Pensionskasse der Rhätischen Bahn
Cassa pensione della Ferrovia retica
Cassa da pensiun da la Viafier retica

Bearbeitungsreglement für automatisierte Bearbeitungen

1. September 2023

Version 1.0/

Inhaltsverzeichnis

1. Einführung

1.1. Rechtsgrundlagen, Zweck und Geltungsbereich dieses Bearbeitungsreglements

Dieses Bearbeitungsreglement gestützt auf Art. 5 und 6 der Verordnung über den Datenschutz vom 31. August 2022 («**DSV**») gilt für alle automatisierten Bearbeitungen von Personendaten durch die Pensionskasse der Rhätischen Bahn, Bahnhofstrasse 25, 7001 Chur («**PK RhB**») als Verantwortliche gemäss dem Bundesgesetz über den Datenschutz vom 25. September 2020 («**DSG**»). 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.

1.2. Aktualität des Bearbeitungsreglements

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

1.3. Definitionen und Abkürzungen

Die folgenden Abkürzungen werden im Dokument verwendet:

Abkürzung	**Beschreibung**
DSB	Datenschutzberater der Pensionskasse der Rhätischen Bahn
DSG	Bundesgesetz vom 25. September 2020 über den Datenschutz
DSV	Verordnung zum Bundesgesetz über den Datenschutz vom 31. August 2022
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

2. Interne Organisation

2.1. Organigramm

Es gilt das jeweils aktuelle Organigramm der PK RhB, welches auf der Internetseite der PK RhB publiziert ist: Pensionskasse der Rhätischen Bahn - Rhätische Bahn RhB (pkrhb.ch)

2.2. Verantwortlichkeiten

Der **Stiftungsrat** der PK RhB trägt die Gesamtverantwortung für die Einhaltung des Datenschutzes. Er delegiert die Umsetzung einer geeigneten Organisation der Geschäftsleitung.

Die **Geschäftsleitung** ist für den Erlass sowie die Umsetzung, Kommunikation, Kontrolle und Überwachung des Datenschutzreglements der PK RhB verantwortlich. Sie stellt sicher, dass die PK RhB über eine effiziente Organisation verfügt, welche die Einhaltung des Datenschutzes unterstützt. Der von der PK RhB beauftragte DSB ist für die Umsetzung der Datenschutzvorgaben besorgt.

Der **DSB** gibt die wichtigsten Verhaltensweisen bezüglich des Datenschutzes vor und sorgt für die Einhaltung der für die PK RhB anwendbaren datenschutzrechtlichen Vorschriften. Der DSB erstellt im Auftrag der Geschäftsleitung und in Zusammenarbeit mit den massgebenden internen Stellen entsprechende Weisungen und Richtlinien für die Einhaltung der Gesetze und Standards.

Die im Auftrag der PK RhB handelnde Person sind in ihrem Zuständigkeitsbereich für die Einhaltung aller datenschutzrechtlichen Bestimmungen verantwortlich. Jede im Auftrag der PK RhB handelnde Person hat bei der Anstellung eine Datenschutzverpflichtung zu unterzeichnen. Die Geschäftsstelle sorgt dafür, dass die betroffenen Personen 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	DSB
Technische Datensicherheit	IT-Abteilung der Rhätischen Bahn («RhB»)
Zugangsprofil	Human Resources und IT-Abteilung

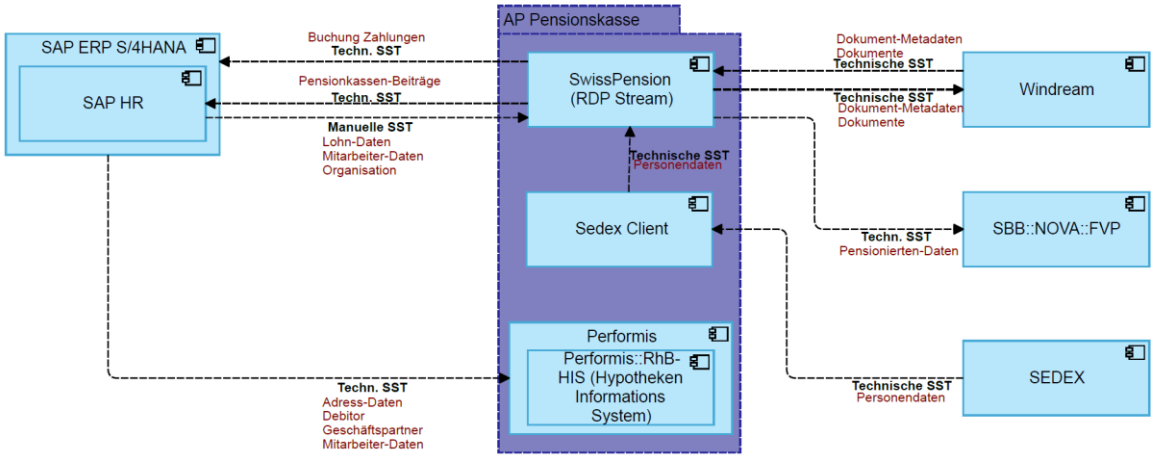
3. Datenbearbeitungs- und Kontrollverfahren

3.1. Informatik-Infrastruktur der PK RhB

Die PK RhB nutzt die IT-Landschaft der RhB.

3.1.1. Übersicht der Kernanwendungen

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



System	**Beschreibung**
Swisspension (SP6)	Pensionskassenprogramm
SharePoint	Langzeit-Archivierung von Dokumenten
SAP	ERP von RhB

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
SAP	Swisspension	Onboarding	Onboarding Personendaten
SP6	SAP	Beiträge	Beiträge
SP6	Windream	Archivdaten	Leistungsausweis, IV-Akten, Verträge
SP6	Aconso	E-Dossier	Leistungsausweis/Korrespondenz

3.2. Datenbearbeitung

3.2.1. Zweck der Datenbearbeitung

Die PK RhB bearbeitet Personendaten in erster Linie zum Zweck der Durchführung der beruflichen Vorsorge im obligatorischen und überobligatorischen Bereich. Dazu gehören z. B.

- der Abschluss und die Abwicklung von **Anschlussverträgen** mit dem Arbeitgeber, der Durchsetzung von Rechtsansprüchen aus Verträgen, der Buchführung und der Beendigung von Verträgen;
- die **Aufnahme versicherter Personen**. Dazu bearbeitet die PK RhB insbesondere Stammdaten. Die PK RhB führt sodann für jede versicherte Person eines oder mehrere Vorsorgekapitalkonten, für die die PK RhB Angaben zu Beiträgen, Einkäufen, Altersguthaben und Auszahlungen bearbeitet;
- die Prüfung und Abwicklung von **Vorsorgefällen** einschliesslich der Koordination mit anderen Versicherern wie z. B. der Invalidenversicherung und die Durchsetzung von Regressansprüchen. Dafür bearbeitet die PK RhB vor allem Vertrags-, Fall- und Leistungsdaten der versicherten Person und von Angehörigen und Begünstigten, auch Gesundheitsdaten und Daten von Dritten wie z. B. externen Sachverständigen und Leistungserbringern.

Daneben bearbeitet die PK RhB Personendaten auch für mit der Durchführung der beruflichen Vorsorge zusammenhängende Zwecke, z. B. 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.

3.2.2. Datenherkunft

Die PK RhB bearbeitet als Verantwortliche in erster Linie die Personendaten, die zur Durchführung der beruflichen Vorsorge benötigt werden, hauptsächlich von der betroffenen Person oder von aktuellen oder ehemaligen Arbeitgebern, welche gesetzlich verpflichtet sind, der PK RhB alle für die Durchführung der beruflichen Vorsorge erforderlichen Daten zuzustellen. Zudem können Personendaten auch von anderen Dritten stammen, z. B. Familienangehörige von versicherten Personen, Behörden oder Vorsorge- und Freizügigkeitseinrichtungen.

3.2.3. Datenkategorien

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

- Stammdaten;
- Kontaktdaten;
- Vertragsdaten;
- Falldaten;
- Leistungsdaten;
- Finanzdaten;
- Kommunikationsdaten;
- Gesundheitsdaten;
- Daten von Dritten (z. B. 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 DSB entscheidet über entsprechende Anträge.

3.2.5. Bekanntgabe von Daten

Die Daten können an folgende Kategorien von Empfängern weitergegeben werden:

- Arbeitgeber;
- Bekanntgaben bei Vorsorgefällen (z. B. Freizügigkeitseinrichtungen, andere Vorsorgeeinrichtungen);
- Behörden und Ämter;
- weitere Personen (z. B. an Verfahren vor Gerichten oder Behörden beteiligte Personen, Zahlungsempfänger, Finanzinstitute und weitere an einem Rechtsgeschäft beteiligte Stellen);
- Auftragsbearbeiter (Dienstleister).

Im Bereich des Obligatoriums ist die Weitergabe von Personendaten auf den gesetzlichen Rahmen (Art. 86a BVG) beschränkt.

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 (z. B. laufendes Vorsorgeverhältnis);
- zur Wahrung der Aufbewahrungspflicht (insb. Art. 27i ff. der Verordnung über die berufliche Alters-, Hinterlassenen- und Invalidenvorsorge, BVV 2);
- zur Wahrung von berechtigten Interessen der PK RhB 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.

Aktuell besteht kein Löschkonzept bei der PK RhB. Ein solches existiert auch nicht bei der RhB.

3.2.7. Pseudonymisierung und Anonymisierung von Personendaten

Auswertungen und Tests erfolgen aufgrund generischer, nicht personenbezogener Daten. Statistische Daten werden gemäss den gesetzlichen Vorgaben anonymisiert. Ein Rückschluss auf bestimmte Personen ist nicht möglich.

3.2.8. Löschung und Vernichtung von Personendaten

Das Verfahren zur Löschung von Daten ist einem detaillierten Aufbewahrungs-/Löschkonzept dokumentiert.

3.3. Kontrollverfahren

3.3.1. Zugriffsberechtigungen

Die im Auftrag der PK RhB handelnde Person gemäss Organisationsreglement der PK RhB hat nur Zugriff auf diejenigen Daten, die er für seine Aufgabenerfüllung benötigt. Welche Organisationseinheiten dies betrifft, ist im Bearbeitungsverzeichnis ersichtlich.

Zum Schutz der Systeme sind generell Zugriffe nur möglich, indem die Autorisierung der zugreifenden Person mittels Benutzername/Kennwort überprüft wird (Authentifizierung). IT-Anwendungen mit Zugriff auf besonders schützenswerte Daten sind mit einer zeitlichen Beschränkung ausgerüstet, d.h. wenn eine IT-Anwendung eine gewisse Zeit lang nicht benutzt wird, so ist eine erneute Eingabe des Kennworts nötig.

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

Die Zugriffsberechtigungen werden mittels angemessener Zugriffskontrollen überwacht (Ziff. 1.1.1.a).

3.3.2. Zutrittsberechtigungen

Zutritt zu Räumlichkeiten, in denen die Daten bearbeitet werden, haben Mitarbeitende, welche in einem Anstellungsverhältnis zur PK RhB stehen. Dritte haben nur Zutritt, sofern sie eine Datenschutz- und Geheimhaltungserklärung unterzeichnet haben. Dieser Zutritt von Mitarbeitenden oder Dritten wird sowohl in räumlicher als auch in zeitlicher Hinsicht auf das notwendige Minimum beschränkt.

Die Zutrittsberechtigungen werden mittels angemessener Zutrittskontrollen überwacht (Ziff. 1.1.1.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 ausdrücklichem Wunsch des Versicherten.

Für die Nutzung von Hard- und Software, Internet und E-Mail sind zudem die Weisungen «DV 0005 Einsatz und Nutzung der Festnetz-, Mobiltelefon- und mobiler Datendienste prüfen» und DV

0002«Einsatz und Nutzung von Informatik-systemen (IT-Nutzungsreglement)» 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 Berechtigungen (Zugangsrechte) 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 jeweiligen Vorgesetzten und des Applikationsverantwortlichen 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 jeden 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;
- über die erteilten Berechtigungen wird eine Liste geführt;
- der Fernzugriff auf die Datenbearbeitungssysteme ist nur autorisierten Personen über verschlüsselte Zugänge mit Mehrfaktor-Authentisierung möglich.

b) Zugangskontrolle

- der Zutritt zu Gebäuden der PK RhB ist mit einem Badgesystem gesichert. Besucher haben sich jeweils beim Empfang anzumelden, bevor sie das Gebäude betreten können;
- die Räume mit technischen Einrichtungen der Datenübertragung und Datenhaltung wie z. B. Server, Router, Switchs usw. sind mit Schliesssystemen oder Zutrittssystemen gesichert und nur einem eingeschränkten Personenkreis zugänglich. Die Räume/Gebäude mit Informatikeinrichtungen, welche Zugriff auf Personendaten ermöglichen, sind mit Zutrittssystemen gesichert.

c) Benutzerkontrolle

- der Zugriff auf Datenbearbeitungssysteme ist grundsätzlich durch technische Massnahmen unterbunden, sofern der Zugriff nicht für die Bearbeitung von Daten notwendig ist. Jeder einzelne Zugriff ist geschützt und muss für den 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 PK RhB.

b) Speicherkontrolle

- unbefugten Eingaben, Veränderungen oder Löschungen in den Speichern wird mittels angemessener Zugangs- und Berechtigungskontrollen (z. B. Benutzername/Kennwort) sowie durch die Konfiguration der IT-Anwendungen vorgebeugt;

- beim Auswechseln von Datenspeichern (Festplatten) oder beim Ersatz von Computern (PC, Laptop und Server) wird dafür gesorgt, dass insbesondere unverschlüsselte Daten sowie der freie Speicherplatz vollständig physisch gelöscht werden. Das regelmässige Update von Betriebssystemen und Anwendungen minimiert Angriffe (z. B. 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 ist der Datenschutz und insbesondere die entsprechende Datensicherheit dank einer starken Authentifizierungsmethode sowie modernsten 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

Um die Datenintegrität zu gewährleisten, besteht ein Überwachungsprogramm, um das Fehlverhalten festzustellen und entsprechend reagieren zu können. Sämtliche Daten sind auf zwei Rechenzentren gespeichert.

b) Systemsicherheit

Um die Systemsicherheit zu gewährleisten, werden die Server regelmässig mit einem Update aufgefrischt. Zudem wird das Applikationssystem regelmässig vom Hersteller auf den neusten Stand gebracht.

4.2.4. Nachvollziehbarkeit

a) Eingabekontrolle

- alle Eingaben und Mutationen von Personendaten im automatisierten Datenbearbeitungssystem werden protokolliert;
- die Protokollierung beinhaltet die Identität der Person, die die Bearbeitung vorgenommen hat, die Art, das Datum und die Uhrzeit der Bearbeitung sowie gegebenenfalls die Identität des Empfängers der Daten.

b) Bekanntgabekontrolle

- Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, werden identifiziert und soweit erforderlich müssen die gesetzlichen Anforderungen für eine Bekanntgabe (gesetzliche Grundlage) erfüllt sein.

c) Beseitigung

Die Massnahmen zur Gewährleistung, dass Verletzungen der Datensicherheit rasch erkannt (Erkennung) und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können, sind in einer internen Richtlinie (DV0002) weiter 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 DSB zuständig. Dieser beschafft sich die Daten, erteilt die Auskunft und sorgt allenfalls für die Datenberichtigung. Das Verfahren betreffend die Ausübung des Rechts auf Auskunft und Datenherausgabe oder -übertragung ist im Übrigen in einer internen Richtlinie dokumentiert.

6. Reglementsänderungen

Aktuelle gültige Version 1.0 vom 1. September 2023

Die jeweils aktuelle Version sowie eine Aufstellung der früheren Versionen sind hier aufgeführt:

Version Nr. 1	1. September 2023