OBERSON
ABELS

Neues Schweizer Datenschutzgesetz: *lessons learned* und ein erstes Fazit nach einem Jahr

Pension Breakfast – November 2024

Vanessa Déglise

Plan

Einführung

Das neue Bundesgesetz über den Datenschutz (DSG) trat am 1. September 2023 in Kraft ohne Übergangsbestimmungen.

Das DSG gilt für alle Akteure in der Wirtschaft , auch für Vorsorgeeinrichtungen (VE).

Schwerpunkte der Reform:

- Verbesserung der Transparenz der Prozesse zur Bearbeitung von Personendaten
- Bessere Durchsetzung (*enforcement*) der Datenschutzbestimmungen
- Anpassung an die EU-Standards (DSGVO) und die Konvention 108 des Europarates

Einführung / Einige Begriffe (Art. 5 DSG)

PERSONENDATEN
=
alle Angaben, die sich auf eine **bestimmte** oder **bestimmbare natürliche Person** beziehen

BESONDERS SCHÜTZENSWERTE PERSONENDATEN
=
insbesondere Daten über:
- die **Gesundheit**, die **Intimsphäre** oder die Zugehörigkeit zu einer **Rasse** oder **Ethnie**
- **verwaltungs-** und **strafrechtliche Verfolgungen** oder **Sanktionen**
- Massnahmen der **sozialen Hilfe**

BETROFFENE PERSON
=
natürliche Person, über die Personendaten bearbeitet werden
(z.B. aktive Versicherte und Rentenbezüger, Kontaktpersonen von Geschäftspartnern, Mitglieder des Stiftungsrats)

BEARBEITEN
=
jeder Umgang mit Personendaten
(insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben)

Plan

Einführung

Anwendbare Regelung

Verzeichnis der Bearbeitungstätigkeiten

Informationspflicht

Bearbeitungsreglement

Verträge mit einer Übermittlung von Personendaten

Datenschutzberaterin oder –berater (DPO)

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Strafbestimmungen

Anwendbare Regelung

In seinem Tätigkeitsbericht 2023/2024 nahm der EDÖB folgende Positionen ein:

- Pensionskassen, die an der Durchführung der obligatorischen beruflichen Vorsorge (BVG-Obligatorium) beteiligt sind, und umhüllende Pensionskassen = **Bundesorgane im Sinne des DSG**
- Pensionskassen, die ausschliesslich im Überobligatorium tätig sind = **Private Personen im Sinne des DSG**
- Pensionskassen, die als kantonale oder kommunale öffentliche Organe handeln = unterliegen im Rahmen des BVG-Obligatoriums der **kantonalen Datenschutzgesetzgebung** sowie der kantonalen oder kommunalen Aufsicht
- Externe Dienstleistungsgesellschaften, die an Vorsorgeeinrichtungen einen Teil oder die Gesamtheit des operativen Geschäftsbetriebs übertragen = **Auftragsbearbeiter**

Die Positionen des EDÖB sind für die Gerichte nicht bindend, schreiben aber dennoch einen gewissen Standard vor.

Anwendbare Regelung / Checkliste

		Bundesorgan	Private Person
Verzeichnis der Bearbeitungstätigkeiten:	✓ Ausstellung	●	○
	✓ Mitteilung an den EDÖB	●	
Informationspflicht (Datenschutzerklärung):	✓ Ausstellung ✓ Mitteilung an die betroffenen Personen (insbesondere aktive Versicherte und Rentenempfänger)	●	●
Bearbeitungsreglement:	✓ Ausstellung und Annahme durch den Stiftungsrat	●	○
Verträge mit einer Übermittlung von Personendaten:	✓ Abschluss von Verträgen (falls nicht vorhanden) oder Anpassung bestehender Verträge	●	●
Datenschutzberaterin oder –berater (DPO):	✓ Ernennung ✓ Veröffentlichung der Kontaktdaten und Mitteilung an den EDÖB	●	

Plan

Einführung

Anwendbare Regelung

Verzeichnis der Bearbeitungstätigkeiten

Informationspflicht

Bearbeitungsreglement

Verträge mit einer Übermittlung von Personendaten

Datenschutzberaterin oder –berater (DPO)

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Strafbestimmungen

Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSG und Art. 24 DSV)

Worum es geht:

- Mapping der Bearbeitung von Personendaten durch die VE
- Wird meist in Form einer Excel-Tabelle dargestellt
- Mehrere mögliche Vorgehensweisen

Vorbereitung:

- Zwingend für Bundesorgane
- Fakultativ (aber dringend empfohlen) für Privatpersonen

Meldung an den EDÖB:

- Zwingend für Bundesorgane
- Empfohlen, dies über die Plattform des EDÖB zu tun
- Zwischen dem 1. April 2023 und dem 31. März 2024 wurden über 1'000 Einträge von VE in das Register der Verzeichniseinträge des EDÖB (Datareg) getätigt (Tätigkeitsbericht 2023/2024 des EDÖB, S. 45).

Plan

Einführung

Anwendbare Regelung

Verzeichnis der Bearbeitungstätigkeiten

Informationspflicht

Bearbeitungsreglement

Verträge mit einer Übermittlung von Personendaten

Datenschutzberaterin oder –berater (DPO)

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Strafbestimmungen

Informationspflicht (Art. 19 ff. und 60 DSG, Art. 13 DSV)

Der Versicherte hat das **Recht,** in angemessener Weise über jede Beschaffung von Personendaten **informiert zu werden.**

Es gibt keine Informationspflicht, wenn die Bearbeitung von Personendaten **gesetzlich vorgeschrieben** ist.

→ Es ist jedoch für alle Pensionskassen ratsam, eine **Datenschutzerklärung** zu verfassen.

Minimaler Inhalt:

- Identität und Kontaktdaten des Verantwortlichen (d.h. der Pensionskasse)
- Zweck der Bearbeitung der Personendaten
- Gegebenenfalls Empfänger, an die die Personendaten weitergegeben werden
- Wenn Personendaten ins Ausland weitergegeben werden, Name des betreffenden Staates und gegebenenfalls eingerichtete Garantien

Plan

Einführung

Anwendbare Regelung

Verzeichnis der Bearbeitungstätigkeiten

Informationspflicht

Bearbeitungsreglement

Verträge mit einer Übermittlung von Personendaten

Datenschutzberaterin oder –berater (DPO)

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Strafbestimmungen

Bearbeitungsreglement (Art. 5 und 6 DSV)

Dieses Dokument ist für Bundesorgane zwingend.

Es muss grundsätzlich nicht der Aufsichtsbehörde vorgelegt werden.

Dieses Dokument enthält in der Regel Bestimmungen über:

- die wesentlichen Rollen der Datenschutzstelle, um die Einhaltung der geltenden Gesetze zu gewährleisten
- das Verfahren zur Beantwortung von Anfragen betroffener Personen
- das Verfahren, das im Falle eines Sicherheitsvorfalls zur Anwendung kommt:
  - Personen, die für die Analyse des Vorfalls, die Entscheidungsfindung, die Kommunikation und den Kontakt mit den Behörden zuständig sind
  - Definition des Vorgehens
  - Meldung an den EDÖB / die betroffenen Personen (Art. 24 DSG und Art. 15 DSV)
- die Regeln für die Archivierung
- Massnahmen zur Gewährleistung der Datensicherheit

Plan

Einführung

Anwendbare Regelung

Verzeichnis der Bearbeitungstätigkeiten

Informationspflicht

Bearbeitungsreglement

Verträge mit einer Übermittlung von Personendaten

Datenschutzberaterin oder –berater (DPO)

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Strafbestimmungen

Verträge mit einer Übermittlung von Personendaten (Art. 9 et 61 DSG, Art. 7 DSV)

Durchsicht der Datenschutzbestimmungen (Beschreibung der Bearbeitung, Anweisungen, usw.):

- Angemessene Sicherheitsmassnahmen
- Informationsverfahren im Falle eines Datenlecks
- Informationsverfahren und vorherige Genehmigung für den Einsatz von Auftragsbearbeiter
- Angemessene Garantien (z.B. Standardvertragsklauseln) bei der Übermittlung von Personendaten in Nicht-EU-Staaten

Ein Nachtrag (*Addendum*) kann den bestehenden Hauptvertrag ändern / ergänzen.

Der EDÖB betrachtet externe Dienstleistungsgesellschaften, an die Vorsorgeeinrichtungen einen Teil oder die Gesamtheit des operativen Geschäftsbetriebs übertragen, als Auftragsbearbeiter.

Einige Dienstleistungsgesellschaften im Bereich der Vorsorgeverwaltung bestreiten diesen Ansatz.

Plan

Einführung

Anwendbare Regelung

Verzeichnis der Bearbeitungstätigkeiten

Informationspflicht

Bearbeitungsreglement

Verträge mit einer Übermittlung von Personendaten

Datenschutzberaterin oder –berater (DPO)

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Strafbestimmungen

Datenschutzberaterin oder –berater (Art. 10 DSG, 23 et 25 ff. DSV)

Die Ernennung eines Datenschutzberaters (*Data Protection Officer;* DPO) ist:

- obligatorisch für Bundesorgane
- fakultativ für Privatpersonen (von begrenztem Interesse)

Rolle des DPO:

- die Mitarbeiter der VE in Sachen Datenschutz zu schulen und zu beraten
- an der Durchsetzung von Datenschutzbestimmungen mitzuwirken
- als Ansprechpartner für die betroffenen Personen und den EDÖB zu fungieren

Plan

Einführung

Anwendbare Regelung

Verzeichnis der Bearbeitungstätigkeiten

Informationspflicht

Bearbeitungsreglement

Verträge mit einer Übermittlung von Personendaten

Datenschutzberaterin oder –berater (DPO)

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Strafbestimmungen

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragte (Art. 4 und 43 ff. DSG, Art. 36 ff. DSV)

Der **Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte** (EDÖB) beaufsichtigt die Anwendung der bundesrechtlichen Datenschutzvorschriften (Art. 4 DSG).

Der EDÖB:

- kann eine **Untersuchung** gegen ein Bundesorgan oder eine private Person eröffnen, wenn genügend Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte (Art. 49 DSG).
- kann **Verwaltungsmassnahmen** anordnen (Art. 51 DSG), z.B.:
  - ✓ verfügen, dass die Bearbeitung ganz oder teilweise angepasst, unterbrochen oder abgebrochen wird und die Personendaten ganz oder teilweise gelöscht oder vernichtet werden
  - ✓ die Bekanntgabe ins Ausland aufschieben oder untersagen
- muss **von Verletzungen der Datensicherheit**, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen, **informiert werden.**

Der EDÖB kann keine strafrechtlichen Sanktionen verhängen.

Plan

Einführung

Anwendbare Regelung

Verzeichnis der Bearbeitungstätigkeiten

Informationspflicht

Bearbeitungsreglement

Verträge mit einer Übermittlung von Personendaten

Datenschutzberaterin oder –berater (DPO)

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Strafbestimmungen

Strafbestimmungen (Art. 60 ff. DSG)

Von der Schweiz gewählter Ansatz:

- Verstösse gegen das DSG können strafrechtlich sanktioniert werden
- Natürliche Personen sind in erster Linie betroffen

Anderer Ansatz im EU-Recht: Verwaltungsbussen gegen juristische Personen

Täter der Straftaten = „Private Personen“

- Die meisten DSG-Strafbestimmungen richten sich an „private Personen“ im Sinne des DSG und nicht an Bundesorgane.
- Risiko, dass sie auf Mitglieder des Stiftungsrats und Mitarbeiter einer Pensionskasse anwendbar sind, insbesondere wenn die Vorsorgeeinrichtung umhüllend ist und somit über das BVG-Obligatorium hinaus agiert ?

Strafbestimmungen (Art. 60 ff. DSG)

DSG	Strafbare Handlung	Täter	Verfolgung
Art. 60 (1)	Vorsätzliche Erteilung falscher oder unvollständiger Auskünfte an die betroffenen Personen oder vorsätzliche Unterlassung der Information	Private Personen	Auf Antrag
Art. 60 (2)	Vorsätzliche Erteilung falscher Auskünfte oder vorsätzliche Verweigerung der Mitwirkung im Rahmen einer Untersuchung.	Private Personen	Von Amtes wegen
Art. 61	Vorsätzliche Verletzung von Sorgfaltspflichten (Bekanntgabe von Personendaten ins Ausland, Einhaltung der Bedingungen von Art. 9 DSG im Falle einer Bearbeitung durch Auftragsbearbeiter, Mindestanforderungen an die Datensicherheit)	Private Personen	Auf Antrag
Art. 62	Vorsätzliche Verletzung der beruflichen Schweigepflicht	Jeder	Auf Antrag
Art. 63	Missachten von Verfügungen des EDÖB oder von einem Entscheid der Rechtsmittelinstanzen	Private Personen	Von Amtes wegen

Strafbestimmungen (Art. 60 ff. DSG)

Verstösse:

- werden mit Busse bis zu 250'000 Franken bestraft
- werden vorsätzlich begangen
- sind Übertretungen (Art. 333 Abs. 3 StGB). Versuch und Gehilfenschaft sind jedoch nicht strafbar (Art. 105 Abs. 2 StGB).

Verstösse gegen die folgenden Regeln stellen keine strafbare Handlung dar:

- Meldung von Verletzungen der Datensicherheit (*data breach notifications*) (Art. 24 DSG)
- Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSG)
- Folgenabschätzung bei hohem Persönlichkeitsrisiko (Art. 22 DSG)

Verjährung der Strafverfolgung = 5 Jahre (Art. 66 DSG)

Strafbestimmungen (Art. 60 ff. DSG)

Klarer Wille des Gesetzgebers, natürliche Personen zu bestrafen:

- Ausnahme: „*Fällt eine Busse von höchstens 50'000 Franken in Betracht und würde die Ermittlung der nach Artikel 6 VStrR strafbaren Personen Untersuchungsmassnahmen bedingen, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären, so kann die Behörde von einer Verfolgung dieser Personen absehen und an ihrer Stelle den Geschäftsbetrieb (Art. 7 VStrR) zur Bezahlung der Busse verurteilen.*“ (Art. 64 Abs. 2 LPD).

- Kann der Arbeitgeber die Geldstrafe anstelle der natürlichen Person zahlen?
  - In der Rechtswissenschaft umstritten
  - Riskant: „*Wer jemanden der Strafverfolgung (…) entzieht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*“ (Art. 305 StGB).
  - Geldstrafe = persönlich

- Kann man sich versichern?
  - Eine Vereinbarung, in der sich eine Person verpflichtet, eine Geldstrafe zu zahlen, die gegen einen Dritten verhängt wurde, ist grundsätzlich ungültig.
  - In der Praxis: Versicherungen schliessen Geldstrafen von der Deckung aus.

Vielen Dank für Ihre Aufmerksamkeit

Vanessa Déglise
Anwältin, LL.M. (Columbia)
Sozialversicherungsfachfrau mit
eidgenössischem Fachausweis

vdeglise@obersonabels.com

T +41 58 258 86 00