Beziehung mit Dritten

Datenaustausch mit Dienstleistern

Vorsorgeeinrichtungen stehen mit einer Vielzahl von Dritten in Beziehung, mit denen oft auch ein Datenaustausch stattfindet. Wir gehen der Frage nach, was es mit Blick auf den Datenschutz beim Austausch von Daten mit Dritten zu beachten gilt.

Evelyn Schilter
Rechtsanwältin, lic. iur., LL.M, WTW

Estelle Caveng
Legal Consultant, MLaw, WTW

Zunächst ist zu eruieren, welche Regelungen anwendbar sind: In der obligatorischen (und umhüllenden) Vorsorge gilt es vorab, die in Art. 86 BVG verankerte Schweigepflicht mit den in Art. 85a, 85b und 86a ff. BVG definierten Ausnahmen zu beachten. Nach Art. 86 BVG haben Personen, die an der Durchführung sowie der Kontrolle oder Beaufsichtigung der Durchführung des BVG beteiligt sind, gegenüber Dritten Verschwiegenheit zu bewahren. Diese Pflicht gilt auch für beauftragte Dritte. In der weitergehenden beruflichen Vorsorge gelten demgegenüber die zivilrechtlichen Behelfe des Persönlichkeitsschutzes[1] und der datenschutzrechtliche Berufsgeheimnisschutz.[2]

Im Datenschutz gelten Vorsorgeeinrichtungen, die das Obligatorium durchführen (und damit auch umhüllende Vorsorgeeinrichtungen) und Freizügigkeitseinrichtungen als Bundesorgane.[3] Für eine Datenbearbeitung durch Bundesorgane ist eine gesetzliche Grundlage erforderlich[4], die insbesondere mit Art. 85a ff. BVG und Art. 25 FZG vorliegt. Die Bestimmungen des Datenschutzrechts sind ergänzend anwendbar.

Demgegenüber gelten Pensionskassen mit ausschliesslich ausser- oder überobligatorischen Leistungen wie 1e-Stiftungen und patronale Stiftungen als Privatpersonen. Sie unterliegen den Bestimmungen des Datenschutzrechts und dürfen Personendaten auch ohne gesetzliche Grundlage bearbeiten, wenn die Persönlichkeit der betroffenen Personen nicht verletzt wird oder Rechtfertigungsgründe vorliegen.

Diese Unterscheidung besteht bereits im aktuellen Datenschutzrecht. Neu ist indessen z. B., dass Bundesorgane – im Unterschied zu privaten Personen – ihr Verzeichnis der Bearbeitungstätigkeiten dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)[5] melden und einen Datenschutzberater ernennen[6] müssen.

Wann liegt eine relevante Bearbeitung von Personendaten vor?

Sodann ist vorab festzuhalten, dass die Datenschutzbestimmungen nur dann greifen, wenn Personendaten bearbeitet werden. Jeder Umgang mit Personendaten ist ein relevanter Bearbeitungsvorgang im Sinne des Datenschutzgesetzes.[7]

Personendaten sind Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person[8] beziehen. Dies ist dann der Fall, wenn eine Partei aufgrund der übermittelten Daten oder zusammen mit ihr sonst zur Verfügung stehenden Daten eine individuelle Person identifizieren kann.

Werden Individualdaten pseudonymisiert, also z. B. der Name durch eine Nummer ersetzt, und hat der Dritte den Schlüssel zur Zuordnung der Nummern zu einzelnen Individuen nicht, so sind die pseudonymisierten Daten aus Sicht dieses Dritten keine Personendaten im Sinne

1 Art. 28 ZGB.
2 Art. 35 DSG; Art. 62 revDSG.
3 Nach Art. 5 lit. i revDSG ist ein Bundesorgan eine Behörde oder Dienststelle des Bundes oder eine Person, die mit öffentlichen Aufgaben des Bundes betraut ist.
4 Art. 34 Abs. 1 revDSG.
5 Art. 12 Abs. 4 revDSG.
6 Art. 25 ff. DSV.
7 Art. 5 lit. d revDSG, also insbesondere das Beschaffen, Übertragen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Personendaten.
8 Art. 5 lit. a revDSG.

des Datenschutzrechts. Die folgenden Ausführungen gelten für die Bearbeitung von Personendaten.

Agiert der Dritte als Controller oder Processor?

Aus datenschutzrechtlicher Sicht erfolgen Datenbearbeitungen entweder in eigener Verantwortung (als Controller) oder als Auftragsbearbeiter (Processor). Verantwortlich ist eine private Person oder ein Bundesorgan, die allein oder zusammen mit anderen über den Zweck (das Wieso?) und die Mittel (das Wie?) der Bearbeitung entscheidet.[9] Auftragsbearbeiter ist eine private Person oder ein Bundesorgan, die im Auftrag des Verantwortlichen Personendaten bearbeitet.[10]

Die Abgrenzung kann im Einzelfall schwierig sein. Nicht jedes zivilrechtliche Auftragsverhältnis macht den Dritten zum Auftragsbearbeiter. Dies ist nur dann der Fall, wenn der Dritte nicht frei über den Zweck und die Mittel der Bearbeitung entscheiden kann. So arbeitet z. B. der externe Rechtsanwalt zwar zivilrechtlich im Auftragsverhältnis, dennoch entscheidet er frei darüber, wieso, welche und wie er die Daten bearbeitet, um die sich stellende Rechtsfrage zu beantworten. Analoges gilt für den Pensionskassenexperten und die Revisionsstelle, die ihre eigenen gesetzlichen Aufträge haben, in deren Ausübung sie eigenverantwortlich über die Bearbeitung der Daten entscheiden.

Anders liegt die Situation z. B. bei einem Dritten, der die technische Verwaltung der Vorsorgeeinrichtung im Auftragsverhältnis ausführt. Der Dritte übernimmt hier die Aufgabe der Vorsorgeeinrichtung und bearbeitet die Daten als verlängerter Arm der Vorsorgeeinrichtung nach Massgabe der gesetzlichen und reglementarischen Bestimmungen, die für die Vorsorgeeinrichtung gelten, und an deren Stelle.

Was ist die Folge dieser Qualifikation?

Weshalb ist diese Unterscheidung, und damit die Qualifikation des Dritten als Verantwortlicher oder Auftragsbearbeiter wichtig? Die Hauptunterschiede sind in der Tabelle zusammengestellt (nicht abschliessend).

Daraus ergibt sich, dass der Verantwortliche wesentlich weitergehende Pflichten hat und die Gesamtverantwortung für die Datenbearbeitung auch des Auftragsbearbeiters trägt. Dem Verantwortlichen ist zu empfehlen, im Vorfeld der Beauftragung eines Auftragsbearbeiters die Anforderungen an die Datensicherheit zu prüfen (Due Diligence, Abstellen auf eine Zertifizierung) und sich vertraglich das Recht für periodische Überprüfungen (Audit Rights) einräumen zu lassen.

[9] Art. 5 lit. j revDSG.
[10] Art. 5 lit. k revDSG.

TAKE AWAYS

- Infolge der Revision des Datenschutzrechts erfordert der Austausch von Personendaten mit Dritten besondere Aufmerksamkeit.
- Die Unterscheidung, und damit die Qualifikation des Dritten als Verantwortlicher oder Auftragsbearbeiter ist wichtig, da der Verantwortliche weitergehende Pflichten hat.
- Dem Verantwortlichen ist zu empfehlen, im Vorfeld der Beauftragung eines Auftragsbearbeiters die Anforderungen an die Datensicherheit zu prüfen und sich vertraglich das Recht für periodische Überprüfungen einräumen zu lassen.
- Ein Datentransfer in Länder der EU ist in der Regel unproblematisch, während bei einem Datentransfer in andere Länder weitere Abklärungen nötig werden.

Abgrenzung Verantwortlicher und Auftragsbearbeiter

Verantwortlicher	– Bleibt für die Datenbearbeitung verantwortlich, auch wenn er sie einem Auftragsbearbeiter überträgt. Die Übertragung muss auf der Grundlage eines Vertrags («Controller to Processor Agreement») oder eines Gesetzes erfolgen.[1] – Bei Übertragung der Daten an einen Verantwortlichen endet die Verantwortung des Übertragenden bezüglich der Bearbeitung durch den Dritten mit der Übertragung an den Dritten. Der übernehmende Dritte verantwortet die korrekte Bearbeitung selbst. – Datenbearbeitung ist technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden. – Muss datenschutzfreundliche Voreinstellungen vornehmen (Art. 7 revDSG). – Muss sich vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten (Art. 9 Abs. 2 revDSG). – Information der betroffenen Personen über die Bearbeitung, insbesondere auch über eine Bekanntgabe ins Ausland (Art. 19 ff. revDSG). – Durchführung von Datenschutz-Folgenabschätzungen (Art. 22 ff. revDSG). – Information an EDÖB und/oder betroffene Personen über eine Verletzung der Datensicherheit (Art. 24 revDSG). – Auf Verlangen einer betroffenen Person: Auskunft über Datenbearbeitung bzw. Herausgabe/Übertragung der Daten (Art. 25 ff. revDSG).
Verantwortlicher und Auftragsbearbeiter	– Verzeichnis der Bearbeitungstätigkeiten. Bezüglich Inhalte, die im Verzeichnis wiederzugeben sind, bestehen Unterschiede.[2] – Durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit gewährleisten. Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.[3]
Auftragsbearbeiter	– Darf Daten nur so bearbeiten, wie es der Verantwortliche selbst auch tun dürfte und nur dann, wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet. – Darf die Bearbeitung seinerseits nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen (Art. 9 Abs. 3 revDSG, Art. 7 DSV). – Meldet eine Verletzung der Datensicherheit dem Verantwortlichen (Art. 24 Abs. 3 revDSG).

[1] Art. 9 Abs. 1 revDSG: Bei einer Übertragung an einen Verantwortlichen ist der Abschluss einer Vereinbarung (Controller to Controller Agreement) nicht zwingend, aber zu empfehlen.
[2] Art. 12 revDSG: Art. 12 Abs. 2 revDSG schreibt den Mindestinhalt für das Bearbeitungsverzeichnis eines Verantwortlichen vor, Art. 12 Abs. 3 revDSG den Inhalt des Bearbeitungsverzeichnisses des Auftragsbearbeiters.
[3] Art. 8 revDSG und Art. 1 ff. DSV: Für automatisierte Bearbeitungen gelten erhöhte Anforderungen (vgl. Pflichten zur Protokollierung und zum Erlass eines Bearbeitungsreglements nach Art. 4 ff. DSV).

Was gilt es bei einem Datentransfer ins Ausland zu beachten?

Ein Datentransfer ist nur zulässig:[11]

- in ein Land mit einem vom Bundesrat anerkannten angemessenen Datenschutzniveau,
- wenn durch besondere Schutzmassnahmen ein geeigneter Datenschutz gewährleistet werden kann, oder
- wenn eine gesetzliche Ausnahme vorliegt, z. B. die betroffene Person ausdrücklich in die Bekanntgabe eingewilligt hat.

Ein Datentransfer in Länder der EU ist in der Regel unproblematisch, während bei einem Datentransfer in andere Länder weitere Abklärungen nötig sind. Bei einem Datentransfer ins Ausland sind auch die Versicherten zu informieren.[12]

Schweizer Vorsorgeeinrichtungen dürften ihre Daten regelmässig primär in der Schweiz bearbeiten. Dennoch ist zu prüfen, ob nicht doch (unbeabsichtigt) Personendaten ins Ausland übermittelt werden, z. B. in folgenden Konstellationen:

- Betriebseigene Pensionskassen mit IT-Anbindung an den Arbeitgeber,
- Beauftragung und Bearbeitung von Personendaten durch einen Dienstleister,
- Datenspeicherung in Cloud-Lösungen,
- Erbringen von Vorsorgeleistungen ins Ausland.

Diesfalls wäre zu prüfen, ob die Bekanntgabe im konkreten Fall den Anforderungen des revDSG genügt und zulässig ist.

[11] Art. 16 f. revDSG; Art. 8 ff. DSV; Die Liste der Länder mit angemessenem Datenschutz findet sich in Anhang 1 der DSV.

[12] Art. 19 Abs. 4 DSG.

Relations avec des tiers

Échange de données avec des prestataires de services

Les institutions de prévoyance sont en relation avec un grand nombre de tiers avec lesquels un échange de données a souvent lieu. Nous nous penchons sur la question de savoir à quoi il faut faire attention sous l'angle de la protection des données lors de l'échange de données avec des tiers.

Il convient tout d'abord de déterminer quelles sont les réglementations applicables: dans la prévoyance obligatoire (et enveloppante), il s'agit en premier lieu de respecter l'obligation de garder le secret ancrée à l'art. 86 LPP, avec les exceptions définies aux art. 85a, 85b et 86a et suivants LPP. Selon l'art. 86 LPP, les personnes qui participent à l'application ainsi qu'au contrôle ou à la surveillance de l'application de la LPP sont tenues de garder le secret vis-à-vis des tiers. Cette obligation s'applique également aux tiers mandatés. Dans la prévoyance professionnelle plus étendue, ce sont par contre les moyens de droit civil de la protection de la personnalité[1] et la protection du secret professionnel prévue par le droit de la protection des données qui s'appliquent.[2]

En matière de protection des données, les institutions de prévoyance qui appliquent le régime obligatoire (et donc aussi les institutions de prévoyance enveloppantes) et les institutions de libre passage sont considérées comme des organes fédéraux.[3] Une base légale est nécessaire pour un traitement de données par des organes fédéraux[4], qui existe notamment avec les art. 85a ss LPP et l'art. 25 LFLP. Les dispositions du droit de la protection des données sont applicables à titre complémentaire.

En revanche, les caisses de pensions offrant exclusivement des prestations surobligatoires ou extra-obligatoires, telles que les fondations 1e et les fondations patronales, sont considérées comme des personnes privées. Elles sont soumises aux dispositions du droit de la protection des données et peuvent traiter des données personnelles même sans base légale si la personnalité des personnes concernées n'est pas atteinte ou s'il existe des motifs justificatifs.

Cette distinction existe déjà dans la législation actuelle sur la protection des données. Ce qui est nouveau, c'est par exemple que les organes fédéraux – à la

[1] Art. 28 du Code civil.

[2] Art. 35 LPD; art. 62 nLPD.

[3] Selon l'art. 5 let. i, de la LPD révisée, un organe fédéral est une autorité ou un service de la Confédération ou une personne chargée de tâches publiques de la Confédération.

[4] Art. 34, 1er alinéa, de la loi révisée sur la protection des données.