Revision des Schweizer Datenschutzgesetzes – Ein Überblick für KMU

Datenschutzerklärung ("DSE")

Sobald planmässig Personendaten bearbeitet werden, obwohl dies gesetzlich nicht notwendig ist, müssen die hiervon betroffenen Personen vorgängig informiert werden. Dies geschieht i.d.R. über eine DSE, welche zumindest die folgenden Fragen beantworten sollte:

- Wer ist für die Datenbearbeitung verantwortlich (inkl. Kontaktdaten)?
- Welche Daten werden erhoben?
- Weshalb werden diese Daten erhoben?
- Wem geben wir die erhobenen Daten weiter?
- In welche Staaten können die Daten weitergegeben werden und gestützt auf welche rechtliche Grundlage?

Verzeichnis der Bearbeitungstätigkeiten

Um einen Überblick über die interne Datenbearbeitung zu gewinnen, bietet es sich an, ein Verzeichnis über die entsprechenden Prozesse zu erstellen. Für Unternehmen, die mind. 250 Mitarbeiter beschäftigen oder Daten bearbeiten, die ein hohes Risiko in sich bergen (bspw. umfassende Bearbeitung besonders schützenswerter Daten[1] / Hochrisiko-Profiling[2]), ist das Führen eines solchen Verzeichnisses **Pflicht**. Der Mindestinhalt wird durch Art. 12 revDSG festgelegt:

- Identität des Verantwortlichen
- Bearbeitungszweck
- Kategorien von betroffenen Personen und der bearbeiteten Personendaten
- Aufbewahrungsdauer
- Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit
- Empfängerstaaten, falls die Personendaten ins Ausland gehen, sowie Garantien zum Datenschutzniveau der betroffenen Empfängerstaaten

Auftragsdatenverarbeitungsvertrag ("ADV")

Sobald ein Dritter mit der Datenbearbeitung beauftragt wird (sog. "Auftragsdatenverarbeiter", wie z.B. IT-Provider, Cloud-Anbieter etc.), muss **zwingend** ein ADV abgeschlossen werden. Darin sollte Folgendes geregelt werden:

- Die weitergegebenen Daten dürfen nur so bearbeitet werden, wie man es selbst tun dürfte.
- Es muss sichergestellt werden, dass der Auftragsdatenverarbeiter die gesetzlichen und vertraglichen Geheimhaltungspflichten einhält.
- Sofern der Auftragsdatenverarbeiter ebenfalls Dritte zur Datenbearbeitung beiziehen möchte, bedarf dies der vorgängigen Genehmigung durch den Auftraggeber.
- Auch der Auftragsdatenbearbeiter muss angemessene Massnahmen zur Datensicherheit gewährleisten (sog. TOMs, vgl. nachstehend zu den "Sorgfaltspflichten").

Datenschutz Folgenabschätzung ("DSFA")

Sind Datenbearbeitungen geplant, die ein besonders hohes Risiko für die betroffenen Personen in sich bergen (z.B. wenn besonders schützenswerte Daten umfangreich bearbeitet werden oder wenn öffentliche Bereiche systematisch und umfassend überwacht werden), muss eine DSFA durchgeführt werden. Die DSFA hat folgenden Inhalt aufzuweisen:

- Umschreibung der geplanten Datenbearbeitung
- Bewertung der Risiken für die betroffenen Personen
- Massnahmen zum Schutz der betroffenen Personen

1 Als besonders schützenswerte Personendaten gelten Informationen zu religiösen, weltanschaulichen, politischen, gewerkschaftlichen Ansichten oder Tätigkeiten, Angaben zur Ethnie, Gesundheit, Intimsphäre oder Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen sowie genetische und biometrische Daten.
2 Ein hohes Risiko liegt vor, wenn die Persönlichkeit / die Grundrechte der betroffenen Person besonders gefährdet sind, indem das Profiling zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer Person erlaubt.

Gelangt man mittels der DSFA zum Schluss, dass trotz der geplanten Massnahmen ein hohes Restrisiko zulasten der betroffenen Personen verbleibt, so muss beim EDÖB eine Stellungnahme eingeholt werden (oder der eigene Datenschutzberater wird konsultiert).

Sorgfaltspflichten

- **Datensicherheit**: Wer personenbezogene Daten bearbeitet, muss technische (insb. IT-Sicherheitsvorkehrungen) und organisatorische Massnahmen (bspw. interne Weisungen und Kontrollen) ergreifen (sog. **TOMs**), um die Daten insbesondere vor unberechtigten Zugriffen und Verlust zu schützen. Je höher das Risiko der Datenbearbeitung eingestuft wird, desto bessere und umfassendere Massnahmen sind zu ergreifen.
- **Weitergabe von Personendaten an einen Dritten:** Werden Personendaten an Dritte weitergegeben, so muss vorgängig darüber informiert werden. Mit dem Dritten ist ein ADV abzuschliessen (siehe vorstehend zu "ADV").
- **Weitergabe von Personendaten ins Ausland**: Bei einer Weitergabe ins Ausland müssen die betroffenen Personen vorgängig informiert werden. Dabei muss auf die rechtliche Grundlage des Datenexports hingewiesen werden. Problemlos ist die Übertragung in Länder mit einem angemessenen Datenschutzniveau (vgl. Anhang I zur revDSV). Bei unsicheren Drittstaaten müssen weitere Massnahmen ergriffen werden.

Betroffenenrechte

Personen, deren Personendaten bearbeitet werden, stehen folgende Rechte zu:

- **Recht auf Auskunft** über die eigenen Daten: Die Auskunft hat grundsätzlich gratis innert 30 Tagen zu erfolgen. Die Erteilung einer falschen / unvollständigen Auskunft ist strafbar (vgl. nachstehend unter "Verantwortung").
- **Recht auf Korrektur** fehlerhafter Daten: Ist nicht klar, wer Recht hat, ist dies entsprechend zu vermerken.
- **Recht auf Löschung** der Daten: Generell gilt: Sämtliche Personendaten müssen gelöscht oder anonymisiert werden, sobald sie für den Zweck der Datenbearbeitung nicht mehr erforderlich sind.
- **Recht auf Datenherausgabe**: Unter gewissen Umständen müssen die Personendaten herausgegeben werden.
- **Widerspruchsrecht**: Im Fall von automatisierten Einzelentscheidungen (sog. "Profiling") hat die betroffene Person das Recht, dass der entsprechende Entscheid von einer natürlichen Person überprüft wird.
- **Recht auf Widerruf** einer erteilten Einwilligung: Für die Bearbeitung besonders schützenswerter Daten (insb. Gesundheitsdaten) / ein Hochrisiko-Profiling muss die betroffene Person vorgängig explizit einwilligen. Grundsätzlich kann jede erteilte Einwilligung in die Personendatenverarbeitung jederzeit widerrufen werden.

Den Betroffenenrechte stehen i.d.R. die eigenen Interessen an der Datenbearbeitung gegenüber, so dass in diesen Fällen eine Interessenabwägung zu erfolgen hat.

Privacy by Default

Allfällige Voreinstellungen zum Datenschutz (bspw. bei Cookies) müssen standardmässig auf ein Minimum eingestellt sein. Es muss der betroffenen Person freistehen, in eine weitergehende Datenbearbeitung einzuwilligen.

Berufliche Schweigepflicht

Geheime Personendaten, die im Rahmen der beruflichen Tätigkeit anvertraut wurden, müssen geheim gehalten werden. Kann dies nicht garantiert werden, muss vorab klargestellt werden, dass dies nicht der Fall ist.

Data Breach: Meldepflicht

Im Falle eines Data Breach (bspw. Datenverlust / wenn Daten Unbefugten offengelegt wurden) muss der EDÖB unverzüglich benachrichtigt werden, sofern dieser ein grosses Risiko für die Persönlichkeit oder die Grundrechte der Betroffenen birgt. Die Verletzung der Datensicherheit muss der betroffenen Person im Übrigen nur mitgeteilt werden, sofern dies zu ihrem Schutz erforderlich ist oder vom EDÖB verlangt wird.

Verantwortung

Wird gegen gewisse Bestimmungen des revDSG (insbesondere berufliche Schweigepflicht, Informations-, Auskunfts- und Sorgfaltspflichten) verstossen, so droht der verantwortlichen Person eine **Busse bis zu CHF 250'000.00**. Gebüsst wird in erster Linie die verantwortliche **natürliche Person** (nicht das Unternehmen).