Neues Datenschutzgesetz

Praxisorientierte Umsetzung für Vorsorgeeinrichtungen

Das neue Datenschutzrecht tritt am 1. September 2023 in Kraft und birgt einige neue Herausforderungen, die ebenfalls Auswirkungen auf die Vorsorgeeinrichtungen haben. Es lohnt sich daher, die bisherigen Datenschutzkonzepte rechtzeitig zu überprüfen und gemäss der neuen Gesetzgebung zu aktualisieren.

Rebecca Lang
MLaw, Libera AG

Nicole A.M. Gisler
MLaw, MAS Pensionskassen Management, Libera AG

Am 31. August 2022 wurde vom Bundesrat das definitive Inkrafttreten des totalrevidierten Datenschutzgesetzes (E-DSG), der neuen Datenschutzverordnung sowie der neuen Verordnung über Datenschutzzertifizierungen per 1. September 2023 beschlossen.[1]

Hybride Funktion der registrierten Vorsorgeeinrichtungen

Registrierte Vorsorgeeinrichtungen nehmen gemäss dem revidierten Datenschutzgesetz eine hybride Funktion wahr – im Bereich des Obligatoriums gelten sie als Bundesorgane und im Bereich des Überobligatoriums als private Verantwortliche. In der Praxis empfiehlt es sich, keine Unterscheidung zwischen den beiden Funktionsweisen zu machen, sondern nach der jeweils strengeren Vorschrift zu handeln. Auf die Situation von rein überobligatorischen Vorsorgeeinrichtungen oder kantonalen Vorsorgeeinrichtungen, die den kantonalen Bestimmungen unterstehen, wird nachfolgend nicht eingegangen.[2]

Hohe Bussen für vorsätzliche Pflichtverletzungen

Bisher waren keine schwerwiegenden Sanktionsvorschriften in der datenschutzrechtlichen Gesetzgebung verankert und für die Umsetzung der datenschutzrechtlichen Verpflichtungen bestand ein Vollzugsdefizit. Mit der neuen Gesetzgebung soll dies nun geändert werden. Insbesondere soll mit der Einführung von neuen Pflichten und der wesentlich höheren Sanktionsmöglichkeit (Busse bis 250 000 Franken) sichergestellt werden, dass die EU die schweizerische Regelung als angemessen erachtet.[3] Es lohnt sich deshalb, die datenschutzrechtlichen Vorgaben einzuhalten.

Ernennung Datenschutzberater

Die Ernennung eines Datenschutzberaters oder einer Datenschutzberaterin ist für Bundesorgane und somit für registrierte Vorsorgeeinrichtungen obligatorisch. Die Datenschutzberaterin ist die Anlaufstelle sowohl für betroffene Personen und Behörden als auch für die Vorsorgeeinrichtung.[4] Sie schult und berät die Vorsorgeeinrichtung und wirkt bei der Umsetzung der datenschutzrechtlichen Vorschriften im Betrieb mit.[5] Der Datenschutzberater muss daher über die erforderlichen Fachkenntnisse verfügen, fachlich unabhängig und weisungsungebunden sein. Hierfür kann eine Person in Frage kommen, die selbst keine Personendaten bearbeitet und deren weitere Tätigkeiten für die Vorsorgeeinrichtung in keinem Spannungsverhältnis zur Auf-

[1] Medienmitteilung Bundesrat vom 31. August 2022.
[2] Vgl. Fachmitteilung Nr. 130 des ASIP.
[3] S. BBl 2017 7099 ff.
[4] Erläuternder Bericht zur Revision der Verordnung über den Datenschutz, S. 52/99.
[5] S. Art. 10 Abs. 2 E-DSG.

gabe als Datenschutzberaterin stehen.[6] Zu denken wäre z. B. an einen Datenschutzberater eines angeschlossenen Arbeitgebers, eine eigene interne Stelle, die keine Personendaten bearbeitet oder einen unabhängigen Dienstleister.

Umsetzung der Dokumentationspflicht

Bereits aktuell besteht für Bundesorgane unter gewissen Voraussetzungen die datenschutzrechtliche Verpflichtung, ein Register der Datensammlung zu erstellen.[7] Ist dieses bereits vorhanden, so ist es anhand der neuen gesetzlichen Anforderungen zu überprüfen und entsprechend zu ergänzen. Ist ein solches Register noch nicht vorhanden, muss ein solches gemäss den neuen gesetzlichen Anforderungen erstellt werden.[8] Das Bearbeitungsverzeichnis ist dem EDÖB (dem Eidgenössischen Daten- und Öffentlichkeitsbeauftragten) einzureichen und wird von ihm veröffentlicht.[9]

Anforderungen an die technischen und organisatorischen Massnahmen, um die Datensicherheit zu gewährleisten, bestehen bereits heute. Mit der neuen Gesetzgebung werden diese jedoch ausgebaut und präzisiert.[10] Es empfiehlt sich deshalb, die Dokumentation der technischen und organisatorischen Massnahmen sowie die Archivierungs- bzw. Löschkonzepte zu überprüfen und zu aktualisieren.

Neue Pflicht zur Risikobeurteilung

Um Risiken, die für eine betroffene Person durch die Datenbearbeitung entstehen können, zu erkennen und zu bewerten, ist gemäss dem neuen Gesetz jeder Verantwortliche (also Bundesorgane und private Verantwortliche) verpflichtet, eine Datenschutzfolgenabschätzung vorzunehmen, sofern ein Bearbeitungsprozess oder mehrere ähnliche Bearbeitungsprozesse ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen birgt.[11]

Ein Bearbeitungsprozess birgt ein solch hohes Risiko, wenn z. B. die Eintrittswahrscheinlichkeit (gemessen an Anzahl involvierter Drittparteien und -länder, Anzahl Zugriffsberechtigter etc.) der Datenschutzverletzung und das damit einhergehende Schadenausmass (gemessen anhand der Kategorie Personendaten, Anzahl betroffener Personen und der Auswirkungen der Verletzung) erheblich sind.

Anhand der Datenschutzfolgeabschätzung zeigt der Verantwortliche auf, welche technischen und organisatorischen Massnahmen er trifft, um das hohe Risiko einzudämmen. Wichtig: Es handelt sich hier um eine eigene Einschätzung, die nach bestem Wissen und Gewissen vorzunehmen ist. Da eine gesetzliche Aufbewahrungspflicht der Datenschutzfolgenabschätzung besteht, ist eine entsprechende Dokumentation zu empfehlen.

Datenbearbeitung durch Dritte

Wie nach dem bisherigen Recht ist die Übertragung von Aufgaben durch einen Verantwortlichen an Dritte (Auftragsbearbeiter) möglich. Die registrierte Vorsorgeeinrichtung muss sich als Verantwortliche vergewissern, dass ihre Auftragsbearbeiter in der Lage sind, die neuen Anforderungen an die Datensicherheit ebenfalls zu gewährleisten.[12] Sollte nicht bereits eine vertraglich hinreichende Grundlage vorliegen, kann dies mittels Auftragsdatenbearbeitungsvereinbarung (ADV) gewährleistet werden. Damit der Verantwortliche der gesetzlich festgelegten Vergewisserungspflicht auch nachkommt, ist es empfehlenswert, die Dokumentation der technischen und organisatorischen Massnahmen und die Bestätigung der jährlichen Überprüfung durch den Auftragsbearbeiter einzuholen. Für das Hinzuziehen eines Subunternehmers ist neu die Einwilligung des Verantwortlichen, also der registrierten Vorsorgeeinrichtung, erforderlich, weshalb die beauftragten Subunternehmer in der ADV miteinzubeziehen sind, mit der Pflicht, die Einhaltung der Datensicherheit zu gewährleisten.

Information bei der Beschaffung von Personendaten

Die Informationspflicht des Verantwortlichen bei der Beschaffung von Personendaten wurde vereinheitlicht und gilt neu sowohl für Bundesorgane als auch Private. Um die Informationspflicht regelmässig und adäquat umzusetzen, ergeben sich für registrierte Vorsorgeeinrichtungen folgende Möglichkeiten, die Versicherten zu informieren:

- Merkblatt bei Anstellungsbeginn und jährliches Infoschreiben an Mitarbeiter,
- Reglement,
- Jahresbericht.

Betreibt eine Vorsorgeeinrichtung zudem eine eigene Website, ist zu prüfen, ob benutzerfreundliche Voreinstellungen vorzunehmen sind (Stichwort: «Privacy by Design and Default»).

Damit eine Datenbearbeitung bei privaten Verantwortlichen nicht widerrechtlich ist, bedarf es eines Rechtfertigungsgrunds (z. B. Erfüllung des Vorsorgevertrages). Bei Fällen, in denen besonders heikle Daten bearbeitet werden, wie dies z. B. bei Invaliditätsfällen der Fall ist, empfiehlt es sich zu prüfen, ob eine Einwilligung der betroffenen Person einzuholen ist.

Weitere Prozesse

Ebenfalls haben die registrierten Vorsorgeeinrichtungen weitere Prozesse zu bestimmen, um die gesetzliche Meldepflicht bei Datenschutzverletzungen einzuhalten und die Rechte der betroffenen Personen wahrnehmen zu können.

TAKE AWAYS

- Die neuen Verpflichtungen sowie die allfällige Aktualisierung der bereits vorhandenen Dokumente sind umfassend und erfordern einen gewissen Zeit- und Ressourcenaufwand, weshalb möglichst bald mit der Umsetzung angefangen werden sollte.
- Nachdem sich die registrierte Vorsorgeeinrichtung einen Überblick über die aktuelle Situation verschafft hat, kann die etappenweise Umsetzung bzw. Überprüfung vorgenommen werden.

Mehr zum Thema

Der Akzentteil der Februarausgabe 2023 befasst sich mit dem Datenschutz.

[6] S. Art. 26 Abs. 1 E-DSV.
[7] S. Art. 11a Abs. 2 DSG.
[8] S. Art. 12 Abs. 2 E-DSG.
[9] S. Art. 12 Abs. 4 E-DSG i.V.m. Art. 56 E-DSG.
[10] S. Art. Art. 8 E-DSG i.V.m. Art. 1 ff. E-DSV.
[11] S. Art. 22 E-DSG.
[12] Art. 9 Abs. 2 nDSG.