

Datenschutz
und
Bearbeitungsreglement
vom
1. September 2023

1 EINLEITUNG

1.1 Präambel

Um den Schutz von personenbezogenen Daten zu gewährleisten, trifft die Pensionskasse Hirslanden Vorkehrungen für die Datensicherheit. Die Hirslanden Pensionskasse verpflichtet sich zur Achtung der Persönlichkeitsrechte und der Privatsphäre von Personen und behandelt sämtliche personenbezogene Daten, insbesondere Daten über gesundheitliche Verhältnisse, mit besonderer Sorgfalt.

2 INHALT DIESER WEISUNG/ANORDNUNG

Diese Weisung/Anordnung regelt die datenschutzkonforme Verarbeitung von Personendaten. Damit will die Pensionskasse Hirslanden ein angemessenes Datenschutzniveau für die Datenverarbeitung durch ihre Mitarbeitenden und Beauftragten gewährleisten.

3 DATENSCHUTZ UND -MINIMIERUNG DURCH TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Die Pensionskasse Hirslanden bekennt sich zum übergeordneten Prinzip des Datenschutzes durch Technikgestaltung («Privacy by design») und durch datenschutzfreundliche Voreinstellungen («Privacy by default»), welches von der Hirslanden Gruppe umgesetzt wird. Dieses Prinzip beinhaltet alle technischen und organisatorischen Massnahmen, die den von der Datenverarbeitung Betroffenen einen angemessenen Schutz gewährleisten. Solche Massnahmen umfassen beispielsweise die Einschränkung von Zugriffen, Datenminimierung, Anonymisierung, Verschlüsselung, angemessene Aufbewahrungsfristen, Löschung etc.

4 GELTUNGSBEREICH

Diese Weisung/Anordnung gilt für die Bearbeitung sämtlicher Personendaten innerhalb der Pensionskasse Hirslanden. Sie richtet sich an folgende Adressaten (nachfolgend «Bearbeitende» genannt):

- a. Mitarbeitende der Pensionskasse Hirslanden und deren Hilfspersonen;
- b. Personen, die aufgrund eines anderen Rechtsverhältnisses mit der Pensionskasse Hirslanden Zugriff auf Personendaten haben (z. B. Dienstleister).

5 ANWENDBARES RECHT

Diese Weisung/Anordnung berücksichtigt die Datenschutzerfordernisse der revDSG und der dazugehörigen Verordnung.

6 DEFINITIONEN

Für das korrekte Verständnis sind folgende Definitionen wichtig:

a. Personendaten:

Mit Personendaten sind alle Angaben gemeint, die sich auf eine bestimmte oder bestimmbare Person (z. B. versicherte Personen) beziehen.

b. Besonders schützenswerte Personendaten:

Als solche gelten personenbezogene Daten, die Auskunft über Privatangelegenheiten der betroffenen Person geben. Dazu zählen insbesondere:

Gesundheitliche, religiöse, weltanschauliche, politische, gewerkschaftliche Daten, Daten zu strafrechtlichen oder administrativen Verfolgungen oder Sanktionen, Sozialhilfeangaben sowie biometrische und genetische Daten.

c. Verarbeitung:

Dieser Begriff umfasst jeden Umgang mit Personendaten. Dazu gehören u. a. das Beschaffen, Verändern, Verwenden, Anzeigen, Bekanntgeben, Speichern und Löschen der Daten. Dabei spielt es keine Rolle, ob die Daten analog oder elektronisch, manuell oder durch automatisierte Programme bearbeitet werden. Für die Bearbeitung der Daten mit der ICT-Infrastruktur sind zusätzlich das «Reglement über ICT-Infrastruktur und Datenschutz» und der «Kodex für Unternehmensführung und Geschäftsethik» der Hirslanden Gruppe zu beachten.

7 VERANTWORTLICHKEITEN VON PERSONEN UND FUNKTIONEN

Alle Personen und Funktionen, die Personendaten verarbeiten, sind dafür verantwortlich, dass die Datenschutzerfordernungen in dieser Weisung/Anordnung und in den anderen Regelungen, auf die verwiesen wird, eingehalten und umgesetzt werden.

a. Personen: Dies sind insbesondere:

- **Bearbeitende**: Alle Personen gemäss Ziffer 4, die Zugriffe auf Personendaten haben, sind dafür verantwortlich, dass die Datenschutzerfordernungen eingehalten werden. Sie sind verpflichtet, die obligatorischen Schulungen zu absolvieren.

b. Funktionen: Folgende Funktionen haben besondere Rollen und Verantwortlichkeiten im Zusammenhang mit dem Datenschutz:

- **Legal der Hirslanden Gruppe** bietet im Rahmen des Datenschutzes rechtliche Unterstützung oder unterstützt bei der Verfahrenssteuerung.
- **ICT & Prozesse der Hirslanden Gruppe** stellt sicher, dass die datenschutzrelevanten Vorgaben sowohl bei der Systemplanung als auch bei der Systemimplementierung und dem Systemmanagement berücksichtigt werden. Sie ist zudem für die detaillierte Definition und die Umsetzung der technischen Sicherheitsanforderungen und Massnahmen zuständig. Unterstützt wird sie durch den ICT-Sicherheitsbeauftragten.

c. Datenschutzorganisation:

- **Datenschutzbeauftragter:**
Der Hirslanden-Datenschutzbeauftragte übernimmt die Verantwortung für das Management des Datenschutzes innerhalb der Pensionskasse Hirslanden. Der/die Datenschutzbeauftragte unterstützt bei rechtlichen Fragen beim Vertragsmanagement im Zusammenhang mit der Beauftragung der Datenbearbeitung sowie bei Verträgen mit anderen Verantwortlichen, insbesondere bei datenschutzrelevanten Vertragsklauseln. Diese Person ist zwingend bei Datenschutzverletzungen beizuziehen. Sie ist Ansprechperson für Aufsichtsbehörden.

8 DATENVERARBEITUNG

8.1 Verarbeitungsgrundsätze

Die Verarbeitung von Personendaten bei der Pensionskasse Hirslanden erfolgt im Rahmen der übergeordneten Prinzipien der Rechtmässigkeit, Zweckbindung, Verarbeitung nach Treu und Glauben und Transparenz.

- **Rechtmässigkeit:** Eine Verarbeitung von Personendaten ist dann rechtmässig, wenn eine Rechtsgrundlage für die Datenverarbeitung vorliegt.
- **Zweckbindung:** Jede Verarbeitung von Personendaten muss für einen definierten Zweck erfolgen. Datenspeicherung «auf Vorrat» oder Datenverarbeitung ohne erklärten Zweck ist nicht zulässig.
- **Datenminimierung und Speicherbegrenzung:** Die Datenbearbeitung muss auf das notwendige Mass beschränkt werden. D. h., auf die Daten darf nicht unnötig zugegriffen werden und sie dürfen nicht unnötig dupliziert werden.
- **Integrität und Vertraulichkeit:** Personendaten müssen auf eine Art und Weise bearbeitet werden, die eine angemessene Sicherheit gewährleistet. Dazu gehört auch der Schutz vor unbefugter und/oder unrechtmässiger Bearbeitung (z. B. Verfälschung, unautorisiertes Löschen) und unbeabsichtigtem Verlust. Alle Bearbeitenden sind zudem verpflichtet, sämtliche Daten, in die sie im Rahmen ihrer Funktion für die Pensionskasse Hirslanden Einsicht erlangen, streng vertraulich zu behandeln. Gegenüber Aussenstehenden ist Stillschweigen zu bewahren.
- **Verarbeitung nach Treu und Glauben:**
Loyales und vertrauenswürdiges Verhalten.
- **Transparenz:** Eine Verarbeitung von Personendaten sowie deren Zweck muss für die betroffene Person erkennbar sein oder die Person muss vorgängig über die Datenbearbeitung aufgeklärt werden (z.B. mittels einer Datenschutzerklärung).

8.2 Verzeichnis der Verarbeitungstätigkeiten

Die Pensionskasse Hirslanden führt zentral ein sogenanntes «Verzeichnis der Verarbeitungstätigkeiten». Für die Einträge und die Pflege des Verzeichnisses ist die Leitung der Pensionskasse in Zusammenarbeit mit der Datenschutzbeauftragten der Hirslanden-Gruppe verantwortlich.

8.3 Rechtsgrundlagen für die Datenverarbeitung

Personendaten dürfen nur bearbeitet werden, wenn einer der folgenden Rechtfertigungsgründe vorliegt:

- Die Verarbeitung dient der Erfüllung bundesrechtlicher Aufgaben gemäss BVG.
- Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich.
- Die Verarbeitung erfolgt im öffentlichen Interesse (z. B. zur Aufdeckung eines Verbrechens).

8.4 Auftragsverarbeitung

Eine Verarbeitung von Personendaten kann auch durch beauftragte Unternehmen erfolgen, die hinreichende technische und organisatorische Massnahmen für eine rechtmässige Verarbeitung von Personendaten garantieren können. In diesem Fall ist ein ADV Vertrag zu erstellen.

8.5 Sicherheit

Die Pensionskasse Hirslanden trifft angemessene organisatorische und technische Massnahmen, um sicherzustellen, dass Versichertendaten der Pensionskasse Hirslanden sicher und vor unbefugten Eingriffen geschützt sind. Dies gilt beim Verarbeiten, beim Transfer und bei der Dokumentation von solchen. Dazu gehören unter anderem folgende Massnahmen:

- a. Unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten verarbeitet bzw. gespeichert werden, zu verwehren. Das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Datenträgern ist zu verhindern.
- b. Die Sicherheit gegen den unbefugten Zugriff ist auch durch entsprechende Massnahmen zu gewährleisten.
- c. Beim Datentransport bzw. -transfer schützen die Bearbeitenden die Daten durch hinreichende Speicherung vor Verlust. Sie verhindern durch geeignete Massnahmen, dass unbefugte Personen die Daten während des Transfers lesen, kopieren, verändern oder löschen können.
- d. Personendaten dürfen strikt nur an der dafür vorgesehenen und dafür geeigneten Stelle gespeichert bzw. abgelegt werden. Die Speicherung auf privaten mobilen Speichermedien ist verboten.
- e. Der Zugriff der Bearbeitenden ist auf diejenigen Personendaten zu beschränken, die für die Erfüllung ihrer Aufgaben notwendig sind. Im Übrigen wird auf die Ausführungen der ICT-Reglemente und Konzepte der Hirslanden Gruppe verwiesen.

9 RECHTE DER BETROFFENEN

Jede betroffene Person hat in Bezug auf die Verarbeitung ihrer persönlichen Daten verschiedene Rechte: Auskunft bzw. Information und Mitteilung, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch und, soweit anwendbar, auch das Recht auf Datenübertragbarkeit. Entsprechende Prozesse, wie die Wahrnehmung dieser Rechte erfolgen soll, sind definiert.

10 DATENSCHUTZ-FOLGENABSCHÄTZUNG

Eine Datenverarbeitung kann zu besonderen Risiken für die Betroffenen führen, z. B. wenn eine umfangreiche Verarbeitung besonders schützenswerter Personendaten erfolgt. Sind derartige «besondere Risiken» von der künftigen oder geänderten Datenverarbeitung zu erwarten, muss eine sogenannte Datenschutz-Folgenabschätzung (DFA) durchgeführt werden. Die Pensionskasse Hirslanden hat einen Prozess und die Verantwortlichkeiten für die Einleitung und Durchführung der Datenschutz-Folgenabschätzung definiert, der den Datenschutzbeauftragten miteinschliesst.

11 MELDUNG VON DATENSCHUTZVERLETZUNGEN

Datenschutzverletzungen müssen unverzüglich gemeldet werden. Erfährt eine Person, die mit der Pensionskasse Hirslanden in einer arbeits-, auftrags- oder anderen vertragsrechtlichen Beziehung steht, von einer Verletzung dieser Weisung/Anordnung und/oder von einem Verstoss gegen datenschutzrechtliche Bestimmungen an sich, ist sie verpflichtet, diese unverzüglich per E-Mail an datenschutz@hirslanden.ch und cc. Leitung der Pensionskasse zu melden.

12 SCHULUNG/AWARENESS

Die Pensionskasse Hirslanden stellt ein generelles Datenschutzverständnis («Awareness») und zielgruppengerechte Schulungen sicher, einerseits prozessspezifisch durch den Datenschutzbeauftragten und andererseits durch umfangreiche bzw. regelmässige und obligatorische Schulungsaktivitäten der Hirslanden Gruppe (z. B. über Intranet-Kommunikation, Newsletter, E-Learnings). Diejenigen Mitarbeitenden oder Hilfspersonen, die Personendaten verarbeiten oder verarbeiten lassen, sind verpflichtet, die obligatorischen Schulungen zu absolvieren.

13 KONTROLLEN/AUDIT

Datenschutzrelevante Kontrollen sind im internen Kontrollsystem (IKS) abzubilden und Risiken, die sich aus der Bearbeitung von Personendaten ergeben, im jeweiligen Risikoregister einzutragen.

14 INKRAFTTRETEN

Diese Weisung/Anordnung tritt per 01. September 2023 in Kraft.