Neues DSG: Auswirkungen auf Pensionskassen und Pensionsversicherungsexperten?

SAV – Schweizerische Aktuarvereinigung
27. August 2021

RA Dr. David Vasella, CIPP/E, CIPM

walderwyss rechtsanwälte

Einleitung und Übersicht

Zur DSGVO

- Treiber der Entwicklungen: Datenschutz-Grundverordnung (**DSGVO**)
- auf VE kaum anwendbar:
  - Niederlassung im EWR (einschliesslich FL)?
  - Ausrichtung von Angeboten auf natürliche Personen in FL (Grenzgänger genügen nicht)?
  - «Verhaltensbeobachtung»: z.B. Online-Tracking – ggf. auf Tracking von Personen aus dem EWR verzichten

Entstehung des revDSG

- langer Vorlauf (seit ca. 2014)
- 15. September 2017: Entwurf und Botschaft des Bundesrats
- 23. Juni 2021: Entwurf der revidierten Verordnung
- Mitte/Ende 2022: Inkrafttreten
- fast keine Übergangsfristen!

Stand heute

- Ansprüche der betroffenen Personen nicht häufig
  - Auskunfts- und Berichtigungsrecht
  - zivilrechtliche Ansprüche
- kaum relevante Strafdrohungen
  - falsche oder unvollständige Auskunft
  - Verletzung bestimmter Informationspflichten, etc.
- relevanter: Verletzung der Schweigepflicht (Art. 76 und 86a BVG; Gefängnis- und Bussendrohung
- Behörden nicht besonders aktiv (eher in der OKP)

Das DSG bekommt Zähne

- Totalrevision DSG/VDSG
- diverse neue Pflichten
- Bussen für Einzelpersonen (!) bis zu CHF 250’000
- Aufmerksamkeit für Datenschutzthemen stark steigend
- strengere Aufsichtsbehörden

+ Informationen: datenrecht.ch

Wesentliche Neuerungen (allgemein)

- Datenschutzerklärungen auch in Bagatellfällen
- Governance:
  - Bearbeitungsverzeichnisse
  - Folgenabschätzungen
  - Meldung von Datensicherheitsverletzungen
- neue Konzepte:
  - Profiling und Profiling mit hohem Risiko
  - automatisierte Einzelentscheidungen
- Stärkung der Betroffenenrechte
- neue Kompetenzen des EDÖB
- neue Strafsanktionen in bestimmten Fällen

Wesentliche Neuerungen (Vorsorge)

- Art. 85a Abs. 2 BVG: Gesetzesgrundlage für «Persönlichkeitsprofile»
- … aber *keine* Grundlage für das Profiling (BSV: nicht nötig… wie im KVG; anders UVG, da Realleistungsprinzip)
- keine Änderung bei der Schweigepflicht nach BVG, aber Datengeheimnis nach Art. 62 revDSG
- Weitergehende Informationspflicht (Überobligatorium)

Handlungsempfehlungen

❶ Rollen definieren

- Verantwortliche vs. Auftragsbearbeiter
  - Verantwortliche: definieren Zweck und wesentliche Rahmenbedingungen der Bearbeitung
  - Auftragsbearbeiter: bearbeiten fremde Daten im Auftrag
  - jeweils die Unternehmen, nicht einzelne Mitarbeiter
- Verantwortliche:
  - Vorsorgeeinrichtungen (strittig)
  - Geschäftsführer
  - Rückversicherer
  - Broker
  - externe Berater
- Auftragsbearbeiter:
  - IT-Dienstleister (Hosting, SaaS-Angebote usw.)
  - Versanddienstleistungen

❶ Rollen definieren

- Verantwortliche untereinander
  - keine zwingenden Bestimmungen
  - Geschäftsführungsvertrag: Regelung der Verantwortlichkeiten und Zuständigkeiten, Weisungsrechte, Zweckbindung, Schweigepflicht, Umgang mit Betroffenenrechten usw.
- Verantwortliche/Auftragsbearbeiter
  - neu: vertragliche Regelung zwingend («ADV»; revDSG: Strafbarkeitsrisiko)
  - wenige Mindestinhalte; i.d.R. aber Vertrag nach dem DSGVO-Standard
- Aufgaben:
  - vertragliche Regelung mit Geschäftsführer treffen
  - ADV mit IT-Dienstleistern schliessen

❷ Information sicherstellen

- heute:
  - aktive Informationspflicht in der obligatorischen, nicht der ausser-/überobligatorischen Vorsorge
- **neu**: aktive Informationspflicht privater Bearbeiter
  - Informationspflicht (nur) in der ausser-/überobligatorischen Vorsorge
  - strafbewehrt
- Aufgaben:
  - Datenschutzerklärung(en) entwerfen
    - ggf. gemeinsam: VE und Geschäftsführer
  - Information planen
    - Arbeitgeber: z.B. im Anschlussvertrag
    - Destinatäre: Information via Arbeitgeber? Informationspflicht überbinden im Anschlussvertrag? Hinweis im Vorsorgeausweis? Website?

❸ Daten-bearbeitungen begrenzen

- VE:
  - interne Datenflüsse und Zugriffe begrenzen
    BVGE 2012/14: «[…] auch innerhalb derselben Behörde […], solange damit nicht die Durchführung der beruflichen Vorsorge verunmöglicht wird»
  - Speicherdauer begrenzen, Löschung sicherstellen (s. Art. 27i ff. BVV 2)
- Geschäftsführer:
  - interne Datenflüsse und Zugriffe begrenzen (Schweigepflicht gilt auch für den GF); «chinese walls» obligatorische Vorsorge und andere Tätigkeiten
  - Speicherdauer begrenzen, Löschung sicherstellen

❸ Daten-bearbeitungen begrenzen

- Bsp. Marketing durch Geschäftsführerin für private Vorsorgeprodukte
  - zumindest Einwilligung der Destinatäre *im Einzelfall* (für die Zweckänderung)
  - falls interne oder externe Bekanntgabe von Daten: (hand-)schriftliche Einwilligung im Einzelfall

❹ Governance sicherstellen

- **neu**: Bearbeitungsverzeichnisse
  - Pflicht, ein Bearbeitungsverzeichnis zu führen (Excel oder Word mit Inventar der bearbeiteten Personendaten)
  - Bundesorgane: Meldung des Verzeichnisses an den EDÖB
- **neu**: Datenschutz-Folgenabschätzungen
  - strukturierte Bewertung der Risiken für Betroffene
  - bei hochriskanten Bearbeitungen, z.B. «umfangreiche Bearbeitung besonders schützenswerter Personendaten»
- **neu**: Meldung von Datensicherheitsverletzungen
  - «breach notification»: Meldung ggü. dem EDÖB (bei hohen Risiken) und den Betroffenen (falls erforderlich)
  - Prävention (Schulung der Mitarbeiter, z.B. betr. Phishing) und Vorbereitung (z.B. auf Ransom-Angriffe) sinnvoll

Vielen Dank!

RA Dr. David Vasella , CIPP/E, CIPM

+41 58 658 52 87
+41 79 417 23 22
david.vasella@walderwyss.com

walderwyss rechtsanwälte