

Datenschutz

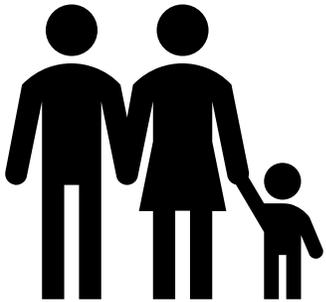
Neuerungen ab September 2023

Rechtsanwältin Sabine Fercher

Übersicht

1. Rollen im Datenschutz
2. Datenschutzberater:in
3. Anwendung des revidierten DSG und der DSV
4. Datenkategorien
5. Informationspflichten
6. Pflichten Verantwortliche + Auftragsbearbeitende
7. Pflichten Verantwortliche I und II
8. Auftragsbearbeitende
9. Betroffenenrechte
10. Anforderungen an Bonitätsprüfung
11. Rechtsfolgen mögliche Sanktionen

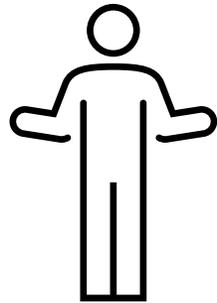
1. Rollen im Datenschutz



Betroffene Person:

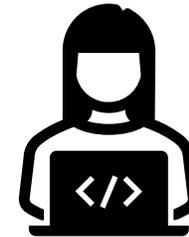
Natürliche Personen über die Personendaten bearbeitet werden

IP Adresse = Personendaten
Bearbeiten = sehr weiter Begriff



Verantwortliche (Controller):

private Person die allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet, wie Personendaten bearbeitet werden



Auftragsbearbeitende (Processor):

private Person die im Auftrag der Verantwortlichen Personendaten bearbeitet

2. Datenschutzberater:in

Verantwortliche kann Datenschutzberater:in ernennen

Datenschutzberater:in

- Schult und berät den Verantwortlichen
- Wirkt mit, dass Datenschutzvorschriften angewendet werden

Ausnahme Pflicht EDÖB* zu konsultieren bei Datenschutz-Folgeabschätzung (sogleich in 6.)

- Datenschutzberater:in wurde ernannt, Kontaktdaten bekannt gemacht (Bsp. Webseite, Datenschutzerklärung), ist unabhängig, hat Fachkenntnisse; und
- Datenschutzberater:in wurde EDÖB mitgeteilt

*EDÖB = Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter “Datenschutzbeauftragter”

3. Anwendung des rev. DSG und der DSV

Revidiertes DSG und die dazugehörige DSV treten am 1. September 2023 in Kraft und sind ohne Übergangsfrist anwendbar.

Anwendungsbereich

Es werden natürliche und keine juristischen Personen (mehr) geschützt.

Es ist weltweit für alle Sachverhalte anwendbar, wenn es sich in der Schweiz auswirkt.

4. Datenkategorien

Erweiterung **besonders schützenswerte** Daten:

+ Ethnie + genetische + biometrische Daten (bisher Gesundheit, Rasse, Religion, Sozialhilfemassn. ...)

Profiling = Automatisierte Bearbeitung von Personendaten zum Bewerten (Analysieren, Vorhersagen) von etwa der

- Arbeitsleistung
- Wirtschaftliche Lage
- Gesundheit
- Persönliche Vorlieben
- Interessen
- Zuverlässigkeit
- Verhalten
- Aufenthaltsort
- Ortswechsel

Profiling mit hohem Risiko = Hohes Risiko für Persönlichkeit oder die Grundrechte der Betroffenen durch Verknüpfung von Daten die Beurteilung von wesentlichen Aspekte der Persönlichkeit erlauben.

5. Informationspflichten

Pflichtangaben

- Identität und Kontaktdaten des Verantwortlichen, Bearbeitungszwecke
- Empfänger oder Kategorie von Empfängern denen Personendaten bekannt gegeben werden
- Bekanntgabe ins Ausland: Staat/internationales Organ ggf. Garantien zum Schutz von Daten
- Kategorien der bearbeitenden Personendaten (wenn indirekte Datenerhebung)
- Durchführung automatisierten Einzelentscheidung

Bekanntgabe an Betroffene

- Grundsätzlich vor Bearbeitung – Ausnahme: bei indirekter Datenerhebung spätestens bei Bekanntgabe an Dritte oder nach einem Monat nach Erhalt

Wortlaut: präzise, transparent, verständlich und leicht zugänglich

6. Pflichten Verantw. & Auftragsbearbeitende

Verzeichnis mit Angaben zur Datenbearbeitung

- Genaue Vorgabe von Mindestangaben (Verantwortlichen bzw. Auftragsbearbeitende benennen, Bearbeitungszweck, diverse Kategorien, Aufbewahrungsdauer, Datensicherheitsmassnahmen, Auslandsbekanntgabe)
- «Ausnahme: weniger als 250 Mitarbeiter am 1.1. des jeweiligen Jahres»
- Gegen Ausnahme: es werden besonders schützenswerte Daten in grossem Umfang bearbeitet oder es werden Profiling mit hohem Risiko durchgeführt.

Bearbeitungsreglement für automatisierte Bearbeitungen:

- Bearbeitung von besonders schützenswerte Personendaten in grossem Umfang
- Durchführung von Profiling mit hohem Risiko
- Fokus: Gewährleistung der Datensicherheit

7. Pflichten Verantwortliche I

Voraussichtlich *hohes Risiko für die Persönlichkeit oder die Grundrechte des Betroffenen:

1. Meldepflicht «data breach notification»

- Auftragsbearbeiter ggü Verantwortliche und Verantwortliche ggü EDÖB
- Verantwortliche ggü Betroffenen, wenn zu deren Schutz erforderlich

2. Datenschutz-Folgeabschätzung:

- Beschreibung der Datenbearbeitung
- Bewertung der Risiken
- Massnahmen zum Schutz

*hohes Risiko insbesondere bei Verwendung neuer Technologien und es wird angenommen bei:

- umfangreicher Bearbeitung besonders schützenswerter Personendaten, oder
- bei systematischer Überwachung von öffentlichen Bereichen

7. Pflichten Verantwortliche II

Datenschutzfreundlichkeit mit technischer Unterstützung

Privacy-by-Design

- bei Planung von Datenbearbeitungen
- Implementierung von angemessenen technischen und organisatorischen Massnahmen toM um Grundsätze wie etwa Datensparsamkeit sicherzustellen

Privacy-by-Default

- Voreinstellungen beschränken Bearbeitung auf Bearbeitungszweck
- Insbesondere auf Webseiten: Verhinderung der Übertragung von Personendaten an Dritte

8. Auftragsbearbeitende

Durch einen Vertrag oder durch die Gesetzgebung kann die Bearbeitung von Personendaten vom Verantwortlichen an einen Auftragsbearbeiter übertragen werden.

Spielregeln

Der Auftragsbearbeiter muss die Daten so bearbeiten, wie es der Verantwortliche tun darf.

Der Verantwortliche muss sich vergewissern und vertraglich regeln, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

Unterauftragsbearbeiter dürfen nur mit vorangehender Genehmigung des Verantwortlichen mit einer Auftragsbearbeitung betraut werden.

9. Betroffenenrechte

Auskunfts-, Änderungs-, Löschungs-, Herausgabe- und insbesondere:

Datenportabilität – das Übertragungsrecht:

- in einem gängigen elektronischen Format
- Herausgabe an Betroffenen oder an einen anderen Verantwortlichen

Grundsätzlich

- ohne Kosten für Betroffene und innerhalb von 30 Tagen

+ Widerspruchsrecht

Bei Widerspruch des Betroffenen, muss eine natürliche Person den automatisierten Einzelentscheid überprüfen (siehe auch Informationspflicht). Ausnahme: Betroffene hat ausdrücklich eingewilligt, dass diese Entscheidung automatisiert erfolgt.

10. Anforderungen an Bonitätsprüfung

Braucht Einwilligung des Betroffenen, oder

ein überwiegendes Interesse:

- Es handelt sich weder um besonders schützenswerte Personendaten noch um Profiling mit hohem Risiko, und
- Bekanntgabe an Dritte nur, wenn diese die Daten für Abschluss oder Abwicklung des Vertrages mit Betroffenen brauchen, und
- Daten sind nicht älter als 10 Jahre, und
- Betroffene = Volljährig

11. Rechtsfolgen mögliche Sanktionen

Strafrechtlich => Busse bis zu CHF 250'000 durch kantonale Staatsanwaltschaften

- Eventualvorsätzliche Verletzung von Informations- Auskunfts- und Sorgfaltspflichten
- Verletzung der beruflichen Schweigepflicht
- Missachtung von Anweisungen vom EDÖB
- Verjährung 5 Jahre

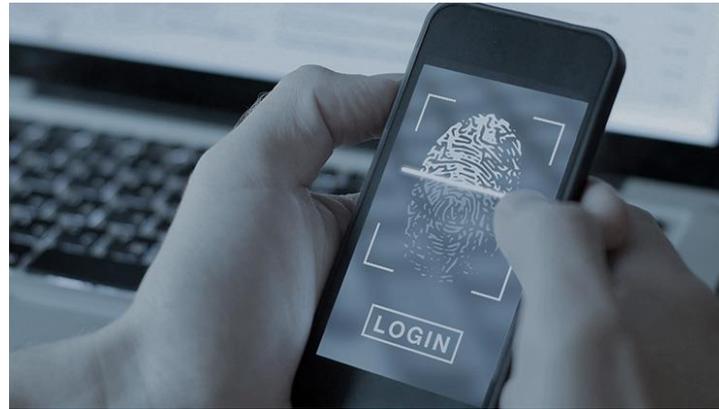
Verwaltungsrechtlich durch EDÖB

- Untersuchungen mit Zugang zu Räumlichkeiten und Unterlagen (nicht bei bsp. Anwälte, Ärzte)
- Verfügungen wie Untersagen von Bearbeitung, Anordnung von Löschung

Zivilrechtlich durch Betroffene

- Schutz der Persönlichkeitsrechte mit Klagerecht auf Beseitigung Unterlassung oder Schadenersatz

Dankeschön



F

FERCHER
COMPLIANCE



sabine@fercher-compliance.ch



079 53 88 000



[linkedin.com/company/fercher-compliance](https://www.linkedin.com/company/fercher-compliance)