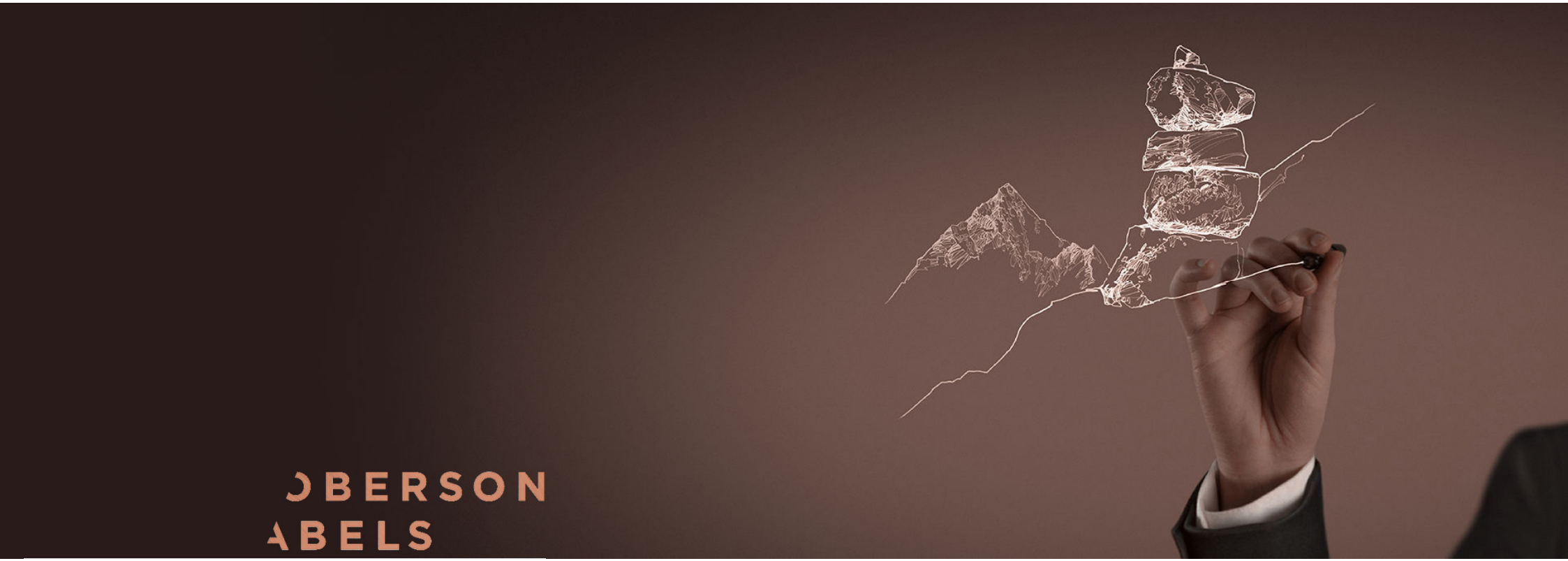

Datenschutz –
Neue Regeln für Pensionskassen

Pension Breakfast – September 2023

Philipp Fischer

Plan

Einführung

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

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 durch:
  - Gewährung neuer Rechte für betroffene Personen
  - Verpflichtung zur Offenlegung von Sicherheitsvorfällen im Zusammenhang mit Personendaten
  - Stärkung der Befugnisse des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)
  - Strengere Sanktionen
- Anpassung an die EU-Standards (DSGVO) und die Konvention 108 des Europarates

Keine Übergangsbestimmungen: Vorsorgeeinrichtungen müssen die Regeln bereits jetzt einhalten.

Plan

Anwendbare Regelung

Das DSG sieht unterschiedliche Regeln vor, je nachdem, ob der Betroffene eine « Privatperson » oder ein « Bundesorgan » ist.

Im Allgemeinen sind die Reglen für Bundesorgane strenger als für Privatpersonen.

Im Bereich der Vorsorge:

- Pensionskassen, die im Bereich der obligatorischen Vorsorge tätig sind, und Freizügigkeitsstiftungen gelten als Bundesorgane.
- Institutionen, die ausschliesslich im über- oder ausserobligatorischen Bereich tätig sind, unterligen den für Privatpersonen geltenden Regeln.
- Kantonale oder kommunale Pensionskassen, die in Form einer öffentlich-rechtlichen Institution organisiert sind, unterliegen grundsätzlich den Regeln des kantonalen Datenschutzrechts.

Anwendbare Regelung

VE	Bereich der Vorsorge	Anwendbare Regelung
Registrierte Pensionskassen	Obligatorische Vorsorge Obligatorische und überobligatorische Vorsorge	Regelung des DSG für Bundesorgane
Freizügigkeitsstiftungen	Freizügigkeit	Regelung des DSG für Bundesorgane
Nicht registrierte Pensionskassen	Über- oder ausserobligatorische Vorsorge	Regelung des DSG für Privatpersonen
Kantonale oder kommunale Pensionskassen, die in Form einer öffentlich-rechtlichen Institution organisiert sind	Obligatorische und/oder überobligatorische Vorsorge	Kantonales Datenschutzrecht

Plan

Einführung

Anwendbare Regelung

Verzeichnis der Bearbeitungstätigkeiten

Informationspflicht

Bearbeitungsreglement

Datenschutzberaterin oder -berater

Verträge mit einer Übermittlung von Personendaten

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 (z.B. ASIP-Vorlage)

Verfahren (Bearbeitungstätigkeiten, für die die PK verantwortlich ist)	Bearbeitungszweck	Kategorien betroffener Personen	Kategorien bearbeiteter Personendaten	Kategorien der Empfänger intern / extern (Zugriff)	Bei Bekanntgabe ins Ausland: Angabe Staat und ggf. Garantien
Arbeitgeber (Durchführung berufliche Vorsorge)					
Arbeitgeber (als Dienstleistungserbringer für die PK)					
Aufsichtsbehörden, Gerichte, Handelsregister, Rechtsvertreter von Versicherten, IV-Stelle					

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

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
- Rund 600 VE haben bislang ihr Verzeichnis der Bearbeitungstätigkeiten auf der Plattform des EDÖB gemeldet.

Plan

Einführung

Anwendbare Regelung

Verzeichnis der Bearbeitungstätigkeiten

Informationspflicht

Bearbeitungsreglement

Datenschutzberaterin oder -berater

Verträge mit einer Übermittlung von Personendaten

Informationspflicht (Art. 19 ff und 60 DSG, 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 für die Verarbeitung 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 ggf. eingerichtete Garantien

Vom ASIP vorgeschlagene Vorlage

Datenschutzerklärung Pensionskasse XY

1. Grundsatz

Die Datenschutzerklärung[1] gilt für die Bearbeitung sämtlicher Personendaten[2], die wir im Zusammenhang mit der Durchführung der beruflichen Vorsorge und der damit verbundenen Tätigkeiten, unter Einschluss von Mietverhältnissen, bearbeiten.

Mit dieser Datenschutzerklärung möchten wir Sie darüber informieren, wie wir Ihre personenbezogenen Daten erheben und bearbeiten, wenn Sie unsere Website besuchen resp. unsere Online-Dienste nutzen, und weiterverarbeiten, speichern und an Dritte weitergeben, wenn wir für Sie Dienstleistungen erbringen.

Wir erheben und bearbeiten Ihre Personendaten nur zu den in dieser Datenschutzerklärung beschriebenen Zwecken und nur im dafür notwendigen Umfang und im Rahmen der anwendbaren Gesetzesvorschriften. Dabei bewahren wir Ihre Personendaten nur soweit und solange auf, als es die Erbringung unserer Dienstleistungen erfordert. Wir garantieren den Schutz unserer Datenbanken vor fremden Zugriffen, Verlusten, Missbrauch oder Fälschung.

Zur Wahrung der Sicherheit Ihrer Personendaten und zu deren Schutz gegen unberechtigte oder unrechtmässige Bearbeitungen und unberechtigte Zugriffe treffen wir angemessene Sicherheitsmassnahmen technischer (z.B. Verschlüsselung und Pseudonymisierung von Personendaten, Protokollierungen, Zugriffsbeschränkungen und Speicherung von Sicherheitskopien) und organisatorischer Natur (z.B. Weisungen an unsere Mitarbeitenden, Vertraulichkeitsvereinbarungen und Kontrollen).

Plan

Einführung

Anwendbare Regelung

Verzeichnis der Bearbeitungstätigkeiten

Informationspflicht

Bearbeitungsreglement

Datenschutzberaterin oder -berater

Verträge mit einer Übermittlung von Personendaten

Bearbeitungsreglement (Art. 5 und 6 DSV)

Dieses Dokument ist für Bundesorgane zwingend.

Es muss grundsätzlich nicht der Aufsichtsbehörde vorgelegt werden (weshalb es meist als Richtlinie bezeichnet wird).

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 15 DSV)
- die Regeln für die Archivierung
- Massnahmen zur Gewährleistung der Datensicherheit

Plan

Einführung

Anwendbare Regelung

Verzeichnis der Bearbeitungstätigkeiten

Informationspflicht

Bearbeitungsreglement

Datenschutzberaterin oder -berater

Verträge mit einer Übermittlung von Personendaten

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 mitwirken
- als Ansprechpartner für die betroffenen Personen und den EDÖB fungieren

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

Anforderungen an den DPO:

- muss über die notwendigen beruflichen Kenntnisse verfügen
- muss seine Funktion unabhängig von der Pensionskasse ausüben und darf keine Anweisungen von dieser erhalten
  - Der DPO sollte kein Mitglied des Stiftungsrats sein
  - Die Ernennung eines Angestellten des angeschlossenen Arbeitgebers ist denkbar, erfordert aber die Einführung strenger Trennungsmassnahmen
  - Der DPO kann ein Externer sein (oft die beste Lösung)
- kann eine natürliche oder juristische Person sein

Die Pensionskasse muss:

- dem Datenschutzberater Zugang zu allen Informationen, Dokumenten, Verzeichnissen von Bearbeitungstätigkeiten und allen Personendaten gewähren, die er zur Erfüllung seiner Aufgaben benötigt
- dafür sorgen, dass der Datenschutzberater über jede Verletzung der Datensicherheit informiert wird

Plan

Einführung

Anwendbare Regelung

Verzeichnis der Bearbeitungstätigkeiten

Informationspflicht

Bearbeitungsreglement

Datenschutzberaterin oder -berater

Verträge mit einer Übermittlung von Personendaten

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

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

Outsourcing	Empfänger	Status nach dem DSG
Technische und administrative Verwaltung	Externe Verwaltung	Auftragsbearbeiter (ASIP) oder Verantwortlicher je nach Grad der Unabhängigkeit des Dienstleisters
Datenspeicherung und -verwaltung	Anbieter von IT-Dienstleistungen	Auftragsbearbeiter: Der IT-Dienstleister handelt auf Anweisung der VE. Der Zweck und die Mittel der Verarbeitung werden von der VE als für die Bearbeitung Verantwortlicher festgelegt.
Expertise in Sachen Vorsorge	Experte für berufliche Vorsorge	Auftragsbearbeiter (OAK BV) oder unabhängiger Verantwortlicher
Überprüfung von Finanzberichten	Revisionsstelle	Unabhängiger Verantwortlicher / Drittperson (verarbeitet in der Regel keine personenbezogenen Daten der VE)
Hinterlegung und/oder Verwaltung von Vermögenswerten	Depotbank / Vermögensverwalter	Unabhängiger Verantwortlicher / Drittperson (verarbeitet in der Regel keine personenbezogenen Daten der VE)
Rückversicherung	Versicherungsgesellschaft	Unabhängiger Verantwortlicher

Vielen Dank für Ihre Aufmerksamkeit

Philipp Fischer
Associé, LL.M. (Harvard)
pfischer@obersonabels.com
+41 58 258 88 88