AXA Stiftung
Berufliche Vorsorge

Berufliche Vorsorge

Datenschutz-Reglement

AXA Stiftung Berufliche Vorsorge, Winterthur

L1287.001-09.23

Dieses Datenschutz-Reglement wird vom Stiftungsrat der AXA Stiftung Berufliche Vorsorge, Winterthur, («Stiftung») gestützt auf Ziffer 2 der Stiftungsurkunde und Ziffer 10 des geltenden Organisationsreglements erlassen.

Zweck

1

Mitarbeitende, Kunden, Versicherte, Leistungsempfänger und andere Personen, deren Personendaten von der Stiftung bearbeitet werden, erwarten von ihr einen verantwortungsvollen und rechtskonformen Umgang mit ihren Personendaten.

Die Stiftung hält sich bei der Bearbeitung von Personendaten an das anwendbare Recht und an dieses Datenschutz-Reglement. Dieses Reglement stellt allgemeine Grundsätze für den Umgang mit Personendaten auf und ist verbindlich für alle Organe der Stiftung, sowie für in die Stiftung delegierte oder direkt von der Stiftung angestellte Mitarbeitende («**Mitarbeitende**»).

Rechtlicher Rahmen

2

Für den Umgang mit Personendaten sind die wichtigsten geltenden Gesetze:
- das Bundesgesetz über den Datenschutz (DSG) mit der dazugehörigen Verordnung,
- das Bundesgesetz über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVG) und die dazugehörigen Verordnungen, sowie
- das Bundesgesetz über die Freizügigkeit in der beruflichen Alters-, Hinterlassenen- und Invalidenvorsorge (FZG) und die dazugehörigen Verordnungen.

Schweigepflicht im Rahmen der beruflichen Vorsorge

3

Unter die Schweigepflicht fallen alle Wahrnehmungen über die persönlichen und finanziellen Verhältnisse der Versicherten und der Arbeitgeber. Bei der Datenbekanntgabe im Bereich der beruflichen Vorsorge werden die spezifischen Anforderungen von Art. 86a BVG beachtet.

Begriffe

4

Zentrale Bedeutung haben im Datenschutz die Begriffe Personendaten und Bearbeiten. Immer wenn **Personendaten bearbeitet** werden, sind die Vorgaben zum Datenschutz in diesem Reglement zu beachten.

Personendaten
Personendaten sind Informationen («Daten»), die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen («betroffene Person»). Sie setzten damit einen Personenbezug voraus, was teilweise erst aus dem konkreten Zusammenhang heraus klar wird. Keine Rolle spielt, ob Personendaten elektronisch gespeichert oder auf einem physischen Träger festgehalten sind.

Personendaten sind beispielsweise:
- Kontaktangaben wie Namen, Vornamen, Adresse, E-Mail-Adresse, Telefonnummer
- Angaben über Merkmale, Verhalten, Leistung, Befindlichkeit, Vorlieben, Eigenschaften, Meinungen, und über soziale, familiäre oder wirtschaftliche Interaktionen
- Identifikationsangaben wie IP-Adressen, Ausweisnummer, AHV-Nummer, Versichertennummer oder Fingerabdruck
- Bild- oder Tonmaterial mit Rückschlussmöglichkeit auf Personen.

Bearbeiten
Bearbeiten von Personendaten umschreibt als überaus weiter Begriff jeder beliebige Umgang mit solchen Personendaten (elektronisch oder physisch). Beispiele:
- Aufbewahren, Speichern und Archivieren
- Erheben/Beschaffen
- Zugriff
- Weitergabe/Übermittlung an Dritte (etwa bei Nutzung einer Cloud-Lösung oder Datenzugriff durch einen externen Service Provider)
- Auswertung/Analyse
- Veröffentlichung
- Löschen/Vernichten
- Anonymisieren/Pseudonymisieren.

Online werden besonders über Tracking-Tools, Social Media und Cookies Personendaten bearbeitet. Applikationen wie Bewerbungsplattformen, zum Beispiel für die Stiftungsratswahlen, werden in jedem Fall Personendaten enthalten. Aber auch mit der Aufbewahrung von Personaldossiers werden Personendaten bearbeitet.

Besonders schützenswerte Personendaten
Für Personendaten, die unter die (abschliessende) Kategorie der besonders schützenwerten Personen fallen, gelten für die Bearbeitung strengere Vorgaben (vgl. unten).

Besonders schützenswerte Personendaten beziehen sich auf:
- Gesundheit
- Religion
- Zugehörigkeit zu Ethnie/Rasse

– Politische/weltanschauliche Überzeugung
– Intimsphäre (sexuelle Orientierung/Sexualleben)
– Gewerkschaftliche Ansichten oder Tätigkeiten
– Genetische/biometrische Daten
– Massnahmen der sozialen Hilfe
– Strafverfolgung/Straftaten[1].

Profiling
Ist jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

Profiling mit hohem Risiko
Ist ein Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

Grundsätze
5

Fairness
Personendaten werden fair und nur so bearbeitet, wie es die betroffene Person erwarten darf.

Transparenz
Wenn Personendaten von der betroffenen Person selbst oder von anderen Quellen beschafft werden, wird die betroffene Person aktiv, rechtzeitig, detailliert und verständlich über die Bearbeitung ihrer Personendaten informiert.

Zweckbindung
Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist. (Beispiel: Die in einem Kontaktformular angegebene E-Mail-Adresse darf nicht zum Versand eines Newsletters verwendet werden).

Datenminimierung
Das Erheben von Personendaten ist auf das notwendige Mass zu beschränken. Zudem sollen Personendaten nach Möglichkeit anonymisiert oder pseudonymisiert werden. (Beispiel: Für die Beantwortung einer Brocker-Anfrage zwecks Offerten Einholung im Auftrag eines Arbeitgebers ist die Weitergabe von Vornamen und Nachnamen der Versicherten regelmässig nicht erforderlich).

Speicherbegrenzung
Personendaten dürfen nur so lange gespeichert werden, wie es für die mit der Bearbeitung verfolgten Zwecke erforderlich ist. (Beispiel: Ein Löschkonzept stellt sicher, dass Personendaten nach Ablauf einer gewissen Dauer gelöscht werden).

Richtigkeit
Personendaten sind sachlich richtig und auf dem neuesten Stand zu halten.

Sicherheit
Personendaten müssen vertraulich behandelt werden und durch angemessene technische und organisatorische Massnahmen vor unbefugter Vernichtung, Verlust, Veränderung oder unbefugte Offenbarung geschützt werden. (Beispiele: Protokollierung, Hardware-Verschlüsselung mobiler Geräte).

Rechtsgrundlage
Datenbearbeitungen setzen dann eine besondere Rechtsgrundlage voraus, wenn einer der oben erwähnten Grundsätze verletzt wird, Dritten besonders schützenswerte Personendaten bekanntgegeben werden oder Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden.

Als konkrete Rechtsgrundlagen kommen in Frage:
– rechtliche Vorschrift (Beispiel: gesetzliche Aufbewahrungsfristen für Buchhaltungsbelege)
– unmittelbarer Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags mit der von einer Datenbearbeitung betroffenen Person
– überwiegendes Interesse von uns an der Datenbearbeitung, wenn dabei ein so gewichtiges Interesse besteht, welches entgegenstehende Interessen der betroffenen Person übertrifft
– Einwilligung der betroffenen Person.

[1] Inkl. administrative Verfolgungen/Sanktionen.

Im Bereich der beruflichen Vorsorge dürfen Personendaten grundsätzlich nur bearbeitet werden, wenn dafür eine gesetzliche Grundlage besteht. Eine Ausnahme davon besteht in den Situationen, in welchen die betroffene Person im Einzelfall in die Bearbeitung eingewilligt oder ihre Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. Die Einwilligung muss ausdrücklich erfolgen für (i) jede Bearbeitung von besonders schützenswerten Personendaten; (ii) ein Profiling mit hohem Risiko ausserhalb der obligatorischen Vorsorge; und (iii) jedes Profiling im Bereich der obligatorischen Vorsorge.

Sobald fraglich ist, ob für eine Datenbearbeitung eine erforderliche Rechtsgrundlage oder eine genügende gesetzliche Grundlage besteht (bzw. ob es eine solche braucht), ist der Datenschutzberater der Stiftung beizuziehen.

Datenschutzerklärung

6

Betroffene Personen sind in verständlicher und leicht zugänglicher Form über die Bearbeitung ihrer Personendaten zu informieren, ausser beispielsweise die Bearbeitung ist gesetzlich vorgesehen.

Die Information an die betroffene Person muss mindestens die folgenden Angaben enthalten:
- Kontaktdaten der datenverantwortlichen Rechtseinheit
- Bearbeitungszweck
- Empfänger oder Kategorien von Empfängern
- Angabe der Staaten bei Auslandübermittlung
- Datenkategorien bei indirekter Datenerhebung (nicht bei betroffener Person)
- Modalitäten von wesentlichen, vollautomatisch getroffenen Entscheidungen.

Bearbeiten von Personendaten im Auftrag

7

Die Bearbeitung von Personendaten kann einem Dienstleister als Auftragsbearbeiter übertragen werden. Gegenüber der betroffenen Person bleibt die Stiftung für die Bearbeitung der Personendaten verantwortlich. Für den Beizug eines Auftragsbearbeiters müssen folgende Voraussetzungen erfüllt sein:
- Bei der Auswahl des Auftragsbearbeiters wurde darauf geachtet, dass dieser den Datenschutz und insbesondere die Datensicherheit gewährleisten kann.
- Die Übermittlung von Personendaten an den Auftragsbearbeiter verstösst nicht gegen gesetzliche oder vertragliche Geheimhaltungspflichten.
- Vor der Übermittlung von Personendaten an den Auftragsbearbeiter wird eine Auftragsbearbeitungsvereinbarung schriftlich oder in Textform geschlossen.
- Soll ein Auftragsbearbeiter mit Sitz im Ausland beauftragt werden, müssen zusätzlich die Voraussetzungen von Ziffer 8 erfüllt sein.

Auftragsbearbeiter müssen in der Auftragsbearbeitungsvereinbarung u.a. verpflichtet werden, Personendaten nur in Übereinstimmung mit ihrem Auftrag und den Instruktionen der Stiftung zu bearbeiten, sie zu keinen anderen Zwecken zu verwenden und die Sicherheit der Datenbearbeitung zu gewährleisten. Unterbeauftragte dürfen nur mit Zustimmung der Stiftung beigezogen werden.

Auslandübermittlung

8

Personendaten dürfen nur dann ins Ausland übermittelt werden, wenn im Empfängerstaat ein angemessenes Datenschutzniveau besteht oder besondere Schutzvorkehrungen wie vertragliche Garantien getroffen wurden.

Privacy by Design: Meldung neuer, wegfallender oder wesentlich veränderter Datenbearbeitungen

9

Um die Datenschutzkonformität eines Prozesses, einer Applikation, eines Projekts oder sonstigen Vorhabens sicherzustellen und die notwendigen Massnahmen anregen zu können, hat die Geschäftsführung der Stiftung den Datenschutzberater möglichst frühzeitig einzubeziehen, indem sie dazu die Checkliste Datenschutz-Folgenabschätzung ausfüllt.

Beispiele für neue oder wesentlich veränderte Datenbearbeitung können sein:
- Einsatz einer neuen Software/Anwendung oder bestimmter Funktionen davon
- Angepasste Marketingmassnahmen
- Veränderte oder neue Analyse/Auswertung/Verknüpfung bestehender Daten mit Personenbezug
- Verwendung bestehender Software/Anwendung zur Erhebung zusätzlicher Personendaten oder für weitere als bisherige Zwecke
- Anlegen neuer Datensammlungen
- Einräumung eines Fernzugriffs auf Personendaten.

Meldung von Vorfällen

10

Befürchtete und effektive Datenschutzverstösse sind schnellstmöglich und ohne jeden Verzug dem Datenschutzberater der Stiftung zu melden (Beispiele für Vorfälle: Verloren gegangenes und nicht hardwareverschlüsseltes Smartphone oder Notebook, E-Mail an falsche Empfänger). Der Datenschutzberater prüft die Benachrichtigung von Behörden, betroffenen Personen und weitere Massnahmen.

Datenschutzberater der Stiftung:
Swiss Infosec AG
Centralstrasse 8A
6210 Sursee
Tel.: +41 (0)41 984 12 12
E-Mail: datenschutzberater@infosec.ch

Weiterleitung von Begehren betroffener Personen

11

Begehren betroffener Personen etwa auf Auskunft, Berichtung, Widerspruch, Datenübertragbarkeit oder Überprüfung automatisierter Einzelentscheide mit Bezug auf ihre Personendaten sind umgehend dem Datenschutzberater der Stiftung weiterzuleiten, der unter anderem bereichsübergreifend die Datenzusammenstellung veranlasst und die Kommunikation mit den betroffenen Personen übernimmt.

Organisation

12

Organe und Mitarbeitende
Organe und Mitarbeitende sind in ihrem Verantwortungs- und Tätigkeitsbereich verantwortlich für die Befolgung der in diesem Reglement festgelegten Grundsätze für den Umgang mit Personendaten.

Dataowner
Dataowner tragen für die betreffende Datensammlung bzw. die betreffende Datenbearbeitung die Hauptverantwortung für die Einhaltung des Datenschutzrechts und dieses Reglements. Sie sorgen für die Dokumentation der betreffenden Datenbearbeitung und erforderlichenfalls die Durchführung einer Datenschutz-Folgenabschätzung.

IT
Die IT trifft in den Informationssystemen die erforderlichen technischen und organisatorischen Massnahmen zur Sicherung der Personendaten.

Datenschutzberater
Der Datenschutzberater der Stiftung hat die Aufgabe, unabhängig zu beraten und organisationsweit die Einhaltung des Datenschutzes zu koordinieren. Dazu ist er auf einen lückenlosen und raschen Informationsfluss durch sämtliche Organe und Mitarbeitenden angewiesen, weil für die Erfüllung gewisser datenschutzrechtlicher Pflichten zwingende Fristen zu beachten sind.

Der Datenschutzberater unterstützt die gesetzlich erforderliche Durchführung einer Datenschutz-Folgenabschätzung, berät betreffend die Führung des Verzeichnisses der Bearbeitungstätigkeiten, der Erstellung des Bearbeitungsreglements, koordiniert die Meldung von Vorfällen und die Erfüllung der Rechte betroffener Personen. Darüber hinaus prüft der Datenschutzberater, ob betroffene Personen bei der Datenbearbeitung im Sinne der Transparenz ausreichend informiert werden. Wo notwendig, formuliert und führt er Datenschutzhinweise nach.

Sanktionen

13

Verletzungen dieses Reglements können disziplinarische, zivilrechtliche oder strafrechtliche Massnahmen nach sich ziehen.

Schlussbestimmung

14

Dieses Reglement kann durch weitere Vorgaben oder Reglemente, die den Umgang mit Personendaten betreffen, ergänzt werden (z.B. IT-Benutzerweisung) und tritt per 1. September 2023 in Kraft.

L1287.001-09.23