichkeitsprofils vergleichbar ist), mit der Konsequenz, dass bei dieser Art von Profiling die Einwilligung, sofern erforderlich, ausdrücklich erfolgen muss. Wie die Risikoprüfung beim Profiling in der Praxis erfolgen soll, wird sich zeigen müssen, für Unternehmen aber sicherlich eine Herausforderung sein.

Zu beachten ist, dass das DSG-neu kein Einwilligungserfordernis für das Profiling mit hohem Risiko einführt, sondern lediglich fordert, dass eine Einwilligung, sofern diese als Rechtfertigungsgrund nach Art. 31 DSG-neu

[7] BBl 2017 7019

überhaupt erforderlich ist, ausdrücklich erfolgen muss. Es sei daran erinnert, dass die Grundkonzeption sowohl des geltenden DSG als auch des DSG-neu anders ist als diejenige der DSGVO. Während nach der DSGVO für die Bearbeitung von personenbezogenen Daten immer ein Rechtsgrund erforderlich ist (Art. 6 und 9 DSGVO), ist die Bearbeitung von Personendaten nach dem DSG und DSG-neu grundsätzlich erlaubt, solange die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzt wird. Nach dem DSG-neu gilt demnach weiterhin das «Erlaubnisprinzip mit Verbotsvorbehalt» während nach der DSGVO das «Verbotsprinzip mit Erlaubnisvorbehalt» gilt.

4. Privacy by Design und Privacy by Default

Neu sind die Prinzipien «Privacy by Design» und «Privacy by Default» wie wir sie bereits aus der DSGVO kennen, nun auch im DSG-neu verankert. In der Praxis ist der Verantwortliche schon heute verpflichtet, die Datenbearbeitung so auszugestalten, dass die Datenschutzvorschriften und die Grundsätze der Datenbearbeitung eingehalten werden. Ausdrücklich geregelt ist nun, dass der Verantwortliche verpflichtet ist, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt (Privacy by Default).

5. Datensicherheit

Der leicht revidierte Artikel 8 DSG-neu hält fest, dass sowohl der Verantwortliche als auch der Auftragsbearbeiter verpflichtet sind, durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten. Neu wird also der risikobasierte Ansatz eingeführt. «Je grösser das Risiko einer Verletzung der Datensicherheit, umso höher sind die Anforderungen an die zu treffenden Massnahmen».[8] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.

6. Datenbearbeitung durch einen Auftragsbearbeiter

Art. 9 DSG-neu übernimmt im Wesentlichen den geltenden Artikel 10a DSG. Der unglückliche Begriff «Dritte» wird mit «*Auftragsbearbeiter*» ersetzt. Die Bearbeitung von Personendaten kann nach wie vor vertraglich oder durch Gesetz einem Auftragsbearbeiter übertragen werden, wenn (a) die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte, und (b) keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten. In Anlehnung an die DSGVO muss ein Auftragsbearbeiter nun die Genehmigung des Verantwortlichen einholen, bevor er einen Unterauftragnehmer für die Datenbearbeitung beizieht.

7. Datenschutzberaterin oder -berater

Verantwortliche können, müssen aber nicht, eine Datenschutzberaterin oder einen Datenschutzberater als Anlaufstelle für die betroffenen Personen und Behörden, die in der Schweiz für den Datenschutz verantwortlich sind, ernennen. Die Aufgaben der Datenschutzberaterin oder Datenschutzberaters bestehen in der Schulung und Beratung des Verantwortlichen in Fragen des Datenschutzes und in der Mitwirkung bei der Anwendung der Datenschutzvorschriften.

[8] BBl 2017 7031

Anders als nach dem geltenden DSG ist die Datenschutzberaterin oder der Datenschutzberater nicht dafür verantwortlich, die betriebsinterne Einhaltung der Datenschutzvorschriften zu überwachen und ein Verzeichnis der Datensammlungen zu führen.

Private Verantwortliche, die aufgrund ihrer Datenbearbeitung Datenschutz-Folgenabschätzungen gemäss Art. 22 DSG-neu durchführen müssen, haben mit der Ernennung einer Datenschutzberaterin oder eines Datenschutzberaters einen Vorteil, sofern sie diese oder diesen konsultieren. Sie können in diesem Fall nämlich von der Konsultationspflicht des EDÖB absehen.[9] Eine Konsultation ist vorgeschrieben, wenn sich aus einer Datenschutz-Folgenabschätzung ergibt, dass die geplante Bearbeitung der Daten trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat. Voraussetzung für den Verzicht auf die Konsultationspflicht ist, dass die Datenschutzberaterin oder der Datenschutzberater (a) ihre oder seine Funktion gegenüber dem Verantwortlichen fachlich unabhängig und weisungsungebunden ausführt, (b) keine Tätigkeiten ausübt, die mit ihren oder seinen Aufgaben als Datenschutzberaterin oder Datenschutzberater unvereinbar sind, (c) über die erforderlichen Fachkenntnisse verfügt, und (d) der Verantwortliche die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters veröffentlicht und dem EDÖB mitteilt.

Verzeichnis der Bearbeitungstätigkeiten

In Anlehnung an die DSGVO müssen der Verantwortliche und Auftragsbearbeiter je ein Verzeichnis ihrer Bearbeitungstätigkeiten führen. Das DSG-neu enthält eine Auflistung der jeweiligen Mindest-Informationen, die diese Verzeichnisse enthalten müssen. Neu muss das Verzeichnis der Bearbeitungstätigkeiten nicht mehr dem EDÖB gemeldet werden.

8. Vertreter in der Schweiz

Ähnlich wie unter der DSGVO müssen private Verantwortliche mit Sitz oder Wohnsitz im Ausland unter gewissen Voraussetzungen eine Vertretung in der Schweiz bezeichnen, wenn sie Personendaten von Personen in der Schweiz bearbeiten. Die Vertretung dient als Anlaufstelle für betroffene Personen und den EDÖB. Der Verantwortliche muss den Namen und die Adresse der Vertretung veröffentlichen. Die Voraussetzungen für die Bezeichnung des Vertreters und dessen Aufgaben werden in Art. 14 und 15 DSG-neu geregelt.

9. Bekanntgabe von Personendaten ins Ausland

Nach geltendem DSG dürfen Personendaten nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. Der EDÖB führt eine Liste mit einer generellen Einschätzung über das in den aufgeführten Ländern herrschende Datenschutzniveau. Diese unverbindliche Liste entbindet den Datenexporteur jedoch nicht von seiner Verantwortung, im Einzelfall zu prüfen, ob ein Land eine Gesetzgebung hat, die einen angemessenen Schutz bietet.

Neu stellt der Bundesrat verbindlich fest, ob die Gesetzgebung eines Staates oder das internationale Organ einen angemessenen Schutz gewährleistet. Ist dies der Fall, dürfen Personendaten ins Ausland transferiert werden. Ansonsten muss der Datenschutz durch Massnahmen gewährleistet werden, wie (a) einen völkerrechtlichen Vertrag, (b) Datenschutzklauseln zwischen den Vertragsparteien, die dem EDÖB vorgängig mitgeteilt wurden, (c) Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat (hierzu gehören die EU Standardvertragsklauseln), oder (d) verbindliche unternehmensinterne Datenschutzvorschriften (sogenannte

[9] Art. 23 Abs. 4 DSG-neu

Binding Corporate Rules - BCR), die vorgängig vom EDÖB oder von einer für den Datenschutz zuständigen Behörde eines Staates, der einen angemessenen Schutz gewährleistet, genehmigt wurden (also beispielsweise die CNIL in Frankreich als Lead Authority). Der Bundesrat kann andere geeignete Garantien vorsehen. Denkbar wäre beispielsweise ein Nachfolgeabkommen des Swiss-US Privacy Shields.[10]

Abweichend von den oben genannten Grundsätzen dürfen Personendaten nur ins Ausland bekanntgegeben werden, wenn eine der Ausnahmen in Art. 17 DSG-neu vorliegt, wie beispielsweise die ausdrückliche Einwilligung der betroffenen Person.

10. Informationspflicht bei der Beschaffung von Personendaten

Die Informationspflicht wurde verschärft. Während heute eine Informationspflicht nur bei der Beschaffung von besonders schützenswerten Daten und Persönlichkeitsprofilen besteht, muss neu der Verantwortliche die betroffenen Personen über die Beschaffung von Personendaten generell informieren. Die Mindestangaben, die in der Datenschutzerklärung gemacht werden müssen, sind in Art. 19 DSG-neu geregelt, wobei unterschieden wird, ob die Daten direkt bei der betroffenen Person beschafft wurden oder indirekt durch andere Quellen. Im Vergleich zur DSGVO sind diese Mindestangaben weniger umfassend. In einem Punkt geht das DSG-neu jedoch weiter als die DSGVO: Sofern Personendaten ins Ausland bekanntgegeben werden, muss nämlich der Verantwortliche den Staat des Empfängers mitteilen.

Die Ausnahmen von der Informationspflicht wurden konkretisiert. Der private Verantwortliche kann weiterhin die Mitteilung der Information in gewissen Fällen einschränken, aufschieben oder darauf verzichten. Dies ist unter anderem möglich, wenn die überwiegenden Interessen des Verantwortlichen dies erfordern, und der Verantwortliche die Personendaten nicht an Dritte bekannt gibt, wobei Unternehmen, die zum selben Konzern gehören, nicht als Dritte im Sinne dieser Ausnahme gelten.

Neu muss der Verantwortliche grundsätzlich die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt (sogenannte «automatisierte Einzelentscheidung») informieren. Die betroffene Person kann verlangen, dass die automatisierte Einzelentscheidung von einer natürlichen Person überprüft wird. Art. 21 DSG-neu sieht entsprechende Ausnahmen vor.

11. Durchführung von Datenschutz-Folgenabschätzungen

In Anlehnung an die DSGVO muss der Verantwortliche neu vor der Datenbearbeitung eine Datenschutz-Folgenabschätzung erstellen, sofern die Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Ein hohes Risiko ergibt sich, insbesondere bei der Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung (namentlich bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten und wenn systematisch umfangreiche öffentliche Bereiche überwacht werden).

Inhalt einer Datenschutz-Folgenabschätzung bildet die geplante Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit und die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte. Art. 22 DSG-neu sieht entsprechende Ausnahmen vor. Sind mehrere ähnliche Bearbeitungsvorgänge geplant, kann eine gemeinsame Abschätzung vorgenommen werden.

[10] Am 8. September hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) festgestellt, dass der Swiss-US Privacy Shield für die Übermittlung von Personendaten aus der Schweiz in die USA nicht mehr angemessen ist (siehe dazu die Stellungnahme des EDÖB).

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 holt der Verantwortliche vorgängig die Stellungnahme des EDÖB ein. Von dieser Verpflichtung kann er absehen, wenn er eine Datenschutzberaterin oder einen Datenschutzberater nach Art. 10 DSG-neu ernannt und diese oder diesen betreffend der in Frage stehenden Bearbeitung konsultiert hat.

12. Meldung von Verletzungen der Datensicherheit

Das DSG-neu führt, wie bereits aus der DSGVO bekannt, eine Meldung von Verletzungen der Datensicherheit ein, d.h. eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

Die gute Nachricht ist, dass die Meldepflicht nach DSG-neu etwas pragmatischer als unter der DSGVO ausgestaltet ist. Der Verantwortliche ist verpflichtet, dem EDÖB *so rasch als möglich* eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, zu melden.

Anders als die DSGVO verlangt das DSG-neu für eine Meldung an den EDÖB ein *hohes Risiko* für die betroffene Person. Mit dieser Regelung soll verhindert werden, dass unbedeutende Verletzungen gemeldet werden. Es bleibt in der Verantwortung des Verantwortlichen, die Auswirkungen der Verletzung und das damit verbundene Risiko für die betroffenen Personen zu bestimmen.

Das DSG-neu schreibt im Gegensatz zur DSGVO keine bestimmte Frist vor, innert welcher die Mitteilung an den EDÖB erfolgen soll, sondern verlangt eine Meldung ab Kenntnisnahme *so rasch als möglich*. Der Verantwortliche muss schnell handeln, hat aber einen gewissen Ermessensspielraum. «Massgebend ist dabei unter anderem das Ausmass der Gefährdung der betroffenen Person. Je erheblicher die Gefährdung, je grösser die Anzahl der betroffenen Personen, umso schneller muss der Verantwortliche handeln».[11] Auch muss der Verantwortliche die betroffene Person nur dann informieren, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt. Massgebend ist, ob durch die Information die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person reduziert werden können. Dies ist insbesondere der Fall, wenn die betroffene Person entsprechende Vorkehrungen zu ihrem Schutz treffen kann, zum Beispiel, indem sie ihre Zugangsdaten oder Passwörter ändert.[12] Der Verantwortliche kann die Information an die betroffene Person unter gewissen Voraussetzungen einschränken, aufschieben oder darauf verzichten.

Der Auftragsbearbeiter hat keine eigene Meldepflicht an den EDÖB, muss aber dem Verantwortlichen so rasch als möglich eine Verletzung der Datensicherheit melden.

Art. 24 DSG-neu listet die Mindestanforderungen an die Meldung an den EDÖB auf.

13. Rechte der betroffenen Person

Auskunftsrecht: Das bisher in Art. 8 DSG geregelte Auskunftsrecht wird neu in Art. 25 DSG-neu geregelt. Der Grundsatz bleibt gleich. Der Verantwortliche teilt der betroffenen Person diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. Diese Informationen entsprechen denjenigen, die schon aufgrund der Informationspflicht mitgeteilt werden müssen. Die Mindestangaben, die aufgrund eines Auskunftsgesuchs gemacht werden müssen, werden im Gesetz aufgelistet. Neu ist die Auskunftspflicht über automatisierte Einzelentscheidungen. In diesem Fall

[11] BBl 2017 7064
[12] BBl 2017 7065

muss die betroffene Person auch über die Logik, auf der die Entscheidung beruht, informiert werden. Die betroffene Person kann verlangen, den eigenen Standpunkt zu äussern und dass die automatisierte Einzelentscheidung von einer natürlichen Person überprüft wird.

Die bisher geltenden Einschränkungen des Auskunftsrechts bestehen weiter. Neu kann ein Verantwortlicher das Auskunftsrecht «verweigern, einschränken oder aufschieben, wenn das Auskunftsgesuch offensichtlich unbegründet oder querulatorisch ist». Gemäss Botschaft[13] ist diese Ausnahme eng auszulegen. Insbesondere muss der Verantwortliche die für die betroffene Person günstigere Lösung wählen. Er muss so weit wie möglich die Auskunft lediglich einschränken, darf sie allenfalls aufschieben und kann sie nur in den absolut eindeutigen, offensichtlichen Fällen verweigern.

Recht auf Datenportabilität: Neu hat die betroffene Person unter gewissen Voraussetzungen ein Recht auf Datenherausgabe oder -übertragung.[14] Die betroffene Person kann verlangen, dass die Daten ihr oder, sofern dies keinen unverhältnismässigen Aufwand erfordert, einem anderen Verantwortlichen übertragen werden. Die Datenherausgabe muss grundsätzlich kostenlos und in einem gängigen elektronischen Format erfolgen. Die gleichen Einschränkungen wie zur Auskunftspflicht können geltend gemacht werden.

Rechtsansprüche: Die bisher geltenden Rechtsansprüche gelten weiterhin und sind in Art. 32 DSG-neu zusammengefasst. Das Recht auf Löschung oder Vernichtung wird im DSG-neu nun ausdrücklich geregelt, obwohl sich dieses implizit bereits aus dem bisherigen Recht ergibt.

14. Verwaltungsmassnahmen und Sanktionen

Dem EDÖB werden in Art. 51 DSG-neu erweiterte Kompetenzen gegeben. Neu kann er nicht nur Massnahmen empfehlen, sondern Verwaltungsmassnahmen auch verfügen. Zu diesen Massnahmen gehören beispielsweise Massnahmen gegen Datenbearbeitungen, die gegen die Datenschutzvorschriften verstossen, einschliesslich der Verfügung, Personendaten zu vernichten oder dem Verbot, Personendaten ins Ausland bekannt zu geben, sowie die Anordnung eine Datenschutz-Folgenabschätzung durchzuführen oder einer betroffenen Person die Auskünfte zu erteilen. Nach wie vor kann der EDÖB keine Bussen aussprechen. Diese Kompetenz obliegt den Kantonen.[15]

Die Strafbestimmungen wurden signifikant verschärft.[16] Neu können unter anderem private Personen (also anders als unter der DSGVO nicht Unternehmen!) auf Antrag mit Busse bis zu 250 000 Franken bestraft werden, wenn sie gegen ihre Informations- oder Auskunftspflichten verstossen oder ihre Sorgfaltspflichten verletzen, namentlich Personendaten ins Ausland bekanntgeben oder die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne die gesetzlichen Anforderungen zu erfüllen, oder die Mindestanforderungen an die Datensicherheit nicht einhalten. Wer dem EDÖB im Rahmen einer Untersuchung vorsätzlich die Mitwirkung verweigert macht sich ebenfalls strafbar.

Strafbar macht sich schliesslich auch, wer vorsätzlich eine berufliche Schweigepflicht verletzt, indem sie oder er geheime Personendaten vorsätzlich offenbart, von denen sie oder er bei der Ausübung ihres oder seines Berufes, der die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat. Mit dieser Bestimmung wird neu auch für Personen (und deren Hilfspersonen), die nicht unter das strafrechtlich sanktionierte Berufsgeheimnis fallen[17], eine Schweigepflicht eingeführt. Die Verletzung der Schweigepflicht kann auf Antrag mit einer Busse bis zu 250 000 Franken bestraft werden.

[13] BBl 2017 7069
[14] Art. 28 DSG-neu
[15] Art. 65 DSG-neu
[16] Art. 60ff DSG-neu
[17] Art. 321 Schweizerisches Strafgesetzbuch (StGB)

Schliesslich wird mit einer Busse bis zu 250 000 Franken bestraft, wer vorsätzlich eine Verfügung des EDÖB oder einer Rechtsmittelinstanz unter Strafandrohung nicht befolgt.

Zu beachten ist, dass Verstösse gegen zentrale, neu im Gesetz verankerte Pflichten, wie das Führen eines Verzeichnisses der Bearbeitungstätigkeiten, die Meldung von Verstössen gegen die Datensicherheit oder die Pflicht zur Durchführung von Datenschutz-Folgenabschätzungen, nicht im Bussgeldkatalog zu finden sind.

Umsetzungsmassnahmen

Unternehmen sollten eine Datenmanagement-Analyse durchführen und ihren Konformitätsgrad mit dem DSG-neu sowie allfällige Lücken und Risiken identifizieren. Dabei sollte der Fokus insbesondere auf folgende Bereiche gelegt werden:

- die Governance Struktur,
- Datenschutz-Standards und Prozesse zur Einhaltung der Grundsätze und Datensicherheit,
- die Transparenz gegenüber den betroffenen Personen,
- das Verzeichnis der Datenbearbeitungen,
- die Datenflüsse innerhalb des Unternehmens und an Dienstleister (wobei hier insbesondere auch auf die neuesten Entwicklungen und das Positionspapier des EDÖB geachtet werden sollte[18]),
- die Prozesse zur Durchführung von Datenschutz-Folgenabschätzungen,
- Meldungen von Datensicherheitsverletzungen an den EDÖB sowie
- die Beantwortung von Auskunftsgesuchen.

Unternehmen, welche bereits ein DSGVO Datenschutzprogramm eingeführt haben, werden einen geringeren Handlungsbedarf haben als Unternehmen, die nicht unter die DSGVO fallen oder noch keine entsprechenden Massnahmen ergriffen haben.

Viele Unternehmen werden aber ohnehin Konzepte wie Privacy by Design sowie Prozesse, die eine gesetzeskonforme Löschung oder Vernichtung der Daten und die Datenportabilität unterstützen, einführen müssen. Auch werden viele Unternehmen ihre Datenschutzerklärungen überprüfen und gegebenenfalls neu anpassen oder aber komplett neu erstellen müssen, um die Vorgaben des DSG-neu zu erfüllen. Verzeichnisse, welche heute Datensammlungen dokumentieren, werden ebenfalls neu strukturiert werden müssen, um Datenbearbeitungsvorgänge zu erfassen.

FABIAN PRIVACY LEGAL steht Ihnen bei Fragen oder Unterstützungsbedarf gerne zur Verfügung.

[18] Stellungnahme des EDÖB