IT & LAW | CONSULTING GMBH

Revision Datenschutzgesetz - Auswirkungen auf Unternehmen

SAQ Zentralschweiz

mag. iur. Maria Winkler

05. März 2021

Agenda

- **Revision DSG – Stand und Ziele**
- Wichtigste Änderungen für Unternehmen
- Wesentliche Unterschiede zur DSGVO und deren Auswirkungen
- Handlungsempfehlungen

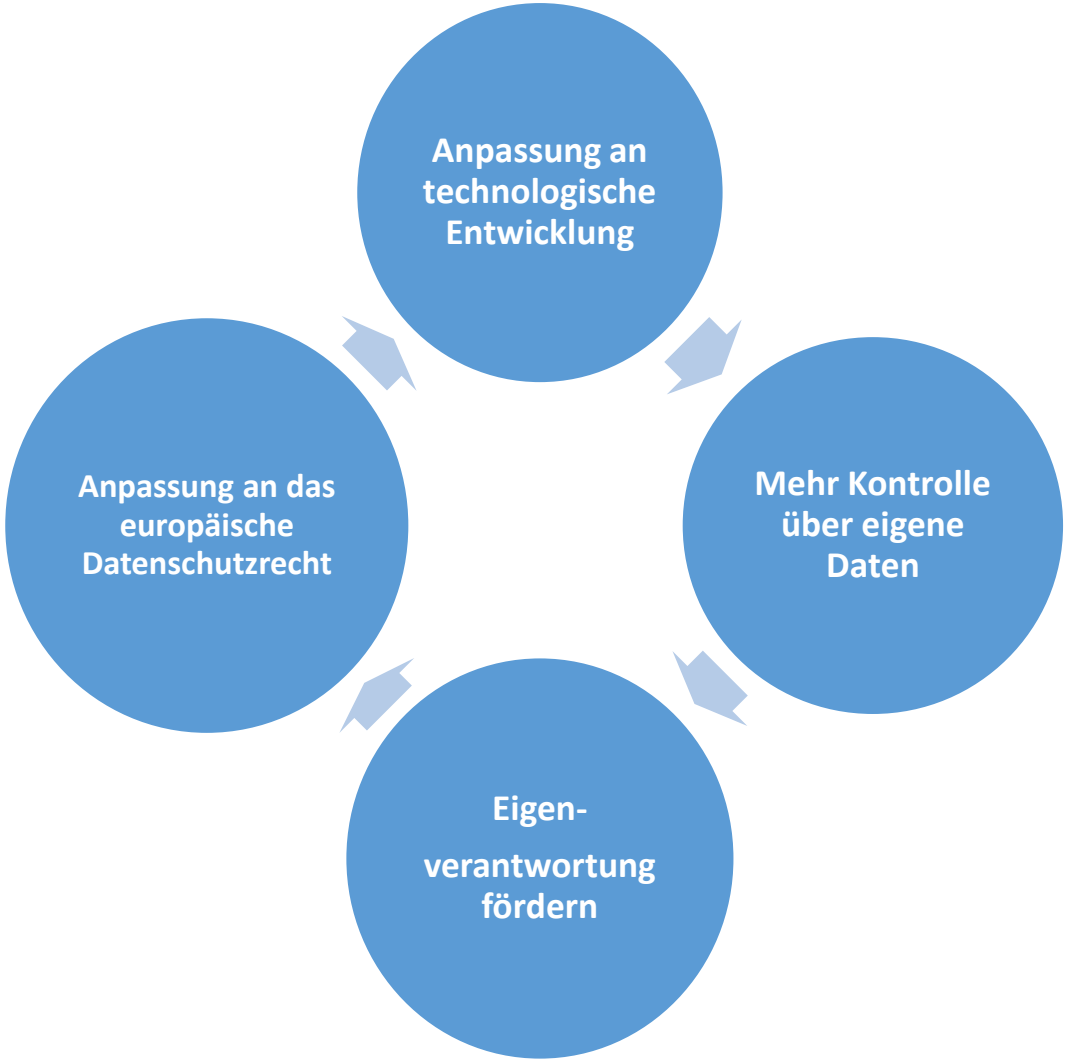
Stand Revision DSG

- Am **15. September 2017** hat der **Bundesrat** den **Entwurf** des Datenschutzgesetzes (E-DSG) veröffentlicht.
- Im gesamten Gesetzgebungsprozess wurde sehr intensiv über den Begriff **Profiling** diskutiert.
- In der **Schlussabstimmung** vom **25. September 2020** wurde die Fassung der Einigungskonferenz im Parlament angenommen (nDSG).
- Mit dem **Inkrafttreten** des **DSG** und der **Verordnungen** (VDSG und VDSZ) ist im Jahr **2022** zu rechnen.

Übergangsfristen

- Der Entwurf des Bundesrates vom 15. September 2017 sah eine zweijährige **Übergangsfrist** für Datenbearbeitungen vor, die unter bisherigem Recht begonnen wurden und nach Inkrafttreten des revidierten DSG fortgesetzt werden. Diese wurden im Verlauf der parlamentarischen Beratungen **gestrichen**.
- Sofern mit der Verordnung keine Übergangsfristen eingeführt werden, müssen, mit wenigen Ausnahmen, ab dem Inkrafttreten die neuen Anforderungen auch bei bereits laufenden Datenbearbeitungen erfüllt werden.
- Folgende **Ausnahmen** bestehen:
  - Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
  - Datenschutz-Folgenabschätzung
  - Konsultation des EDÖB

Ziele der Revision



Begriffe

Art. 5 nDSG

Neu oder geändert

- **Personendaten** bezeichnen nur mehr die Daten von natürlichen Personen
- **Besonders schützenswerte Personendaten** umfassen neu auch biometrische Daten und genetische Daten
- **Profiling** bezeichnet die automatisierte Auswertung von Personendaten, um bestimmte Verhaltensweisen zu analysieren oder vorherzusagen
- **Verantwortlicher** ist das Unternehmen, die Behörde oder private Person, die über die Mittel und Zwecke der Datenbearbeitung entscheidet
- **Auftragsbearbeiter** bearbeitet die Personendaten im Auftrag und auf Weisung des Verantwortlichen
- **Datenschutzberater** ist die neue Bezeichnung für den Datenschutzverantwortlichen

Gelöscht

- **Datensammlung** wird ersetzt durch die Verzeichnisse der Bearbeitungstätigkeiten
- **Inhaber der Datensammlung** ist neu der Verantwortliche
- **Persönlichkeitsprofil** wird gestrichen, das Profiling ist nicht gleichbedeutend mit dem Persönlichkeitsprofil (wird durch Profiling mit hohem Risiko durch die Hintertür wieder eingefügt)
- **Datenschutzverantwortlicher** wird ersetzt durch Datenschutzberater

Profiling (1/2)

(Art. 5 lit. f und g nDSG)

«Normales 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, persönlicher 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.»

Profiling (2/2)

(Art. 5 lit. f und g nDSG)

- Das Parlament diskutierte eingehend über die Definition des Profiling.
- Beim Profiling handelt es sich um einen **Datenbearbeitungsprozess**, somit um einen dynamischen Vorgang.
- Profiling ist nicht mit einem **Persönlichkeitsprofil** nach geltendem Recht identisch – letzteres ist das Ergebnis einer Datenbearbeitung.
- Profiling ist weiterhin meistens ohne **Einwilligung** erlaubt.
- Wird für ein Profiling «mit hohem Risiko» auf eine Einwilligung abgestellt, muss diese ausdrücklich erfolgen.
- **Bundesorgane** benötigen ein **formelle gesetzliche Grundlage** für Profiling.

Automatisierte Einzelentscheidung

(Art. 21 nDSG)

- Wird eine Entscheidung ausschliesslich mit automatisierten Methoden getroffen, liegt eine automatisierte Entscheidung im Einzelfall im Sinn des nDSG vor, sofern sie mit **Rechtsfolgen** für die betroffene Person verbunden ist oder diese erheblich davon beeinträchtigt wird.
- In diesem Fall muss:
  - die betroffene Person **informiert** werden
  - auf Antrag die Möglichkeit erhalten, ihren **Standpunkt** darzulegen;
  - die **Entscheidung** auf Verlangen der betroffenen Person von einer natürlichen Person **geprüft** werden.
- **Ausnahmen** bestehen bei einem unmittelbaren Zusammenhang mit dem Abschluss oder Abwicklung eines Vertrags oder bei Einwilligung der betroffenen Person.
- **Empfehlung:** Prüfen Sie, ob Sie automatisierte Entscheidungen im Einzelfall treffen.

Automatisierte Einzelentscheidung - Beispiel

(Art. 21 nDSG)

- Analysiert eine Bank die Daten ihrer Kunden mittels automatisierter Verfahren mit dem Zweck, die Kunden je nach ihrem Einkommen und Vermögen in verschiedene Kategorien «X», «Y» und «Z» einzuteilen, um ihnen dann entsprechende Werbung zuzustellen, dann handelt es sich um ein Profiling.
- Nur wenn die Entscheidung beispielsweise über einen Kreditantrag automatisiert und ohne Eingreifen des Kundenberaters bzw. der Kundenberaterin (oder eines anderen Mitarbeitenden der Bank) erfolgt, dann handelt es sich um eine automatisierte Einzelentscheidung.
- **Empfehlung:** Prüfen Sie bei der Digitalisierung von Prozessen, ob Sie automatisierte Entscheidungen im Einzelfall treffen.

Datenschutzberaterin oder –berater

(Art. 10 nDSG)

Was bleibt gleich?

- Freiwillige Ernennung durch Verantwortliche
- Anforderungen
  - Mitarbeitende oder externe Personen
  - Fachkompetenz (Datenschutzrecht, Informationssicherheit, Datenbearbeitungen)
  - Ausschluss von Interessenskonflikten
- Stellung
  - Fachliche Unabhängigkeit
  - Weisungsungebundenheit
- Verantwortung bleibt beim Verantwortlichen

Was ist neu?

- Bezeichnung als „Datenschutzberaterin oder –berater“
- Meldung der Kontaktdaten an den EDÖB
- Veröffentlichung der Kontaktdaten
  - Website
  - Datenschutzerklärung
- Befreiung von der Pflicht zur Vorlage der Datenschutz-Folgenabschätzung beim EDÖB bei verbleibendem hohem Risiko (Art. 22 Abs. 4 nDSG); siehe Ausführungen zur Datenschutz-Folgenabschätzung)

Kontaktdaten: Postadresse und Mailadresse, wobei eine allgemeine Adresse wie datenschutz@firma.ch bei der Publikation auf der Website genügen wird.

Vertretung

(Art. 14 nDSG)

- Private Verantwortliche mit Sitz oder Wohnsitz im Ausland müssen eine **Vertretung in der Schweiz** bezeichnen, wenn sie Personendaten in der Schweiz bearbeiten und eine der folgenden Voraussetzungen erfüllt ist:
  - die Datenbearbeitung steht im Zusammenhang damit, in der Schweiz Waren oder Dienstleistungen anzubieten oder das Verhalten dieser Personen zu beobachten;
  - es handelt sich um eine umfangreiche Bearbeitung;
  - es handelt sich um eine regelmässige Bearbeitung;
  - die Bearbeitung bringt ein hohes Risiko für die Persönlichkeit der betroffenen Personen mit sich.
- Die Vertretung dient als Anlaufstelle für die Betroffenen und den EDÖB.

Pflichten der Vertretung

(Art. 15 nDSG)

- Die Vertretung dient als **Anlaufstelle** des Verantwortlichen in der Schweiz:
- Die Vertretung **führt** ein **Verzeichnis** der Bearbeitungstätigkeiten **für** den **Verantwortlichen**.
- Auf Anfrage **teilt** die Vertretung dem **Beauftragten (EDÖB)** die im Verzeichnis enthaltenen Angaben mit.
- Auf Anfrage **gibt** die Vertretung den **betroffenen Personen Auskünfte** darüber, wie sie ihre Rechte ausüben können.

Bearbeitungsgrundsätze: Wird alles anders?

- **Nein.** Die Bearbeitungsgrundsätze bleiben im Wesentlichen gleich.
- Rechtmässigkeit, Transparenz, Zweckbindung und Verhältnismässigkeit der Datenbearbeitungen sowie die Richtigkeit der Daten bleiben wichtige Grundsätze.
- Datenbearbeitungen bleiben weiterhin **grundsätzlich erlaubt**. Ein Rechtfertigungsgrund (Gesetz, Einwilligung oder überwiegendes Interesse) ist wie bisher nur bei einer ansonsten persönlichkeitsverletzenden Datenbearbeitung erforderlich.
- **Bundesorgane** benötigen weiterhin für alle Datenbearbeitungen eine **gesetzliche Grundlage.**

Einwilligung

- Eine Einwilligung ist weiterhin nicht für jede Datenbearbeitung erforderlich!
- Einwilligungen können weiterhin über AGB eingeholt werden.
- Sofern eine Einwilligung überhaupt erforderlich ist, muss sie **ausdrücklich** erfolgen für:
  - die Bearbeitung von besonders schützenswerten Personendaten;
  - ein Profiling mit hohem Risiko durch eine private Person; oder
  - ein Profiling durch ein Bundesorgan

Datenminimierung

- Die Bearbeitung ist auf das **Notwendige** und **tatsächlich Erforderliche** beschränkt.
- Personendaten müssen vernichtet oder anonymisiert werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.
- Dieser Grundsatz hängt eng zusammen mit dem neu eingeführten **Privacy by Design,** wonach Systeme zur Datenbearbeitung technisch und organisatorisch so auszugestalten sind, dass sie insbesondere dem Grundsatz der Datenminimierung entsprechen.
- „Entsprechend dem Konzept der **Datenminimierung** wird eine Datenbearbeitung bereits von Beginn weg so angelegt, dass möglichst wenige Daten anfallen und bearbeitet werden oder dass Daten zumindest nur möglichst kurze Zeit aufbewahrt werden.“

(Quelle: Botschaft zum E-DSG S. 7029.)

Datenschutzrechtliche Rolle

(Art. 5 lit. j und k nDSG)

- **Verantwortlicher**: Natürliche oder juristische Personen oder Behörden, die über die Zwecke und die Mittel der Verarbeitung von personenbezogenen Daten entscheiden.
- **Auftragsbearbeiter**: Natürliche oder juristische Personen oder Behörden, die im Auftrag des Verantwortlichen solche Daten verarbeiten (Dienstleister, Provider).

Hinweise:

- Die Klärung der Rolle, die das Unternehmen bei einer Datenbearbeitung einnimmt, ist wichtig, da diese unterschiedliche Pflichten haben.
- Der Grossteil der datenschutzrechtlichen Pflichten obliegt dem Verantwortlichen.
- Die Rolle ist im Hinblick auf eine Datenbearbeitung zu bestimmen. Daher hat auch ein Auftragsbearbeiter in der Regel die Rolle eines Verantwortlichen (z.B. betr. Mitarbeiterdaten).

Auslagerung der Datenbearbeitung

Art. 9 nDSG

- Die Vorschriften für die Auslagerung von Datenbearbeitungen an Dienstleister bleiben im Wesentlichen gleich.
- Der Verantwortliche muss sicherstellen, dass
  - er mit der Auslagerung keine Geheimhaltungspflichten verletzt,
  - der Auftragsbearbeiter die Daten nur so bearbeitet wie er es selbst darf,
  - der Auftragsbearbeiter die Datensicherheit gewährleistet.
- Der Abschluss eines **schriftlichen Vertrages** ist weiterhin nicht zwingend vorgesehen, aber zu empfehlen. Darin sind Zweckbindung, Kontrollrechte und technische und organisatorische Massnahmen zu vereinbaren.
- Auftragsbearbeiter dürfen **neu** nur mit Einwilligung des Verantwortlichen **Subunternehmer** beiziehen.
- **Hinweis:** Die Verletzung dieser Vorschriften ist neu mit Strafe bedroht!

Datenbekanntgabe ins Ausland (1/2)

Art. 16 nDSG

- Personendaten dürfen ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates (oder das internationale Organ) einen **angemessenen Schutz** gewährleistet.
- Verfügt ein Land nicht über eine Gesetzgebung mit einem angemessenen Datenschutz, ist die Bekanntgabe möglich, wenn die Sicherheit der Daten durch **anderweitige Garantien** sichergestellt werden.
- **Bisher** konnten Datenübermittlungen in **unsichere Drittländer** durch die Verwendung der sog. **EU-Standardvertragsklauseln** abgesichert werden.
- Ebenbürtig «sicher» war die Datenübermittlung in die USA, wenn das US-Unternehmen Swiss-U.S. **Privacy Shield** (bzw. EU-U.S. Privacy Shield) zertifiziert war.

Datenbekanntgabe ins Ausland – Drittländer (2/2)

- Der Europäische Gerichtshof (**EuGH**) erklärte im **Urteil** zum **Schrems II** Fall das EU-U.S. Privacy Shield für ungültig.
- Die EU-Standardvertragsklauseln können weiterhin verwendet werden, setzen aber eine Risikoabwägung im Einzelfall sowie Anpassungen der Verträge und allfällige weitere Massnahmen voraus.
- Der **EDÖB** teilte am 08.09.2020 mit, dass das CH-U.S. Privacy Shield weiterhin gültig sei, dass es aber keinen angemessenen Schutz mehr biete.
- **Er schloss sich** sowohl betr. Privacy Shield als auch den EU-Standardvertragsklauseln **der Meinung des EuGH an**. Link zur Stellungnahme des EDÖB: https://www.edoeb.admin.ch/edoeb/de/home/aktuell/medien/medienmitteilungen.msg-id-80318.html

Was bedeutet das für CH-Unternehmen?

- Datenübermittlungen auf der Basis des Swiss-U.S. **Privacy Shields** in die USA verletzen das Schweizer DSG. Dies ist nach Inkrafttreten des nDSG strafbar.
- Datenübermittlungen auf der Basis der **EU-Standardvertragsklauseln** sind zulässig, es muss aber im Einzelfall geprüft werden, ob diese einen ausreichenden Schutz bieten.
- **Mögliche Massnahmen**: Anonymisierung oder Pseudonymisierung der Daten, Verschlüsselung der Daten (Schlüsselverwaltung liegt beim auslagernden Unternehmen), Anpassung der EU-Standardvertragsklauseln.
- **Empfehlung**: Der Landesbeauftragte für Datenschutz Baden Württemberg publizierte Erläuterungen, in denen er konkrete Anpassungen des Anhangs der EU-Standardvertragsklauseln empfiehlt.
- Link: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/LfDI-BW-Orientierungshilfe-zu-Schrems-II.pdf

Rechte der Betroffenen

- Betroffene Personen können verschiedene Rechte geltend machen, die das Unternehmen erfüllen muss.
- Das **Auskunftsrecht** betrifft die Information, ob das Unternehmen über die auskunftsersuchende Person bearbeitet. Diese Gesuche müssen innerhalb von 30 Tagen beantwortet werden.
- Das **Berichtigungsrecht** gibt den betroffenen Personen die Möglichkeit, die Berichtigung von falschen Personendaten zu verlangen.
- Unter gewissen Voraussetzungen besteht ein **Löschrecht** bzw. auch eine Löschpflicht. Das Unternehmen muss z.B. Personendaten, die sie nicht mehr benötigt und für deren Bearbeitung sie keinen Rechtfertigungsgrund nachweisen kann, löschen.
- **Fazit:** Die eingesetzten IT-Systeme müssen eine (kontrollierte) Berichtigung und Löschung von Daten sowie eine Abfrage der bearbeiteten Personendaten ermöglichen.

Auskunftsrecht

(Art. 25 nDSG, Art. 26 nDSG)

Geltendes Recht

- Alle über die betroffene Person in der Datensammlung vorhandenen Daten
- Verfügbare Angaben über die Herkunft der Daten
- Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens
- Kategorien der bearbeiteten Personendaten
- Kategorien der an der Sammlung Beteiligten
- Kategorien der Datenempfänger

Künftiges Recht

- **Alle Informationen, die erforderlich sind**, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist.
- **Mindestens:**
  - **Identität und die Kontaktdaten des Verantwortlichen**
  - bearbeitete Personendaten
  - Bearbeitungszweck
  - **Aufbewahrungsdauer**
  - Verfügbare Angaben über die Herkunft der Personendaten
  - Vorliegen einer **automatisierten Einzelentscheidung** sowie die Logik, auf der die Entscheidung beruht, sofern mit einer Rechtsfolge / erheblicher Beeinträchtigung verbunden ist
  - Empfänger bzw. Kategorien der Empfänger

Lösch- und Berichtigungsrecht
(Art. 6 Abs. 2 und Art. 32 nDSG)

- Betroffene können vom Verantwortlichen verlangen, dass ihre Personendaten berichtigt oder (wenn eine Berichtigung nicht möglich ist) gelöscht werden.
- **Ausnahmen** bestehen, wenn eine gesetzliche Vorschrift die Änderung (und somit auch die Löschung) verbietet oder die Personendaten für Archivzwecke im öffentlichen Interesse bearbeitet werden.
- Es gibt kein **bedingungsloses "Recht auf Vergessenwerden".** Kann der Verantwortliche einen Rechtfertigungsgrund geltend machen, dann muss er die Daten nicht löschen (z.B. gesetzliche Grundlage oder ein «überwiegendes eigenes Interesse»).
- Daten sind korrekt gelöscht, wenn sie nicht ohne unverhältnismässigen Aufwand wiederhergestellt werden können.

Recht auf Datenherausgabe und –übertragung

(Art. 28 und 29 nDSG)

- Jede Person kann vom Verantwortlichen kostenlos die **Herausgabe** ihrer **Personendaten**, die sie ihm bekanntgegeben hat, 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 Vertrages zwischen dem Verantwortlichen und der betroffenen Person bearbeitet werden.
- Die betroffene Person kann zudem vom Verantwortlichen verlangen, dass er ihre Personendaten einem anderen Verantwortlichen **überträgt**, wenn die Voraussetzungen erfüllt sind und dies keinen unverhältnismässigen Aufwand erfordert.
- Zurzeit ist noch unklar, auf welche Datenbearbeitungen diese Bestimmung tatsächlich anwendbar ist. Die Bestimmung ist jedoch sehr offen formuliert!

Informationspflichten

(Art. 19 ff. nDSG)

- **Verantwortliche** müssen die betroffenen Personen informieren, wenn sie Personendaten erheben (bei der betroffenen Person selbst oder bei Dritten).
- Bisher musste nur über die Beschaffung (Bearbeitung) von **besonders schützenswerten Personendaten oder Persönlichkeitsprofilen** informiert werden, neu muss die betroffene Person über jede **Beschaffung von Personendaten** informiert werden.
- Die Informationspflicht wird somit auf **alle Personendaten** ausgeweitet, was zu erheblichem Mehraufwand für die Unternehmen führen wird.
- Es bestehen allerdings auch Ausnahmen.

Inhalt und Form

Worüber muss informiert werden?

- Name und Kontaktdaten des Verantwortlichen
- Bearbeitungszweck
- Empfänger
- Kategorien der bearbeiteten Personendaten (falls die Daten nicht bei der betroffenen Person selbst beschafft werden)
- Bei Datenübermittlung ins Ausland das Land und bei Datenübermittlungen an eine Land ohne angemessenen Datenschutz die Massnahmen zur Gewährleistung des angemessenen Datenschutzes

Wie wird informiert?

- Keine gesetzlichen Formvorschriften.
- Üblicherweise wird in einer Datenschutzerklärung informiert.
- Die Information der betroffenen Personen auf einer Website wird in der Regel ausreichen.
- Die Person muss die Information erhalten, ohne zuerst danach fragen zu müssen.
- Mehrstufige Erklärung: In der Praxis empfiehlt es sich, zunächst eine allgemeine Information zu geben. Die betroffene Person hat aber die Möglichkeit, für einzelne Themen konkretere Informationen einzuholen (z.B. über entsprechende Links).

Verzeichnis der Bearbeitungstätigkeiten

(Art. 12 nDSG)

Grundsätze

- Ersetzt die **Meldepflicht für Datensammlungen**.
- Im Gegensatz zum geltenden Recht müssen **alle Datenbearbeitungen** dokumentiert werden.
- Es handelt sich um eine **schriftliche Darstellung der wesentlichen Informationen** zu allen Datenbearbeitungen des Verantwortlichen oder des Auftragsbearbeiters.
- Mit der Schriftform ist die **dokumentierte Form** gemeint (Textform, unabhängig vom Format).
- Es wird **nicht** verlangt, **einzelne Bearbeitungsschritte** zu beschreiben.
- Auftragsbearbeiter führen ein verkürztes Verzeichnis.
- **Bundesorgane** müssen die Verzeichnisse weiterhin melden.
- Unternehmen mit weniger als 250 Mitarbeitenden müssen keine Verzeichnisse erstellen, wenn ihre Datenbearbeitungen nur ein geringes Risiko für die betroffenen Personen haben.

Verzeichnis des Verantwortlichen

(Art. 12 Abs. 2 nDSG)

Was bleibt gleich?

- Identität (Name, Adresse)
- Bearbeitungszweck
- Kategorien der betroffenen Personen (Arbeitnehmer, Kunden)
- Kategorien der bearbeiteten Personendaten
- Kategorien der Empfängerinnen und Empfänger
  - z.B. Sozialversicherungen, Aufsichtsbehörden, Vereine
  - Begriff „Empfänger“ ist nicht definiert
  - Auftragsbearbeiter gelten neu auch als Empfänger

Was ist neu?

- Aufbewahrungsdauer (wenn möglich)
  - Mindestens Kriterien zur Bestimmung der Aufbewahrungsdauer
- Allgemeine Beschreibung der Datensicherheitsmassnahmen (wenn möglich)
  - Nur, wenn Massnahmen hinreichend genau beschrieben werden können
  - Keine detaillierte Angabe sensibler Informationen
- Bei Auslandsbekanntgabe
  - Angabe des Staates (auch „sicherer“ Staat)
  - Garantien nach Art. 16 Abs. 2 nDSG

Verzeichnis des Auftragsbearbeiters

(Art. 12 Abs. 3 nDSG)

- Identität des Auftragsbearbeiters (Name, Adresse)
- Identität **jedes Verantwortlichen** (Name, Adresse), für den die Bearbeitungen erfolgen
- Kategorien von Bearbeitungen, die für den Verantwortlichen durchgeführt werden
- Allgemeine Beschreibung der Datensicherheitsmassnahmen (wenn möglich)
- Bei Auslandsbekanntgabe Angabe des Staates und der Garantien nach Art. 16 Abs. 2 nDSG
- **Anmerkung:** Die Pflicht, alle Verantwortlichen (also der Auftraggeber) aufzuführen, ist in der Praxis sehr aufwändig.

Datenschutz-Folgenabschätzung (DSFA)

Art. 22 nDSG

Grundsätze

- Der Verantwortliche erstellt **vorgängig** eine DSFA, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann.
- Bei mehreren **ähnlichen Bearbeitungsvorgängen** kann eine DSFA erstellt werden.
- **Hohes Risiko**:
  - Berücksichtigung von Art, Umfang, Umständen und Zweck der Datenbearbeitung
  - Bei einer umfangreichen Bearbeitung besonders schützenswerter Personendaten, bei einem **Profiling mit hohem Risiko** und bei einer systematischen umfangreichen Überwachung öffentlicher Bereiche liegt immer ein hohes Risiko vor

Vorgehen

- **Stufe 1:** Klärung, ob die Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt
- **Stufe 2:** Durchführung der DSFA
  - Beschreibung der Datenbearbeitung
  - Bewertung der Risiken
  - Massnahmen zur Reduktion der Risiken
- **Stufe 3**: Konsultation des EDÖB oder des Datenschutzberaters, falls trotz der ergriffenen Massnahmen ein hohes Risiko bleibt

Konsultation des EDÖB

(Art. 23 nDSG)

- Wenn **trotz der ergriffenen Massnahmen** ein hohes Risiko für die betroffenen Personen bleibt, muss der EDÖB konsultiert werden.
- Der EDÖB nimmt innerhalb von 2 Monaten Stellung (Verlängerung auf 3 Monate möglich).
- Der EDÖB kann **Massnahmen** vorschlagen, wenn er Einwände gegen die geplante Datenbearbeitung hat. Dafür kann er dem Verantwortlichen **Gebühren** in Rechnung stellen (Art. 59 Abs. 1 lit. c nDSG).
- Der EDÖB muss nicht konsultiert werden, wenn die DSFA der Datenschutzberaterin oder dem –berater vorgelegt wurde.

Auswirkungen auf die Praxis

- Die Durchführung einer DSFA ist im Hinblick auf die präventive datenschutzrechtliche Prüfung von geplanten Datenbearbeitungen sinnvoll.
- In der Praxis wird die **Definition des hohen Risikos** ausschlaggebend dafür sein, wieviel Aufwand die Unternehmen in Zukunft mit DSFAs haben werden.
- Nicht nur die eigentliche Durchführung der DSFA sondern bereits die Klärung, ob eine solche durchgeführt werden muss und das Ergebnis dieser Prüfung, sollten **dokumentiert** werden (Schwellwertanalyse).
- An die **Form der Dokumentation** werden keine besonderen Anforderungen gestellt, weshalb sowohl die physische als auch die elektronische Form zulässig sind.

Technische und organisatorische Massnahmen

- Personendaten müssen durch angemessene technische und organisatorische Massnahmen geschützt werden. Die Angemessenheit der Massnahmen bestimmt sich insbesondere nach dem Risiko für die betroffenen Personen, dem Stand der Technik und den Kosten.
- **Privacy by Design:** Die Grundsätze des nDSG **durch geeignete Technik** sicherstellen. Z.B.:
  - rasche Pseudonymisierung oder Anonymisierung, wenn Personenbezug nicht notwendig;
  - regelmässige Löschung von Daten, wenn möglich;
  - der Betroffene gibt die zu bearbeitenden Daten selber frei (Einwilligung durch Anklicken der freizugebenden Daten).
- Datenbearbeitungen und IT-Systeme sollen so **gestaltet** werden, dass datenschutzrechtliche Grundsätze eingehalten werden.
- **Hinweis**: Die ergriffenen TOMs müssen daher periodisch geprüft und falls notwendig ersetzt werden.

Meldung von Datensicherheitsverletzungen

(Art. 24 nDSG)

- Verstösse gegen Massnahmen zur Datensicherheit müssen durch Verantwortliche dem EDÖB **gemeldet** werden, wenn sie voraussichtlich zu einem hohen Risiko für die betroffenen Personen führen.
- **Datensicherheitsverletzung**: Verletzung der Sicherheit, die dazu führt, dass Personendaten verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden (Art. 5 lit. h nDSG).
- Wenn es der EDÖB verlangt bzw. wenn es zum Schutz der betroffenen Person erforderlich ist, muss auch die betroffene Person informiert werden.
- **Auftragsbearbeiter** müssen alle Datensicherheitsverletzungen dem Verantwortlichen ohne Verzug melden.
- **Empfehlung**: Es muss ein Prozess eingeführt werden, um die Datensicherheitsverletzungen zu dokumentieren, zu bewerten und in den vorgesehenen Fällen zu melden.

Agenda

- Revision DSG – Stand und Ziele
- Wichtigste Änderungen für Unternehmen
- **Wesentliche Unterschiede zur DSGVO und deren Auswirkungen**
- Handlungsempfehlungen

Wesentliche Unterschiede nDSG – DSGVO (I)

- **Erlaubnis mit Verbotsvorbehalt:** Datenbearbeitungen sind grundsätzlich erlaubt, sofern nicht gegen das Gesetz verstossen wird.
- **Keine Rechenschaftspflicht**, normale Verteilung der der Beweislast im Datenschutz. Die Anforderungen an die Dokumentation sind daher geringer.
- **Datenschutzberater / Datenschutzberaterin:** Die Bezeichnung bleibt freiwillig, der EDÖB ist zu informieren.
- **Profiling**: Unterscheidung zwischen «normalem» Profiling und Profiling mit hohem Risiko.
- **Informationspflichten** sind nicht abschliessend definiert, der Mindestinhalt ist aber enger als in der DSGVO.

- **Verbot mit Erlaubnisvorbehalt:** Für alle Datenbearbeitungen muss eine Rechtsgrundlage vorhanden sein.
- **Rechenschaftspflicht**: Der Verantwortliche muss die Einhaltung der DSGVO nachweisen können. Hieraus resultieren umfangreiche Dokumentationspflichten.
- **Datenschutzbeauftragter:** Bei Vorliegen der Voraussetzungen von Art. 37 DSGVO (oder gemäss Bestimmungen des Mitgliedsstaates) besteht eine Pflicht zur Bezeichnung eines Datenschutzbeauftragten.
- **Profiling** wird nicht speziell nach Risiken unterteilt und löst keine unmittelbaren Rechtfolgen aus.
- **Informationspflichten** gehen weiter (Information über Rechtsgrundlagen, über Betroffenenrechte, etc.).

Wesentliche Unterschiede nDSG und DSGVO (II)

- **Meldung von Verletzungen der Datensicherheit:** So rasch als möglich, Information der betroffenen Personen nur bei hohem Risiko oder auf Verlangen des EDÖB
- **Sanktionen**: Busse von bis zu CHF 250‘000.00; bestraft werden die verantwortlichen Personen. Die Sanktionierung des Unternehmens ist als **Ausnahmebestimmung** konzipiert (Art. 64 Abs. 2 nDSG).

- **Meldung von Verletzungen der Datensicherheit:** Innerhalb von 72 Stunden ab Kenntnis Meldung an Aufsichtsbehörde. Information der betroffenen Personen bei hohem Risiko und unverzüglich.
- **Sanktionen**: Geldbussen bis zu 10 Mio. € resp. 20 Mio. € oder im Falle eines Unternehmens bis zu 2% resp. 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, **welcher der Beträge höher ist.**

Agenda

- Revision DSG – Stand und Ziele
- Wichtigste Änderungen für Unternehmen
- Wesentliche Unterschiede zur DSGVO und deren Auswirkungen
- **Handlungsempfehlungen**

Handlungsempfehlungen (I)

- Ernennen Sie allenfalls einen **Datenschutzberater** im Unternehmen und melden Sie diesen beim EDÖB.
- Erstellen Sie die **Verzeichnisse aller Datenbearbeitungen**, bei denen Sie die Rolle des Verantwortlichen haben.
- Erstellen Sie ein (verkürztes) **Verzeichnis der Datenbearbeitungen**, in denen Sie Auftragsbearbeiter sind.
- Führen Sie einen Prozess für **Datenschutz-Folgenabschätzungen** bei neuen Datenbearbeitungen ein.
- Prüfen Sie Ihre **Datenschutzerklärungen** und passen sie diese an die neuen Vorgaben an.
- Identifizieren Sie die Fälle der **Auftragsbearbeitungen** und passen Sie die Verträge an.
- Prüfen Sie, ob Daten ins **Ausland** übermittelt werden.

Handlungsempfehlungen (II)

- Führen Sie einen Prozess zur Meldung und Bearbeitung von **Datensicherheitsverletzungen** ein.
- Führen Sie einen Prozess mit Vorgaben zur Beantwortung von **Begehren betroffener Personen** ein (Auskunftsbegehren, Löschbegehren, Berichtigungsbegehren, Datenportabilität).
- Identifizieren Sie **automatisierte Einzelentscheide** und regeln Sie diese.
- Schulen Sie Ihre Mitarbeitenden.
- Planen Sie **Audits**.

Vielen Dank für Ihre Aufmerksamkeit

mag. iur. Maria Winkler
IT & Law Consulting GmbH
Sternenstrasse 18
8002 Zürich
maria.winkler@itandlaw.ch