

Welche Pflichten sieht das neue Schweizer Datenschutzgesetz für Stiftungen vor?

Nando Stauffer von May

4. und 9. Mai 2023

Datenschutzgesetzgebung(en)



Neues DSG

Ab 1. September 2023

Bussen bis zu CHF 250'000 für die
fehlbare(n) Personen



GDPR

Seit 25. Mai 2018

Bussen bis zu EUR 20 Mio. (oder
4% des weltweiten
Jahresumsatzes) für das fehlbare
Unternehmen



UK-GDPR u.v.m.

Datenschutzgesetzgebung(en)



DSG – Bundesorgan

Behörde oder Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist



DSG – Private

Natürliche (sobald Personendaten nicht mehr ausschliesslich zum persönlichen Gebrauch bearbeitet werden) oder juristische Person.



Kanton und Gemeinden

Kanton, Gemeinden, Organe von Körperschaften und Anstalten sowie Private, soweit ihnen öffentliche Aufgaben übertragen sind.

Personendaten und die damit zusammenhängenden Pflichten für Private

Personendaten

Alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.



Bearbeitungsverzeichnis



Bearbeitungsverzeichnis

Ab 250 Mitarbeitern oder bei **Bearbeitung von besonders schützenswerten Personendaten in grossem Umfang** oder bei Profiling mit hohem Risiko.



Besonders schützenswerte Personendaten

Religiöse, weltanschauliche oder politische oder gewerkschaftliche Ansichten oder Tätigkeiten; Gesundheit, Intimsphäre oder Zugehörigkeit zu einer Rasse oder Ethnie; biometrische Daten, die eine natürliche Person eindeutig identifizieren; genetische Daten



Besonders schützenswerte Personendaten

Biometrische Daten, die eine natürliche Person eindeutig identifizieren; genetische Daten; Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen; Daten über Massnahmen der sozialen Hilfe

Besonders schützenswerte Personendaten



Personendaten

Ethnie/Rasse?

Gesundheit?

weltanschauliche oder
politische Ansichten?

Bearbeitungsreglement + Protokollierungspflicht



Reglement für automatisierte Bearbeitungen u.a. notwendig, wenn besonders schützenswerte Personendaten in grossem Umfang bearbeitet werden.

Können überdies die präventiven Massnahmen den Datenschutz nicht gewährleisten, so muss das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten protokolliert werden.

Datenschutzfolgenabschätzung (DSFA)



Der Verantwortliche erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann.

Informationspflicht

Der Verantwortliche informiert die betroffene Person angemessen über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden (Art. 19 nDSG).



Informationspflicht

Verantwortlicher: Person, die allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet



Informationspflicht

Bearbeiten: Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten



Informationspflicht

Betroffene Person:

Natürliche Person, über die
Personendaten bearbeitet
werden



Informationspflicht

Informieren:

- in präziser, transparenter, verständlicher und leicht zugänglicher Form
- Gesetzlich vorgeschriebener Mindestinhalt
- Datenschutzerklärung



Auskunftspflicht



Jede Person kann vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.

Technische und organisatorische Massnahmen (TOMs)

- Risikoangemessen
- Stand der Technik
- Mindestanforderungen an die Datensicherheit
- Privacy by Default & by Design

Ziele in Bezug auf die Personendaten:

- Verfügbarkeit: Risikomitigation von versehentlicher oder nicht autorisierter Vernichtung
- Vertraulichkeit: Schutz vor unbefugtem Zugriff
- Integrität: Korrektheit der Daten
- Nachvollziehbarkeit der Bearbeitung



Meldepflicht von Verletzungen der Datensicherheit

Der Verantwortliche meldet 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.

Der Verantwortliche informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.



Datenübermittlung ins Ausland

Prüfen, ob zulässig:

- Angemessenheitsbeschluss
- Standardvertragsklausel
- Einwilligung
- Vertragsabwicklung



Weitere Pflichten



Vertreter in ...

der EU, der Schweiz, im UK und ...



Auftragsdatenbearbeitung

Botschaft des Bundesrats: «Der Verantwortliche muss analog wie bei Artikel 55 OR Verstösse gegen das DSG verhindern. Er ist daher verpflichtet, seinen Auftragsbearbeiter sorgfältig auszuwählen, ihn angemessen zu instruieren und soweit als nötig zu überwachen.»



Löschung

Personendaten müssen vernichtet werden, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind. → Aufbewahrungsfristen festlegen

Motivation?



Motivation – Persönlichkeitsschutz



Grundsätze der Datenbearbeitung:

- Rechtmässigkeit
- Treu und Glauben
- Verhältnismässigkeit
- Erkennbarkeit
- Zweckgebundenheit
- Richtigkeit
- Sicherheit

Busse bis zu CHF 250'000

Vorsätzlich falsche oder unvollständige Auskunftserteilung im Zusammenhang mit der

- Informationspflicht (Datenschutzerklärung) oder dem
- Auskunftsrecht der betroffenen Person.

Vorsätzlicher

- Verstoss gegen Regeln zur Bekanntgabe von Personendaten ins Ausland
- Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne Einhalten der Voraussetzungen hierfür
- Mindestanforderungen an die Datensicherheit nicht eingehalten

«Kleines Berufsgeheimnis»

Wer 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, wird auf Antrag mit Busse bis zu 250 000 Franken bestraft.



Los geht's!





Was tun?



Übersicht über Bearbeitung von Personendaten

- Bearbeitungsverzeichnis (Word/Excel-Vorlagen)
- Unnötige Personendaten nicht mehr bearbeiten
- Risiko identifizieren (Notwendigkeit DSFA?)



Datensicherheit

Besprechen Sie mit Ihrem Informatiker Art. 3 der Datenschutzverordnung (TOMs)

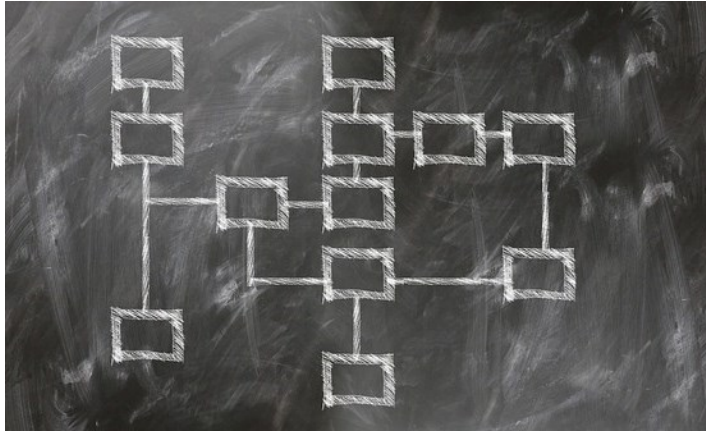


Datenschutzerklärung

Publizieren Sie eine möglichst umfassende Datenschutzerklärung auf der Website.

(Keine Vorlagen eins zu eins verwenden, so dass der Inhalt kaum etwas mit Ihrer Datenbearbeitung zu tun hat.)

Was tun?



Dokumentation

- Verantwortlichkeiten festlegen / delegieren
- Prozesse für Auskunftersuchen & Meldung von Verletzungen der Datensicherheit festlegen
- Lösch-/Archivkonzept
- Bearbeitungsreglement



Mitarbeiterschulung

Sensibilisieren Sie die Mitarbeiter auf Datenschutz und definieren Sie eine interne (oder externe) Ansprechperson (evtl. sog. Datenschutzberater)



Auftragsbearbeitungsverträge

- Auftragsbearbeitungen identifizieren
- Auftragsbearbeitungsverträge abschliessen (evtl. stellt Anbieter ein Muster zur Verfügung)
- Datenübermittlungen ins Ausland prüfen

Vielen Dank.

Nando Stauffer von May

Partner | Dr. iur. | Notar des Kantons Bern | Rechtsanwalt

stauffer@gbf-legal.ch

Zürich

gbf Rechtsanwälte AG
Hegibachstrasse 47
8032 Zürich
T +41 43 500 48 50

Genf

gbf Avocats SA
Route de Pré-Bois 20
1215 Genève Aéroport
T +41 22 533 48 50

Notariat Bern

Notar Stauffer von May
Von-Werdt-Passage 3
3011 Bern
T +41 43 500 48 50

Notariat Olten

Notar Novoselac
Solothurnerstrasse 235
4600 Olten
T +41 43 500 48 50

gbf Attorneys-at-law
Rechtsanwälte
Avocats