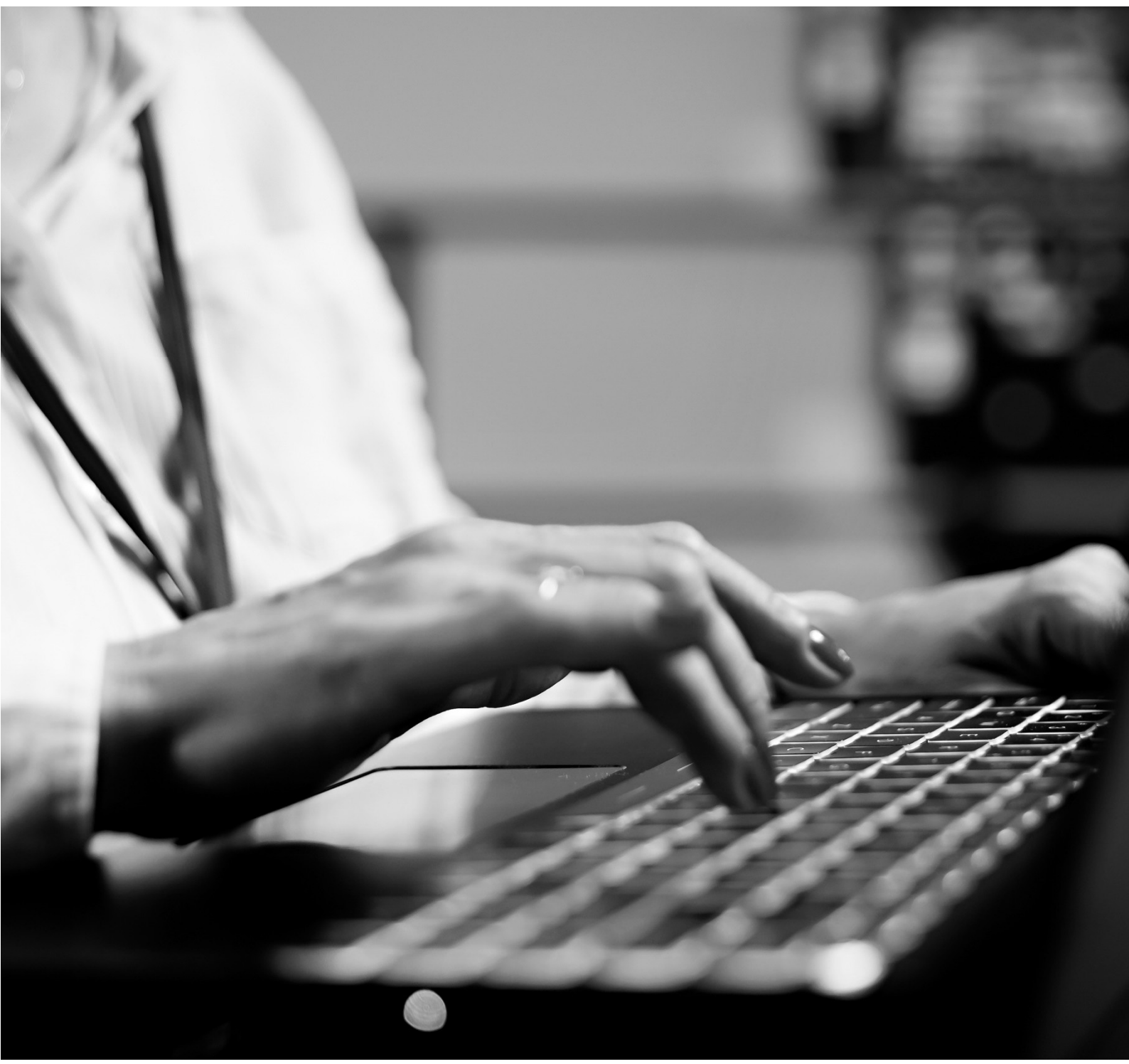


Datenschutz- Bearbeitungsreglement

Stand: 1. Juli 2026



INHALTSVERZEICHNIS

1	Einführung	3
1.1	Rechtsgrundlagen, Zweck und Geltungsbereich dieses Bearbeitungsreglements	3
1.2	Aktualität des Bearbeitungsreglements	3
2	Interne Organisation	3
2.1	Organigramm	3
2.2	Verantwortlichkeiten	4
3	Datenbearbeitungs- und Kontrollverfahren	5
3.1	Informatik-Infrastruktur der SVE	5
3.1.1	Übersicht der Kernanwendungen	5
3.1.2	Schnittstellenbeschreibung	6
3.2	Datenbearbeitung	6
3.2.1	Zweck der Datenbearbeitung	6
3.2.2	Datenherkunft	7
3.2.3	Datenkategorien	7
3.2.4	Berichtigung von Daten	7
3.2.5	Bekanntgabe von Daten	7
3.2.6	Speicherung, Aufbewahrung und Archivierung von Personendaten	8
3.2.7	Pseudonymisierung und Anonymisierung von Personendaten	8
3.2.8	Löschung und Vernichtung von Personendaten	8
3.3	Kontrollverfahren	8
3.3.1	Zugriffsberechtigungen	8
3.3.2	Zutrittsberechtigungen	8
4	Massnahmen zur Gewährleistung der Datensicherheit	8
4.1	Allgemeine Massnahmen	8
4.2	Spezielle Massnahmen	9
4.2.1	Vertraulichkeit	9
4.2.2	Verfügbarkeit	9
4.2.3	Integrität	10
4.2.4	Nachvollziehbarkeit	10
5	Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung	10
6	Inkrafttreten	10

1 Einführung

1.1 Rechtsgrundlagen, Zweck und Geltungsbereich dieses Bearbeitungsreglements

Dieses Bearbeitungsreglement gilt für alle Mitarbeitenden, die bei der Sulzer Vorsorgeeinrichtung angestellt sind. Es ist für alle Tätigkeiten im Zusammenhang mit Personendaten für die Sulzer Vorsorgeeinrichtung, die Johann Jakob Sulzer Stiftung, den Wohlfahrtsfonds Sulzer und die Sulzer-Stiftung anzuwenden.

Gestützt auf Art. 5 und 6 der Verordnung über den Datenschutz vom 31. August 2022 gilt dieses Reglement für alle automatisierten Bearbeitungen von Personendaten durch die Sulzer Vorsorgeeinrichtung, Zürcherstrasse 12, 8400 Winterthur («SVE») als Verantwortliche gemäss dem Bundesgesetz über den Datenschutz vom 25. September 2020. Das Bearbeitungsreglement enthält Angaben über die für den Datenschutz und die Datensicherheit verantwortlichen Organe, eine Beschreibung der Datenbearbeitungs- und Kontrollverfahren sowie eine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit.

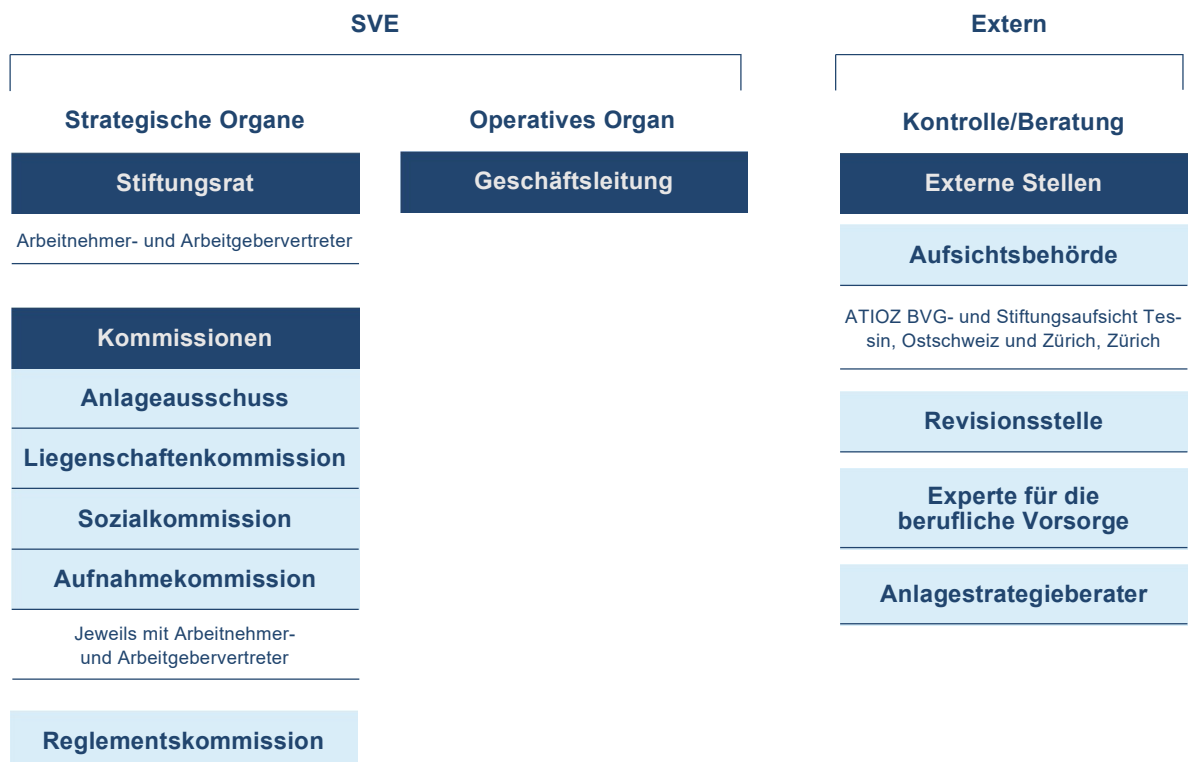
Unter einer automatisierten Bearbeitung ist eine Bearbeitung von Personendaten zu verstehen, die computergestützt erfolgt.

1.2 Aktualität des Bearbeitungsreglements

Das Bearbeitungsreglement wird von der Geschäftsleitung der SVE regelmässig aktualisiert und dem Datenschutzberater oder der Datenschutzberaterin der SVE zur Verfügung gestellt, um insbesondere Systemänderungen zu dokumentieren. In jedem Fall überprüft die Geschäftsleitung das Reglement jährlich auf dessen Aktualität und teilt dem Datenschutzberater oder der Datenschutzberaterin allfällige Änderungen mit oder bestätigt die Aktualität. Die jeweils aktuelle Version sowie eine Aufstellung der früheren Versionen sind in Ziffer 6 aufgeführt.

2 Interne Organisation

2.1 Organigramm



2.2 Verantwortlichkeiten

Der **Stiftungsrat** der SVE trägt die Gesamtverantwortung für die Einhaltung des Datenschutzes. Er stellt sicher, dass das Datenschutzgesetz eingehalten ist und dass die notwendigen Reglemente, Prozesse und Massnahmen in geeigneter Form umgesetzt werden, beispielsweise Datenschutzerklärung, Datenschutz-Bearbeitungsreglement, Wahl des Datenschutzberaters oder der Datenschutzberaterin.

Die **Geschäftsleitung** ist für die Umsetzung, Kommunikation, Kontrolle und Überwachung des Bearbeitungsreglements der SVE verantwortlich. Sie stellt sicher, dass die SVE über eine effiziente Organisation verfügt, welche die Einhaltung des Datenschutzes unterstützt.

Der **Datenschutzberater** oder die **Datenschutzberaterin** der SVE gibt die wichtigsten Verhaltensweisen bezüglich des Datenschutzes vor und sorgt für die Einhaltung der für die SVE anwendbaren datenschutzrechtlichen Vorschriften. Der Datenschutzberater oder die Datenschutzberaterin erstellt in Zusammenarbeit mit den massgebenden internen Stellen entsprechende Weisungen und Richtlinien für die Einhaltung der Gesetze und Standards.

Alle **Mitarbeitenden** der SVE sind in ihrem Zuständigkeitsbereich für die Einhaltung aller datenschutzrechtlichen Bestimmungen verantwortlich. Alle Mitarbeitenden der SVE haben bei der Anstellung oder bei Inkrafttreten das vorliegende Reglement sowie die Datenschutzrichtlinie zur Kenntnis genommen und dessen Umsetzung bestätigt. Die SVE sorgt dafür, dass die Mitarbeitenden laufend über die geltenden gesetzlichen und internen Bestimmungen informiert werden.

In dieser Tabelle sind die Rollen und die entsprechenden Verantwortlichkeiten aufgeführt:

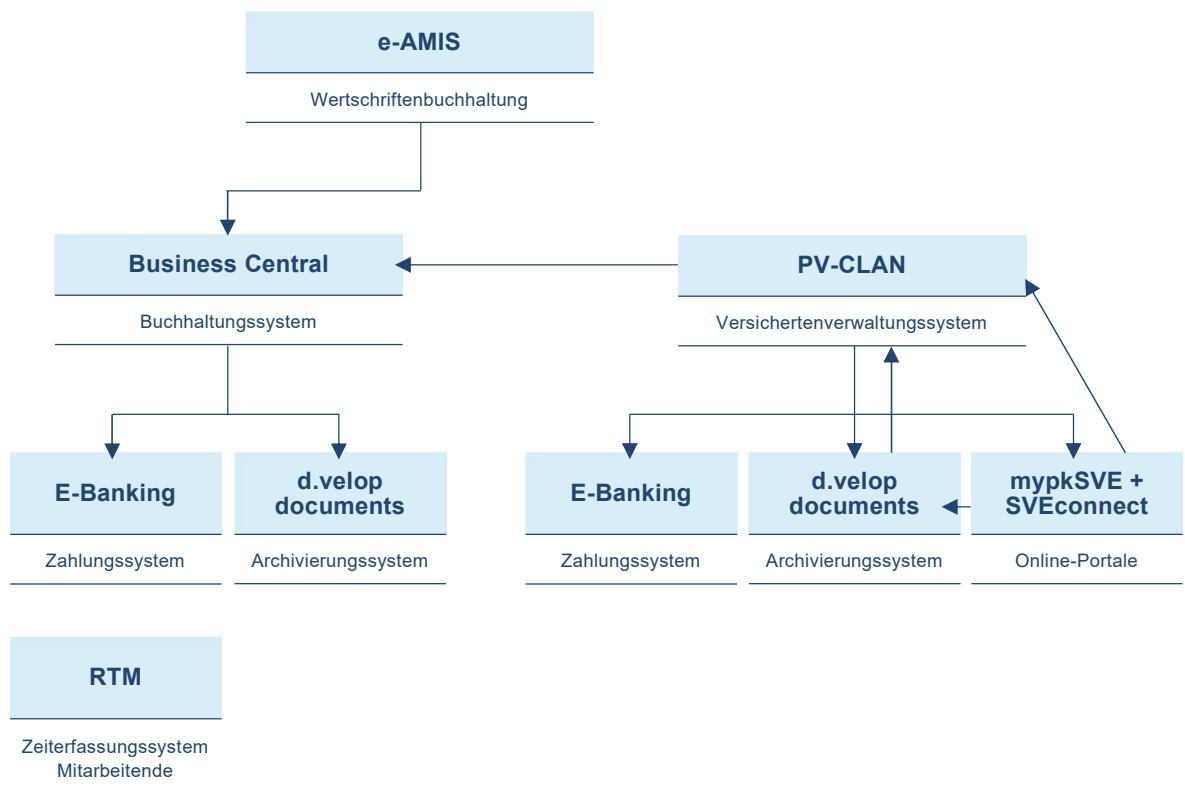
Rolle	Verantwortlichkeit
Gesamtverantwortung	Stiftungsrat
Erlass, Umsetzung, Kommunikation, Kontrolle und Überwachung des Datenschutzreglements	Geschäftsleitung
Ausführungsvorschriften zum Datenschutzreglement (Weisungen und Richtlinien), Schulungen	Datenschutzberater/-in
Technische Datensicherheit	Leitung IT/Digitalisierung
Zugangsprofil	Leitung IT/Digitalisierung

3 Datenbearbeitungs- und Kontrollverfahren

3.1 Informatik-Infrastruktur der SVE

3.1.1 Übersicht der Kernanwendungen

Die Durchführung der beruflichen Vorsorge erfolgt über die dargestellte Informatik-Infrastruktur:



System	Beschreibung
Adobe PDF	Standardprogramm zur Bearbeitung von PDF-Dateien
Business Central	Haupt-Buchhaltungssystem
d.velop documents	Revisionstaugliches Archivierungssystem
e-AMIS	Wertschriftenbuchhaltungs- und Reportingsystem
Microsoft Office	Word, Excel, Outlook, Power Point, One Note, Microsoft Teams
mypkSVE	Versichertenportal zur selbstständigen Abfrage der eigenen PK-Werte sowie Möglichkeit, persönliche Mutationen zu beantragen
PV-Clan	System für die Verwaltung der Versicherten, Rentnerinnen und Rentnern
RTM	Zeiterfassungssystem (enthält die Arbeitszeiten der Mitarbeitenden)
SVEconnect	Arbeitgeberportal für die Kommunikation und den Datenaustausch mit den Arbeitgebern

3.1.2 Schnittstellenbeschreibung

Aufzählung der wichtigsten Schnittstellen zwischen Systemen, welche schützenswerte Daten vorwiegend automatisiert übermitteln. Zwischen System A und System B bestehen meistens bidirektionale Datenflüsse.

System A	System B	Zweck	Daten
PV-Clan	d.velop documents	Die Unterlagen sind elektronisch in d.velop documents archiviert.	Personendaten: Informationen zu den Versicherten (aktiv Versicherte + Rentner/-innen)
PV-Clan	mypkSVE	Versichertenportal: Daten von PV-Clan werden in mypkSVE angezeigt.	Personendaten: jederzeitige, direkte Abfrage der PK-Details durch die Versicherten. Mutationen können direkt in mypkSVE beantragt werden
PV-Clan	SVEconnect	Arbeitgeberportal: Ein- und Austritts- sowie Mutationsmeldungen von Mitarbeitenden durch die Arbeitgeber, Übermittlung von Dokumenten und Informationen zwischen Arbeitgebern und SVE sowie Bereitstellung von Rechnungen, Reglementen etc.	Personendaten: Austausch von vertraulichen Unterlagen zwischen Arbeitgebern und SVE
d.velop documents	mypkSVE + SVEconnect	Die Unterlagen aus den beiden Online-Portalen sind elektronisch in d.velop documents archiviert und vordefinierte Dokumenttypen werden von d.velop documents an die Online-Portale übergeben.	Personendaten: Informationen zu den Versicherten (aktive Versicherte)
E-Banking	PV-Clan	Zahlungen werden aus Business Central und PV-Clan mittels elektronischer Zahlungsdatei im E-Banking in Auftrag gegeben.	Personendaten: Rentenzahlungen, Auszahlungen von Freizügigkeitsleistungen, Wohneigentums-, Scheidungsbezügen, Unterstützungsleistungen beim WOF und der SST, etc.
E-Banking	Business Central	Zahlungen werden aus Business Central und PV-Clan mittels elektronischer Zahlungsdatei im E-Banking in Auftrag gegeben.	Personendaten: Kreditorenzahlungen
Business Central	PV-Clan	Buchhalterische Daten werden monatlich in Business Central übernommen.	Personendaten: Ein- und Auszahlungen von oder an Versicherte, Rentenzahlungen, Bestandsänderung der versicherungstechnischen Buchhaltung
Business Central	e-AMIS	Buchhalterische Daten werden monatlich in Business Central übernommen.	Keine Personendaten: Daten der Wertschriftenverwaltung (Bestandsanpassung, Erfolgs-Verbuchung, Verrechnungssteuer etc.)

3.2 Datenbearbeitung

3.2.1 Zweck der Datenbearbeitung

Die SVE bearbeitet Personendaten in erster Linie zum Zweck der Durchführung der beruflichen Vorsorge im obligatorischen und überobligatorischen Bereich. Dazu gehören beispielsweise

- der Abschluss und die Abwicklung von Anschlussverträgen mit den Arbeitgebern, die Durchsetzung von Rechtsansprüchen aus Verträgen, die Buchführung und die Beendigung von Verträgen;
- die Aufnahme versicherter Personen. Dazu bearbeitet die SVE insbesondere Stammdaten. Die SVE führt für jede versicherte Person eines oder mehrere Vorsorgekapitalkonten, für welche Angaben zu Beiträgen, Einkäufen, Altersguthaben und Auszahlungen bearbeitet werden;
- die Prüfung und Abwicklung von Vorsorgefällen einschliesslich der Koordination mit anderen Versicherern wie beispielsweise der Invalidenversicherung und die Durchsetzung von Regressansprüchen. Dafür

bearbeitet die SVE vor allem Vertrags-, Fall- und Leistungsdaten der versicherten Personen und von Angehörigen und Begünstigten, auch Gesundheitsdaten und Daten von Dritten wie beispielsweise externen Sachverständigen und Leistungserbringern.

Daneben bearbeitet die SVE auch Personendaten für mit der Durchführung der beruflichen Vorsorge zusammenhängende Zwecke, beispielsweise zur Kommunikation, Vertragsabwicklung, Sicherheit und Prävention, Einhaltung rechtlicher Anforderungen, Rechtswahrung und im Rahmen der internen Abläufe und Administration.

Im Bereich des Obligatoriums beschränkt sich die Bearbeitung von Personendaten auf die in Art. 85a des Bundesgesetzes über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVG) genannten Zwecke.

Des Weiteren bearbeitet die SVE Personendaten für die Wahrung der überwiegenden Interessen sowie für die Weiterentwicklung von Angeboten, Dienstleistungen, Websites sowie IT-Lösungen.

3.2.2 Datenherkunft

Die SVE bearbeitet als Verantwortliche in erster Linie die Personendaten, die zur Durchführung der beruflichen Vorsorge benötigt werden, hauptsächlich von aktuellen oder ehemaligen Arbeitgebern, welche gesetzlich verpflichtet sind, der SVE alle für die Durchführung der beruflichen Vorsorge erforderlichen Daten zuzustellen. Zudem können Personendaten auch von anderen Dritten (beispielsweise Familienangehörige von versicherten Personen, Behörden oder Vorsorge- und Freizügigkeitseinrichtungen) oder aus öffentlich zugänglichen Quellen (beispielsweise Betreibungsregister, Grundbücher, Handels- und Vereinsregister, Presse, Internet) stammen.

3.2.3 Datenkategorien

Folgende Datenkategorien werden in den jeweiligen Anwendungen (Systeme) bearbeitet und sind durch angemessene technische und organisatorische Massnahmen (siehe Ziffer 4) vor unbefugter Einsicht geschützt:

- Stammdaten
- Identifikationsdaten
- Kontaktdaten
- Vertragsdaten
- Falldaten
- Leistungsdaten
- Finanzdaten
- Kommunikationsdaten
- Gesundheitsdaten
- Daten von Dritten (beispielsweise Angehörige, Arbeitgeber, externe Sachverständige, Leistungserbringer)

3.2.4 Berichtigung von Daten

Erfasste Personen können nach erfolgter Identifizierung verlangen, dass über sie erfasste Daten berichtigt oder vernichtet werden. Der Datenschutzberater oder die Datenschutzberaterin entscheidet über entsprechende Anträge.

3.2.5 Bekanntgabe von Daten

Die Daten können an folgende Kategorien von Empfängern weitergegeben werden:

- Arbeitgeber;
- Freizügigkeits- oder Vorsorgeeinrichtungen;
- Behörden, Ämter, Gerichte oder andere staatliche Institutionen;
- weitere Personen, beispielsweise an in Verfahren vor Gerichten oder Behörden beteiligte Personen, Zahlungsempfänger, Finanzinstitute und weitere an einem Rechtsgeschäft beteiligte Stellen;
- Auftragsbearbeiter, Dienstleister sowie sonstige Geschäftspartner;
- Dritte wie beispielsweise Anwälte oder Versicherer, die für die SVE Rechts- oder Versicherungsdienstleistungen erbringen;
- Revisionsstelle;
- Pensionskassenexperte (Datenaustausch für Statistiken, IAS19- oder US GAAP-Gutachten sowie für Erstellung der Pensionskassenrückstellungen, Abklärungen von Rechtsfällen etc.);
- andere Parteien in möglichen oder tatsächlichen Rechtsverfahren.

Im Bereich des Obligatoriums ist die Weitergabe von Personendaten auf den gesetzlichen Rahmen (Art. 86a BVG) beschränkt. In allen übrigen Fällen, in denen die SVE nicht von Gesetzes wegen legitimiert beziehungsweise verpflichtet ist (beispielsweise Anfragen von Arbeitgebern, ehemaligen Arbeitgebern, Pensionierten-

Vereinigungen etc.), Daten weiterzugeben, erfolgt die Datenbekanntgabe an Dritte nur mit schriftlicher Einwilligung der betroffenen Person.

3.2.6 Speicherung, Aufbewahrung und Archivierung von Personendaten

Die Speicherung und Aufbewahrung von Personendaten erfolgt für folgende Zwecke und Zeitdauer:

- solange es für den jeweiligen Zweck der Bearbeitung erforderlich ist, beispielsweise laufendes Vorsorgeverhältnis;
- zur Wahrung von Aufbewahrungspflichten, insbesondere Art. 27i ff. der Verordnung über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge (BVV 2);
- zur Wahrung von berechtigten Interessen der SVE an der Speicherung von Personendaten. Das kann insbesondere dann der Fall sein, wenn Personendaten für die Durchsetzung oder zur Abwehr von Ansprüchen benötigt werden sowie zu Archivierungszwecken und zur Gewährleistung der IT-Sicherheit.

Das Verfahren zur Aufbewahrung von Daten sowie zur Archivierung ist in der Datenschutzrichtlinie dokumentiert.

3.2.7 Pseudonymisierung und Anonymisierung von Personendaten

Statistische Daten werden gemäss den gesetzlichen Vorgaben bearbeitet. Daten werden beispielsweise anonymisiert, sobald der Bearbeitungszweck dies erlaubt. Ein Rückschluss auf bestimmte Personen ist nicht möglich.

3.2.8 Löschung und Vernichtung von Personendaten

Das Verfahren zur Löschung von Daten ist in der Datenschutzrichtlinie dokumentiert.

3.3 Kontrollverfahren

3.3.1 Zugriffsberechtigungen

Alle Mitarbeitenden der SVE haben nur Zugriff auf diejenigen Daten, die sie für ihre Aufgabenerfüllung benötigen. Welche Organisationseinheiten dies betrifft, ist in der Datenschutzrichtlinie ersichtlich.

Zum Schutz der Systeme sind generell Zugriffe nur durch Authentifizierung möglich, indem die Autorisierung der zugreifenden Person mittels Benutzername und Kennwort überprüft wird.

Im internen Zugriffsberechtigungskonzept, innerhalb der Datenschutzrichtlinie, wird detailliert festgehalten, welche Berechtigungsprofile (Rollen) welche Funktionen ausüben können und auf welche Datenfelder zugegriffen werden kann.

Die Zugriffsberechtigungen werden mittels angemessener Zugriffskontrollen überwacht (siehe Ziffer 4.2.1 a.).

3.3.2 Zutrittsberechtigungen

Zutritt zu Räumlichkeiten, in denen die Daten bearbeitet werden, haben Mitarbeitende, welche in einem Anstellungsverhältnis zur SVE oder unserem IT-Dienstleister stehen. Der Zutritt dieser Mitarbeitenden wird sowohl in räumlicher als auch in zeitlicher Hinsicht auf das notwendige Minimum beschränkt.

Die Zutrittsberechtigungen werden mittels angemessener Zutrittskontrollen überwacht (siehe Ziffer 4.2.1 b.).

4 Massnahmen zur Gewährleistung der Datensicherheit

4.1 Allgemeine Massnahmen

Zum Schutz der Personendaten gegen unbefugte oder zufällige Vernichtung, zufälligen Verlust, technische Fehler, Fälschungen, Diebstahl oder widerrechtliche Verwendung und unbefugte Bearbeitung bestehen folgende Massnahmen:

- Datensicherungen
- Protokollierung
- Zugriffsschutz
- gesicherte Netzwerke
- externe Kommunikation (E-Mail, Internet) besonders schützenswerter Personendaten nur mit ausreichender Verschlüsselung

Für die Nutzung von Hard- und Software, Internet und E-Mail ist zudem die Weisung zur IT-Nutzung massgebend.

4.2 Spezielle Massnahmen

4.2.1 Vertraulichkeit

- a) Zugriffskontrolle
 - Der Zugriff auf Daten der automatisierten Bearbeitung ist den Mitarbeitenden nur mittels IT-Anwendungen möglich. Die hierfür notwendigen Zugangsrechte und Berechtigungen sind von den Mitarbeitenden zu beantragen.
 - Die Mitarbeitenden besitzen nur Zugangsrechte für IT-Anwendungen, die sie zur Aufgabenerfüllung benötigen, und innerhalb der IT-Anwendungen nur für Funktionsbereiche, die ihren Aufgaben entsprechen.
 - Die Berechtigungsanträge sind durch die Leitung IT/Digitalisierung oder die system-verantwortliche Person zu genehmigen. Die Berechtigungen sind den Mitarbeitenden wieder zu entziehen, wenn sie für die übertragenen Aufgaben nicht mehr notwendig sind.
 - Die interne Organisation legt für alle Mitarbeitenden die Zugangsrechte fest. Dazu erarbeitet sie eine Zugangsrechtematrix. Je sensibler die Daten, die bearbeitet werden, desto höher sind die Anforderungen an die Authentifizierung des oder der Zugriffsberechtigten.
 - Alle Anträge werden zentralisiert aufbewahrt. Die erteilten Berechtigungen werden jährlich überprüft.
 - Der Fernzugriff auf die Datenverarbeitungssysteme ist nur speziell autorisierten Personen über verschlüsselte Zugänge mit Mehrfaktor-Authentifizierung möglich.
- b) Zutrittskontrolle
 - Der Zutritt zu den Büroräumlichkeiten der SVE ist mittels Schlüssel gesichert. Die Tür ist jederzeit von aussen abgeschlossen. Besucherinnen und Besucher haben sich jeweils beim Haupteingang telefonisch oder mittels Türklingel anzumelden.
 - Die Räume mit technischen Einrichtungen der Datenübertragung und Datenhaltung (Server, Router, Switchs usw.) werden von der Optimo Service AG, der IT-Dienstleisterin von SVE, betreut. Sie sind mit Schliess-Systemen oder Zutrittssystemen gesichert und nur einem eingeschränkten Personenkreis zugänglich. Die Gebäude und Räume mit Informatikeinrichtungen, welche Zugriff auf Personendaten ermöglichen, sind mit Zutrittssystemen gesichert.
 - Am Netzwerk der SVE dürfen nur Endgeräte angeschlossen werden, die von der SVE genehmigt worden sind.
- c) Benutzerkontrolle
 - Der Zugriff auf Datenverarbeitungssysteme ist grundsätzlich durch technische Massnahmen (Firewall usw.) unterbunden, sofern der Zugriff nicht für die Bearbeitung von Daten notwendig ist. Jeder einzelne Zugriff ist geschützt und muss für die einzelnen Mitarbeitenden genehmigt werden.
 - Das Informationssystem gewährt den Mitarbeitenden differenzierte Zugangsrechte. Der Zugriff der berechtigten Personen wird dabei auf diejenigen Daten beschränkt, welche die berechtigten Personen zur Erfüllung ihrer Aufgabe tatsächlich benötigen.

4.2.2 Verfügbarkeit

- a) Datenträgerkontrolle
 - Durch informationstechnische Vorkehrungen ist es ausschliesslich befugten Personen möglich, die Daten auf den elektronischen Datenträgern zu bearbeiten.
 - Nur dazu befugte Personen erhalten Zugriff auf das Informationssystem der SVE.
- b) Speicherkontrolle
 - Unbefugten Eingaben, Veränderungen oder Löschungen in den Speichern wird mittels angemessener Zugangs- und Berechtigungskontrollen (beispielsweise Benutzername oder Kennwort) sowie durch die Konfiguration der IT-Anwendungen vorgebeugt.
 - Beim Auswechseln von Datenspeichern oder beim Ersatz von PCs, Laptops oder Servern wird dafür gesorgt, dass insbesondere unverschlüsselte Daten sowie der freie Speicherplatz vollständig physisch gelöscht werden. Das regelmässige Update von Betriebssystemen und Anwendungen minimiert Angriffe, beispielsweise durch Malware.
- c) Transportkontrolle
 - Personendaten werden grundsätzlich elektronisch oder in Papierform übermittelt. Für eine gesicherte Datenübermittlung werden angemessene technische Massnahmen getroffen, damit keine unbefugten Personen lesen, kopieren, ändern oder löschen können.

- Beim elektronischen Datentransport sind der Datenschutz und insbesondere die entsprechende Datensicherheit dank einer starken Authentifizierungsmethode sowie modernster Datenübermittlungs- und Verschlüsselungstechnologien gewährleistet.
 - Der physische Datentransport wird mittels eines gesicherten Transportsystems durchgeführt, die Daten werden für den Transport mit einem anerkannten Verfahren verschlüsselt, und der Schlüssel wird separat transportiert.
- d) Wiederherstellung
- Die Datenbanken werden jede Nacht automatisiert in ein separates Verzeichnis kopiert und davon ein Backup erstellt.
 - Die Wiederbeschaffung der Daten ist dank des Backup Systems innert zwei Tagen möglich.

4.2.3 Integrität

- a) Datenintegrität
Optimo Service AG stellt sicher, dass die Daten jederzeit vollständig und korrekt sind. Allfällige Fehlfunktionen werden der Optimo Service AG gemeldet und innert nützlicher Frist behoben.
- b) Systemsicherheit
Weiter gewährleistet die Optimo Service AG, dass die IT-Sicherheit auf dem neuesten Stand ist und dass jederzeit eine Firewall im Einsatz ist, die den höchsten Sicherheitsanforderungen entspricht.

4.2.4 Nachvollziehbarkeit

- a) Eingabekontrolle
- Alle Eingaben und Mutationen von Personendaten in den unter Punkt 3.1.1 genannten IT-Systemen werden protokolliert.
 - Die Protokollierung beinhaltet die Identität der Person, die die Bearbeitung vorgenommen hat, die Art und das Datum der Bearbeitung sowie gegebenenfalls die Identität der Empfängerin oder des Empfängers der Daten.
- b) Bekanntgabekontrolle
- Datenempfängerinnen und Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, werden identifiziert und es müssen, soweit erforderlich, die gesetzlichen Anforderungen für eine Bekanntgabe (gesetzliche Grundlage, Einverständniserklärung) erfüllt sein.
 - Datenübertragungen werden protokolliert und die Identität der Daten wird vor deren Übertragung geprüft.
- c) Beseitigung
- Die Massnahmen zur Gewährleistung, dass Verletzungen der Datensicherheit rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können, sind in der Datenschutzrichtlinie ausgeführt.

5 Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung

Für die Gewährung der Einsichtsrechte von Versicherten in ihre eigenen Daten ist der Datenschutzberater oder die Datenschutzberaterin zuständig. Er oder sie beschafft sich die Daten, erteilt die Auskunft und sorgt allenfalls für die Datenberichtigung. Das Verfahren zur Ausübung des Rechts auf Auskunft und Datenherausgabe oder -übertragung ist in der Datenschutzrichtlinie dokumentiert.

6 Inkrafttreten

Das vorliegende Datenschutz-Bearbeitungsreglement tritt am 1. Juli 2026 in Kraft und ersetzt das Datenschutz-Bearbeitungsreglement vom 1. September 2023. Es kann jederzeit durch Beschluss des Stiftungsrats und unter Beachtung der gesetzlichen und statutarischen Bestimmungen geändert werden.