Webinar Teil 2

Die neuen Pflichten im Detail

Anna Kuhn, RA Mlaw

Esther Zysset, RA Dr. iur.

Agenda

Teil 2: Die neuen Pflichten im Detail

1 Was letztes Mal geschah

2 Die neuen Pflichten im Detail (1/2)

a) Verzeichnis der Bearbeitungstätigkeiten
b) Auftragsdatenbearbeitung
c) Datentransfer ins Ausland
d) Informationspflichten

Agenda

Teil 2: Die neuen Pflichten im Detail

2 Die neuen Pflichten im Detail (2/2)

- e) Data Breach Notifications
- f) Datenschutz-Folgenabschätzung
- g) Betroffenenrechte
- h) Interne Datenschutzberaterin

3 Aufsicht und Sanktionen

4 Pro memoria: Praktische Tipps zur Implementierung

1 Was letztes Mal geschah 1/2

The Basics:

- «Personendaten» sind Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen (sehr breiter Begriff)
- Daneben gibt es «besonders schützenswerte Personendaten»
- Jeder Umgang mit Personendaten stellt eine «Datenbearbeitung» im Sinne des Gesetzes dar

1 Was letztes Mal geschah 2/2

Grundprinzipien:

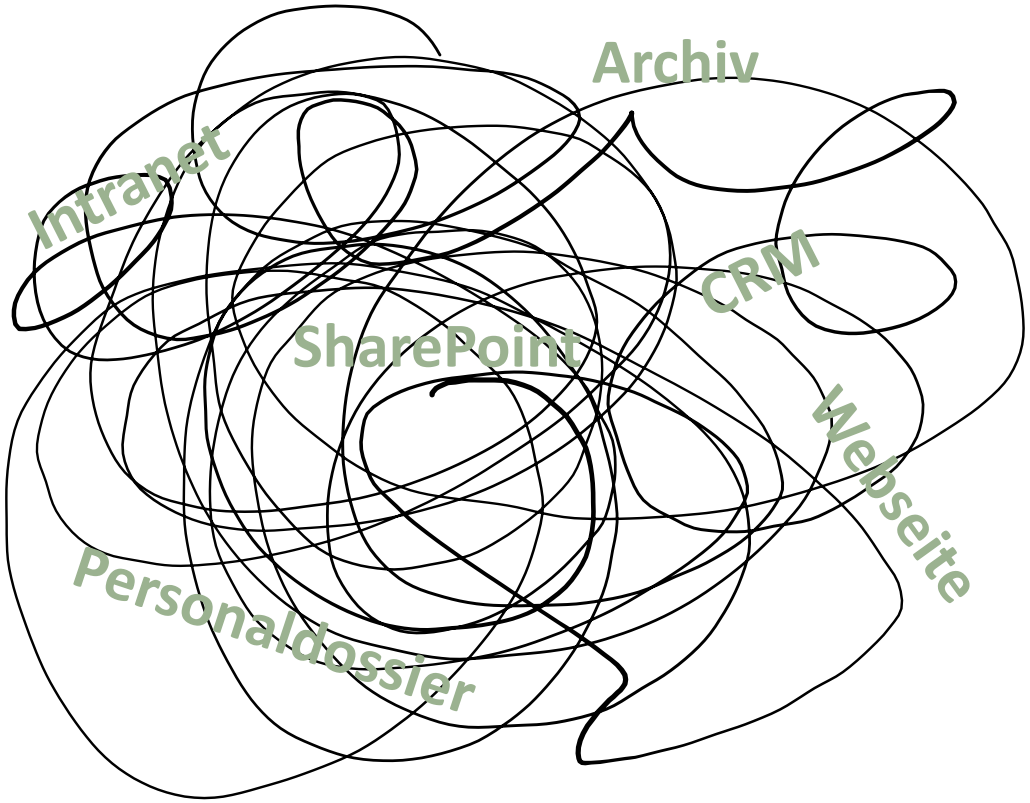
2 Die neuen Pflichten im Detail

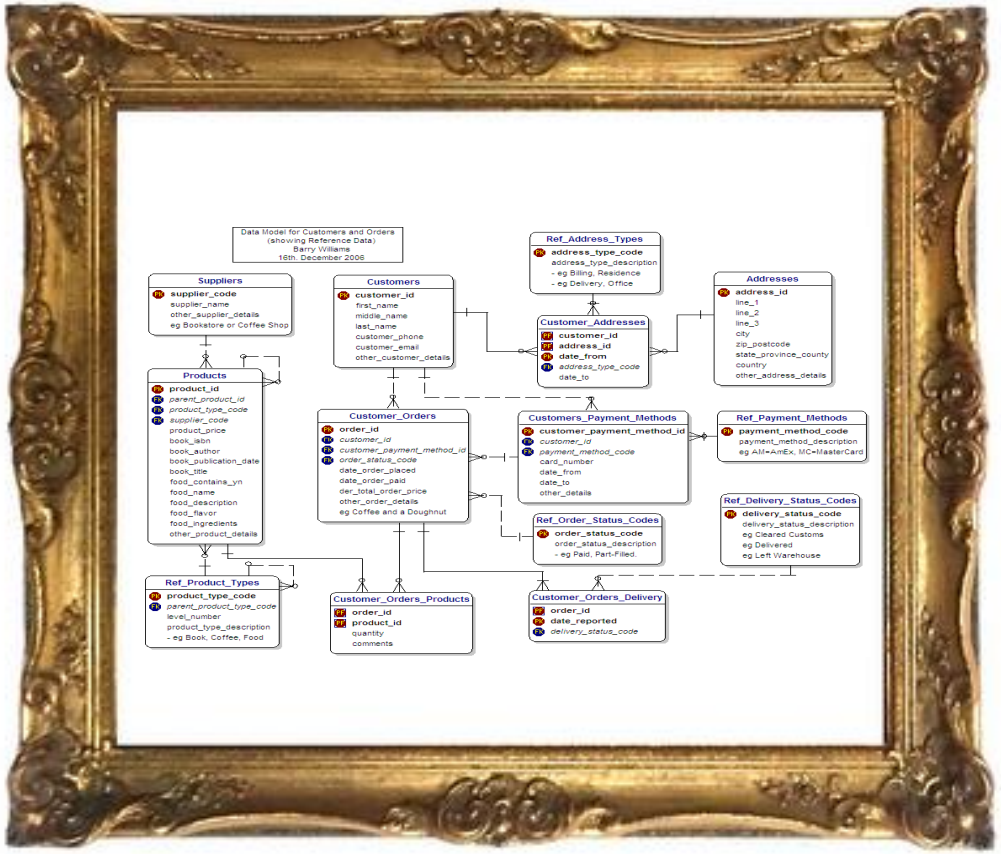
Es gibt einige . . .

a) Verzeichnis der Bearbeitungstätigkeiten
b) Auftragsdatenbearbeitung
c) Datenbekanntgabe ins Ausland
d) Informationspflichten
e) Data Breach Notifications
f) Datenschutz-Folgenabschätzung
g) Betroffenenrechte
h) Interne Datenschutzberaterin

a) Verzeichnis der Bearbeitungstätigkeiten

Vom Chaos zur Struktur!





a) Verzeichnis der Bearbeitungstätigkeiten

Es ist ein Verzeichnis der Bearbeitungstätigkeiten, d.h. mit den **wichtigsten Datenbearbeitungen**, zu erstellen (Art. 12 revDSG)

Das Gesetz legt den **Mindestinhalt** fest:

- Identität der Verantwortlichen
- Bearbeitungszweck
- Kategorien betroffener Person und bearbeiteter Daten
- Kategorien der Empfängerinnen
- Empfängerstaat bei Auslandtransfer und Schutzmassnahmen

a) Verzeichnis der Bearbeitungstätigkeiten

Ausnahmen (Art. 24 DSV):

- Unternehmen, die weniger als 250 Mitarbeitende beschäftigen
- natürliche Personen
- sofern deren Datenbearbeitungen ein **geringes Verletzungsrisiko** der Persönlichkeit der betroffenen Personen bedeuten (bspw. bei Profiling).

Bundesorgane unterliegen einer **Meldepflicht an den EDÖB** (Art. 12 Abs. 4 revDSG)

a) Verzeichnis der Bearbeitungstätigkeiten

Mögliche Datenbearbeitungen

- Rekrutierungsprozess
- Mitarbeitendenverwaltung
- Marketing
- Finanz- und Rechnungswesen etc.

Praxistipps

- Orientierung an **bestehenden Unternehmensprozessen**!
- Umsetzung mit Excel-Sheets oder **Datenschutz-Software**

b) Auftragsdatenbearbeitung

Unterscheidung zweier Rollen

Verantwortliche

- «Chefin» der Datenbearbeitung
- Kann dritte Personen beiziehen
- Muss mit diesen eine schriftliche Regelung der Auftragsdatenbearbeitung vereinbaren (ADV)
- Art. 5 lit. j revDSG

Auftragsbearbeiterin 1

Auftragsbearbeiterin 2

- Müssen sich nach den Anweisungen der Verantwortlichen richten (gemäss ADV)
- Haben selbst für die notwendige Sicherheit der Daten in ihrer Obhut zu sorgen
- Art. 5 lit. k revDSG

b) Auftragsdatenbearbeitung

Auslagerung von Datenbearbeitungen

- Beizug Software (z.B. CRM, Collaboration [Microsoft Teams], SAP)
- Hosting-Services durch Dritte (bspw. Webseite auf AWS)
- Versand Newsletter, Marketing-Services durch Agentur

Vorausgesetzt ist stets, dass die Dritten im Zusammenhang mit dem Auftrag **Personendaten bearbeiten**.

Auftragsbearbeiter darf Daten nur **weisungsgebunden** bearbeiten (Art. 9 revDSG).

b) Auftragsdatenbearbeitung

Pflicht zum Abschluss eines schriftlichen Vertrags
(Auftragsdatenbearbeitungsvertrag, «ADV» oder «DPA»)

- Umschreibung des Projekts/der Dienstleitung
- Angabe Bearbeitungszweck und Verbot, die Daten für eigene Zwecke zu benutzen (Zweckbindung)
- Pflicht, Daten nur nach Weisung der Verantwortlichen zu bearbeiten
- Pflicht zur Angabe von Unterauftragnehmerinnen und Datenstandorten sowie Genehmigungspflicht
- Pflicht zur Umsetzung geeigneter TOMs zwecks Datensicherheit
- Auditrechte und Pflichten bei Vertragsende

c) Datenbekanntgabe ins Ausland

Angemessener Datenschutz trotz Anwendbarkeit ausländischer Gesetzgebung (vgl. Art. 16 f. revDSG)

Definition Auslanddatentransfer:

- Veröffentlichung der Daten im Ausland
- Transfer an einen ausländischen Verantwortlichen (z.B. ausländische Sozialversicherungsbehörde)
- Transfer an ausländische Auftragsbearbeiterin (bspw. Verwendung Teams von Microsoft, USA)

Physischer Datentransfer wie auch **Fernzugriff** (*remote access*) erfasst.

c) Datenbekanntgabe ins Ausland

Kaskade, um angemessenes Datenschutz-Niveau herzustellen

Sicherer Drittstaat

EWR-Staaten, Andorra, Norwegen, Neuseeland etc.

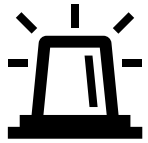
USA, China, Russland etc.

Vgl. Liste aller Drittstaaten in Anhang 1 DSV

Geeignete Schutzmassnahmen

Völkerrechtlicher Vertrag
Datenschutzklauseln (wurden EDÖB vorgelegt)
Standarddatenschutzklauseln (bspw. der EU-Kommission)
Binding Corporate Rules etc.

Ausnahmegrund



Ausdrückliche Einwilligung
Wahrung überwiegender öffentlicher Interessen
Daten wurden allgemein zugänglich gemacht
Daten aus gesetzlich vorgesehenem Register etc.

d) Informationspflichten

Pflicht zur **Information aller betroffener Personen** über jede Datenbeschaffung (Art. 19 ff. revDSG)

Gesetzlich definierter Mindestinhalt

- Identität und Kontakt der Verantwortlichen
- Bearbeitungszweck(e)
- Empfängerinnen der Daten
- Empfängerstaaten und getroffene Schutzmassnahmen

d) Informationspflichten

Grundsätzlich keine Formvorschrift; **Dokumentation und Schriftform** jedoch empfohlen (Beweisgründe!)

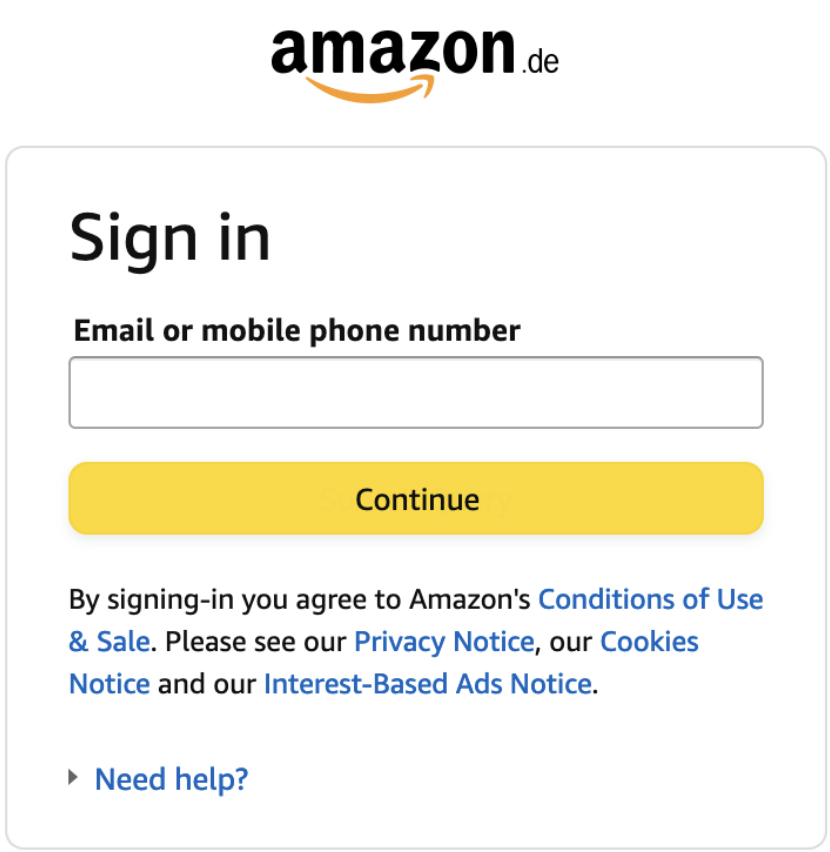
- z.B. Datenschutzerklärung Webseite
- *Privacy Policy* für Kunden
- Arbeitsreglement für Mitarbeitende

Anforderungen an die Information (Art. 13 DSV)

- Präzise, transparente und einfach verständliche Sprache
- vollständig
- leicht zugänglich

d) Informationspflichten

Beispiele



d) Informationspflichten

PUBLIC SECTOR LAW

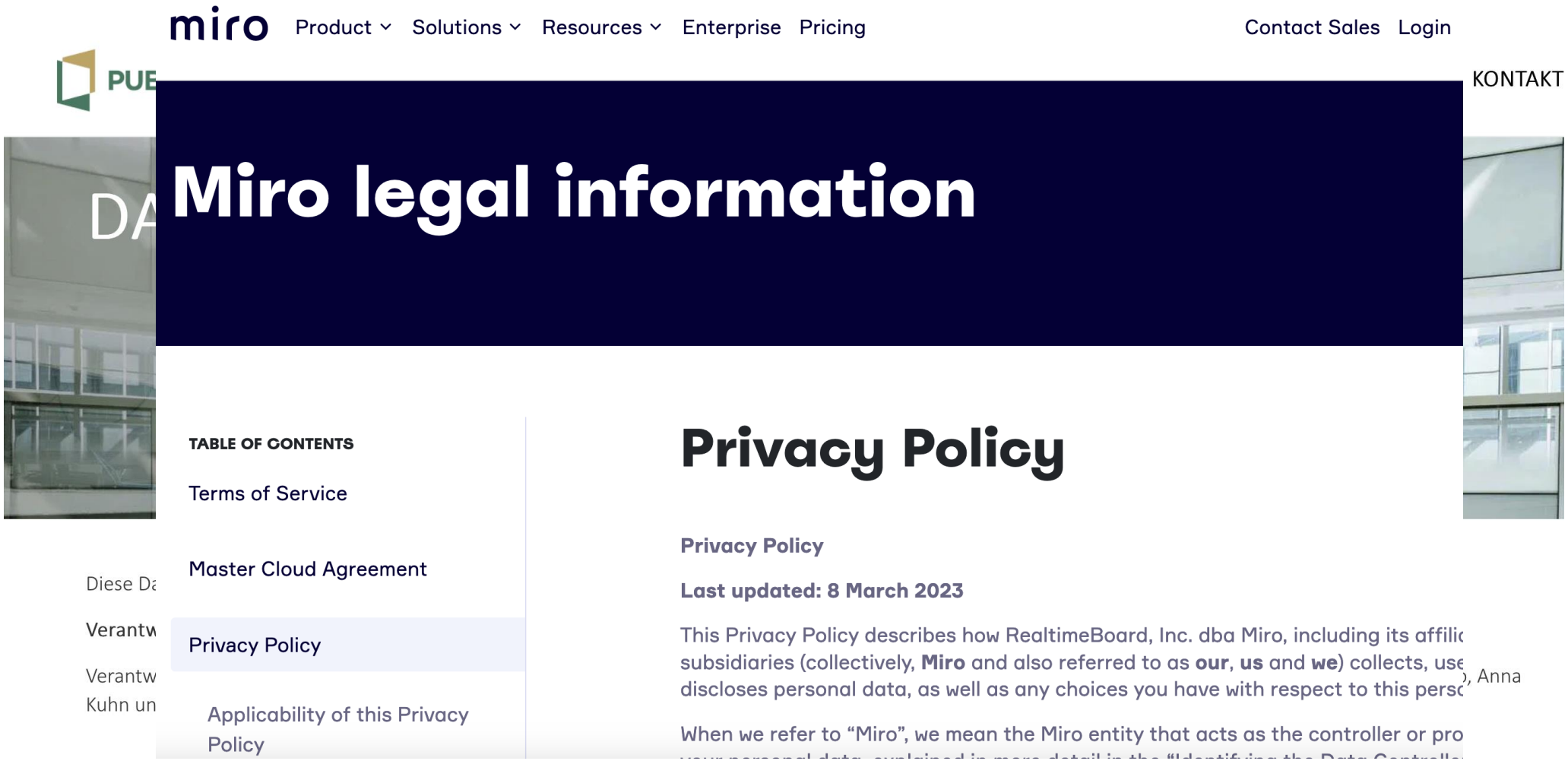
ARBEITSBEREICHE TEAM NEWS FAQs KONTAKT

Diese Datenschutzerklärung hat zum Zweck, Sie über die Verarbeitung persönlicher Daten durch PUBLIC SECTOR LAW zu informieren.

Verantwortliche Stelle

Verantwortliche Stelle für die Erhebung, Verarbeitung und Nutzung Ihrer personenbezogenen Daten ist die Anwaltskanzlei PUBLIC SECTOR LAW, Philipp do Canto, Anna Kuhn und Esther Zysset.

d) Informationspflichten



e) Data Breach Notifications

Meldepflicht für Datensicherheitsverletzungen (Art. 24 revDSG)

Definition (Art. 5 lit. h revDSG)

- Personendaten gehen **verloren**, werden **unbeabsichtigt gelöscht, verändert** oder unbefugten Personen **zugänglich** gemacht

Beispiele

- Verlust USB-Stick, ein Laptop oder Mobiltelefon mit geschäftlichen Daten
- Unberechtigte Person hat Datenzugriff (z.B. Logins wurden geteilt)
- Datenspeicherung auf nicht zugelassenen Cloud-Lösungen
- Vermutung eines Cyberangriffes (DDoS, Ransomware, Phishing etc.)

e) Data Breach Notifications

Wann muss man melden?

- Nur, sofern die Datenschutzverletzung voraussichtlich zu einem **hohen Risiko** für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

Wem muss man melden?

- Der Datenschutzaufsicht (bspw. EDÖB)
- Der Auftragsbearbeiter meldet eine Verletzung dem Verantwortlichen
- Der betroffenen Person, sofern zu ihrem Schutz erforderlich (bspw. für Passwort-Wechsel)

e) Data Breach Notifications

Wie muss man melden?

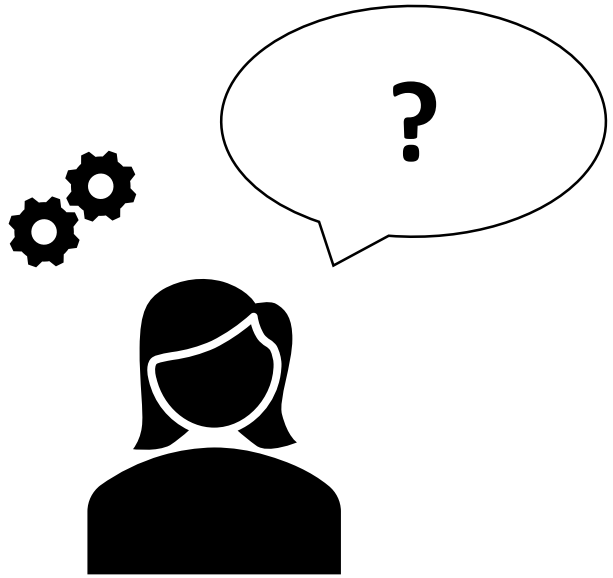
- «So rasch als möglich» (Art. 24 Abs. 3 revDSG; 72 Std. gemäss Praxis)
- Schriftlich und Aufbewahrung der Dokumentation für 2 Jahre (Art. 15 Abs. 4 DSV)

Was muss man mindestens melden? (Art. 25 Abs. 1 DSV)

- Art der Verletzung
- Zeitpunkt und Dauer
- Kategorien und ungefähre Anzahl betroffener Personen und Daten
- Folgen und Risiken für die Betroffenen
- Ergriffene und vorgesehene Massnahmen
- Kontaktdaten einer Ansprechperson

f) Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung ist ein **dokumentiertes «Nachdenken»** über Datenbearbeitungen (vgl. Art 22 revDSG)



f) Datenschutz-Folgenabschätzung

Zweck: Erkennung und Bewertung von Datenschutzrisiken (Risiko = Schaden x Wahrscheinlichkeit des Eintretens)

Erstellungspflicht: Durch Verantwortliche vor einer neuen Bearbeitung von Personendaten oder bei wesentlicher Änderung der bisherigen Bearbeitungsweise; zusätzlich periodische Überprüfung

Inhalt: Beschreibung, Risikoanalyse, Identifikation von besonderen Risikofaktoren, Risikobewertung, Massnahmen zur Bewältigung der Risiken, Entscheid über Vorlage an Datenschutzaufsicht (bspw. EDÖB)

f) Datenschutz-Folgenabschätzung

Vorgehen

Hohes Risiko für Grundrechte?

Art, Umfang, Umstände und Zweck der Datenbearbeitung

Beispiele:

- umfangreiche Bearbeitung besonders schützenswerter Personendaten
- Profiling
- Systematische Überwachung öffentliche Bereiche

↓

Durchführung der DSFA

1. Beschreibung Datenbearbeitungen
2. Bewertung der Risiken
3. Massnahmen zur Reduktion der Risiken

↓

Konsultation Datenschutzaufsicht / betroffene Person

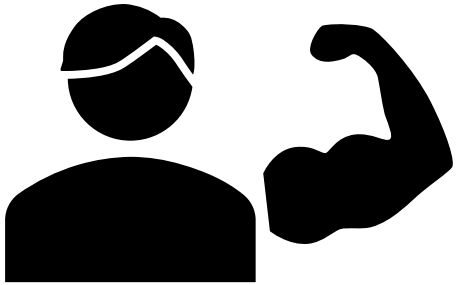
Wenn nach wie vor hohes Risiko für die Persönlichkeit/Grundrechte der betroffenen Personen besteht.

g) Betroffenenrechte

Betroffene Personen haben gewisse Rechte im Zusammenhang mit der Bearbeitung der eigenen Personendaten (insb. Art. 25 ff. revDSG)

Darunter fallen folgende Rechte:

- Recht auf Auskunft
- Recht auf Löschung
- Recht auf Berichtigung der Daten
- Recht auf Datenherausgabe und -übertragung



g) Betroffenenrechte

Was gilt für Betroffenenrechte generell?

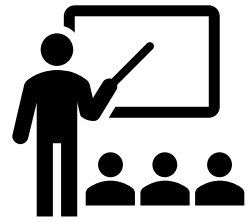
- Frist von 30 Tagen
- Identifikation der gesuchstellenden Person
- Schriftliches Gesuch und Antwort empfohlen (Beweiszwecke!)
- Betroffenenrechte werden grundsätzlich kostenlos gewährt
- Es sind diverse Ausnahmen zu beachten (bspw. Aufbewahrungspflichten)
- Praxistipp: Fristgerechte Umsetzung braucht gute Übersicht über die Datenbearbeitungen. Implementierung eines Prozesses ist empfohlen, wenn häufig Gesuche eingehen.

h) Interne Datenschutzberaterin

Ernennung Datenschutzberaterin (Art. 10 revDSG)

- **Beratende Funktion** in Datenschutzbelangen, ist die **Ansprechperson** für Behörden und betroffene Person
- **Freiwillig** für private Datenbearbeitende

- **Pflicht** für Bundesorgane (Möglichkeit gemeinsame Ernennung)
- **Gesetzliche Anforderungen** an die Rolle (Art. 23 f. , Art. 25 ff. DSV)
  - Hat Zugang zu notwendigen Informationen
  - Verfügt über notwendige Ressourcen
  - Genügend Fachkenntnisse
  - Weisungsungebunden und fachlich unabhängig



3 Aufsicht und Sanktionen

Aufsicht

Untersuchungsbefugnisse EDÖB (Art. 49 revDSG)

EDÖB kann u.a. (Art. 50 revDSG):

- **Zugang** zu allen Unterlagen, Räumlichkeiten, Anlagen anordnen
- **Zeugen** einvernehmen

Verfügungsrecht des EDÖB (Art. 51 revDSG):

- Verbote
- Anpassungen
- Löschungen
- Durchführung DSFA

3 Aufsicht und Sanktionen

Sanktionen

- Geldstrafen bis zu CHF 250‘000.00
- Strafen für **Mitarbeitende** (Unternehmen nur ausnahmsweise, Art. 64 Abs. 2 revDSG)!
- **(Eventual-)Vorsatz** ist Voraussetzung

Unter Strafe stehen u.a.:

- Verletzung von **Informations-, Auskunfts- und Mitwirkungspflichten** (Art. 60 revDSG)
- Datenbekanntgabe in **unsicheres Drittland ohne genügend Schutzmassnahmen**
- Übertragung der Datenbearbeitung an **Dritte** ohne Gewährleistung Datensicherheit
- Nichteinhaltung der Mindestanforderungen der **Datensicherheit**
- Missachtung von **Verfügungen** des EDÖB (Art. 63 revDSG).

4 Pro memoria: Praktische Tipps zur Implementierung

- Schritt 1 – Prüfung anwendbare Vorgaben
- Schritt 2 - Data mapping / Verzeichnis der Bearbeitungstätigkeiten
- Schritt 3 – Massnahmenkatalog
- Schritt 4 – Umsetzung Schritt für Schritt
- Schritt 5 – Review und Verbesserung

Vielen Dank für Ihre Aufmerksamkeit.

RA MLaw Anna Kuhn, CIPP/E
kuhn@publicsector.ch
+41 44 586 22 73

RA Dr. iur. Esther Zysset, CIPP/E
zysset@publicsector.ch
+41 44 586 22 02

PUBLIC SECTOR LAW