

Neues Datenschutzgesetz

Auswirkungen auf Vorsorgeeinrichtungen

Die Schweiz revidiert ihr Datenschutzgesetz (DSG), um den veränderten technologischen und gesellschaftlichen Verhältnissen Rechnung zu tragen. Es sollen die Transparenz von Datenbearbeitungen verbessert und die Selbstbestimmung der betroffenen Personen über ihre Daten gestärkt werden.

IN KÜRZE

Die revidierten Datenschutzbestimmungen könnten per Mitte 2022 in Kraft gesetzt werden. Vor dem Hintergrund möglicher Sanktionen und eines Reputationschadens bei Verletzungen sollte dem Thema rechtzeitig Aufmerksamkeit geschenkt und die nötigen Anpassungen umgesetzt werden.

Die Revision des DSG ist insbesondere auch vor dem Hintergrund der europäischen Verordnung (EU) 2016/679 vom 27. April 2016, der Datenschutz-Grundverordnung (DSGVO), zu sehen. Für die Schweiz ist es zentral, von der EU weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkannt zu werden, damit die grenzüberschreitende Datenübermittlung auch künftig ohne Hürden möglich bleibt. Die Schweizer Datenschutzbestimmungen werden zu diesem Zweck an die DSGVO angeglichen, weichen jedoch in diversen Punkten von den Regelungen der DSGVO ab («Swiss Finish»).

Die Totalrevision des DSG wurde am 25. September 2020 vom Parlament verabschiedet. Aktuell wird die Anpassung der Ausführungsbestimmungen vorbereitet, insbesondere der Verordnung zum Datenschutzgesetz (VDSG). Die Vernehmlassung zur Revision der VDSG soll in der ersten Jahreshälfte 2021 eröffnet werden. Die revidierten Datenschutzbestimmungen könnten per Mitte 2022 in Kraft gesetzt werden.

Welche Datenschutzbestimmungen gelten für Vorsorgeeinrichtungen?

In der beruflichen Vorsorge ist zu beachten, dass die spezialgesetzlichen Datenschutzvorschriften des BVG und des FZG (Art. 85a ff. BVG und Art. 25 FZG) die Vorschriften des DSG mitunter verdrängen. Vorsorgeeinrichtungen, welche die obligatorische berufli-

che Vorsorge durchführen, unterliegen den vorsorgerechtlichen Datenschutzvorschriften. Die Vorschriften des DSG, insbesondere die Grundsätze der Datenbearbeitung (Art. 6 revDSG), kommen ergänzend zur Anwendung. Vorsorgeeinrichtungen gelten unter dem DSG als Bundesorgane und benötigen für die Bearbeitung und Bekanntgabe von Personendaten eine gesetzliche Grundlage, welche mit Art. 85a ff. BVG vorliegt.

Im Bereich der weitergehenden, über- und ausserobligatorischen beruflichen Vorsorge gelten Vorsorgeeinrichtungen als private Personen und es sind allein die Vorschriften des DSG (mit den in Art. 49 Abs. 2 BVG genannten Ausnahmen) anwendbar. Als private Personen dürfen sie Personendaten auch ohne gesetzliche Grundlage bearbeiten, sofern die Persönlichkeit der betroffenen Personen dabei nicht widerrechtlich verletzt wird. An dieser Systematik ändert das totalrevidierte DSG nichts.

Was ist anders im revidierten DSG?

Das revDSG gilt nach wie vor für die Bearbeitung von Personendaten natürlicher Personen, also Angaben, die sich auf eine bestimmte oder bestimmbar natürliche Person beziehen. Besondere Regeln gelten für besonders schützenswerte Personendaten wie beispielsweise Gesundheitsdaten. Daten von juristischen Personen werden demgegenüber vom revDSG nicht mehr erfasst.



Evelyn Schilter
Lic. iur., Rechtsanwältin,
LL.M.,
Willis Towers Watson



Estelle Caveng
MLaw,
Willis Towers Watson

Die Grundsätze der Datenbearbeitung bleiben im Wesentlichen gleich. Nach wie vor wird eine rechtmässige und verhältnismässige Bearbeitung vorausgesetzt. Die Daten dürfen nur zweckgemäss beschafft und bearbeitet werden und sind zu vernichten, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind. Neuerungen bestehen insbesondere im Bereich von Entscheidungen, die ausschliesslich automatisch getroffen werden (Profiling und Profiling mit hohem Risiko). Der Datenschutz muss weiterhin auch technisch gewährleistet sein. Neu sind datenschutzfreundliche Voreinstellungen («privacy by design and default») erforderlich (Art. 7 Abs. 3 revDSG).

Hinsichtlich der Prozesse und Dokumentation gibt es verschiedene Neuerungen: Insbesondere muss neu ein Verzeichnis der Bearbeitungstätigkeiten erstellt, über die Beschaffung von Personendaten informiert, ein Prozess zur Datenschutz-Folgenabschätzung und zur Meldung von Verletzungen der Datensicherheit eingeführt sowie der Prozess zur Auskunftserteilung angepasst und ein neuer Prozess für die Datenherausgabe oder -übertragung auf Verlangen eingeführt werden.

Zum Vollzug des revDSG ist anzumerken, dass der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) weitergehende Untersuchungs- und Handlungskompetenzen erhält und Verwaltungsmassnahmen ergreifen kann (Art. 49 ff. revDSG). Der EDÖB kann für bestimmte Dienstleistungen unter dem revDSG gegenüber privaten Personen Gebühren erheben (Art. 59 revDSG). Sodann werden der Anwendungsbereich der Sanktionen erweitert und die möglichen Bussen, die neu bis zu 250 000 Franken betragen können, signifikant erhöht.

Zudem werden die gesetzliche Grundlage für die Bearbeitung von Personen-

daten in der obligatorischen beruflichen Vorsorge redaktionell angepasst und eine ausdrückliche gesetzliche Grundlage für die Bearbeitung von Personendaten zur Beurteilung der Gesundheit, der Bedürfnissen und der wirtschaftlicher Situation der versicherten Person eingeführt (Art. 85a revBVG), mithin für die Bearbeitung von besonders schützenswerten Personendaten nach Art. 5 lit. c revDSG.

Wo haben Vorsorgeeinrichtungen Handlungsbedarf?

In Beachtung, dass die noch ausstehenden Ausführungsbestimmungen des Bundesrats weitere Anpassungen erfordern könnten, besteht aus heutiger Sicht insbesondere in folgenden Bereichen Handlungsbedarf:

- Anpassen der Datenschutzdokumente (neue Terminologie; Art. 5 revDSG) und der Datenschutzverträge (insbesondere betreffend Auftragsbearbeitung; Art. 9 revDSG);
- Implementieren datenschutzfreundlicher Voreinstellungen («privacy by design and default»; Art. 7 Abs. 3 revDSG);
- Erstellen eines Verzeichnisses der Bearbeitungstätigkeiten (Art. 12 revDSG);
- Überprüfung, ob Datentransfers ins Ausland stattfinden und datenschutzrechtlich genügend geschützt sind (Art. 16 revDSG);
- Implementierung einer Datenschutzerklärung bei der Beschaffung von Personendaten (neue Informationspflicht; Art. 19 f. revDSG);
- Eruieren, ob eine Datenschutz-Folgenabschätzung nötig ist und entsprechend eines festgelegten Prozesses erarbeitet werden kann (Art. 22 revDSG) sowie gegebenenfalls Implementierung eines Prozesses zur Konsultation des EDÖB (Art. 23 revDSG);
- Implementierung von Prozessen zur Meldung von Verletzungen der Daten-

sicherheit (Art. 24 revDSG), zur Auskunft über Datenbearbeitungen im Einklang mit dem revidierten DSG (Art. 25 revDSG) und zur Datenherausgabe oder -übertragung (Art. 28 f. revDSG).

Umsetzung

Die Vorsorgeeinrichtungen müssen mit Blick auf das revidierte Datenschutzgesetz insbesondere ihre Datenbearbeitungsprozesse analysieren, dokumentieren und anpassen, Datenschutzdokumente und -vereinbarungen prüfen und anpassen, Datenschutz durch technische Vorkehrungen und datenschutzfreundliche Voreinstellungen gewährleisten und die Informationsrechte und -pflichten sicherstellen. Umhüllende Einrichtungen sollten eine Lösung anstreben, welche die unterschiedlichen Anforderungen an Bundesorgane und private Personen in Einklang bringt.

Mit einem systematischen Ansatz und einem straff geführten Umsetzungsprojekt sollten die erforderlichen Anpassungen in der Regel relativ schlank umsetzbar sein. Vor dem Hintergrund möglicher Sanktionen und eines Reputationsschadens bei Verletzungen sollte dem Thema rechtzeitig Aufmerksamkeit geschenkt und die nötigen Anpassungen umgesetzt werden. ■