Bearbeitungsreglement

Einsiedler Krankenkasse

Klassifizierung	**Öffentlich**
Version	**1.3**
Letzte Bearbeitung	**2024_10_25**
Freigabe am	**2024_10_25**
Genehmigungsinstanz	**Geschäftsführung**
Verteiler	**GL Einsiedler Krankenkasse** **Mitarbeitende Einsiedler Krankenkasse – zDAS** **Homepage Einsiedler Krankenkasse**

1. Allgemeine Bestimmungen

1.1 Einsiedler Krankenkasse

Die Einsiedler Krankenkasse, nachfolgende EKK genannt, ist eine Krankenversicherung gemäss KVG und bietet Familien wie auch Einzelpersonen einen umfassenden Schutz in der Krankenversicherung (KVG) sowie diverse Versicherungen im Zusatz-Bereich (VVG) an.

1.2 Rechtliche Grundlagen

Gestützt auf Art. 5 und 6 DSV i. V. m. Art. 84b KVG hat die EKK ein Bearbeitungsreglement zu erstellen. Im Rahmen der Datenbearbeiten werden die Gesetze des KVG, VVG und DSG sowie die Verordnungen KKV (insbesondere Art. 59a), DSV und die VDSZ berücksichtigt. Die nachfolgenden Bestimmungen gelten sinngemäss auch für den Bereich der angebotenen Zusatzversicherungen nach VVG.

1.3 Ziel des Bearbeitungsreglements

Das Bearbeitungsreglement umschreibt insbesondere die Datenbearbeitungs- und Kontrollverfahren und den Betrieb der Datenbearbeitung. Es enthält Angaben über das für den Datenschutz und die Datensicherheit verantwortliche Organ, über die Herkunft der Daten und die Zwecke, für welche sie regelmässig bekannt gegeben werden und das Verfahren für die Erteilung der Zugriffsberechtigungen auf die entsprechenden Informationssysteme und Verzeichnisse. Das vorliegende Reglement wird laufend den gesetzlichen, organisatorischen und betrieblichen Änderungen angepasst.

1.4 Informationspflicht (Art. 19 DSG)

Das DSG verlangt die angemessene Information der betroffenen Person über die Beschaffung von Personendaten (Art. 19 DSG). Aufgrund des gesetzlichen Auftrags nach KVG zur Bearbeitung von Gesundheitsdaten gilt die Ausnahmereglung nach Art. 20 Abs. 1 lit. b DSG, wonach die Informationspflicht für die Datensammlung entfällt, wenn die Bearbeitung gesetzlich vorgesehen ist.

1.5 Interessierte Parteien

Die interessierten Parteien sind das BAG, EDÖB und die Versicherten.

1.6 Definitionen und Abkürzungen

Die folgenden Abkürzungen werden im Dokument verwendet:

Abkürzung	Beschreibung
Art.	Artikel
AG	Aktiengesellschaft
ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts
BAG	Bundesamt für Gesundheit
BBTI	BBTIndividual
BBTP	BBTPortal
DRG	Diagnosis-Related Groups
DSB	Datenschutzberater
DSG	Bundesgesetz über den Datenschutz
DSV	Verordnung zum Bundesgesetz über Datenschutz
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

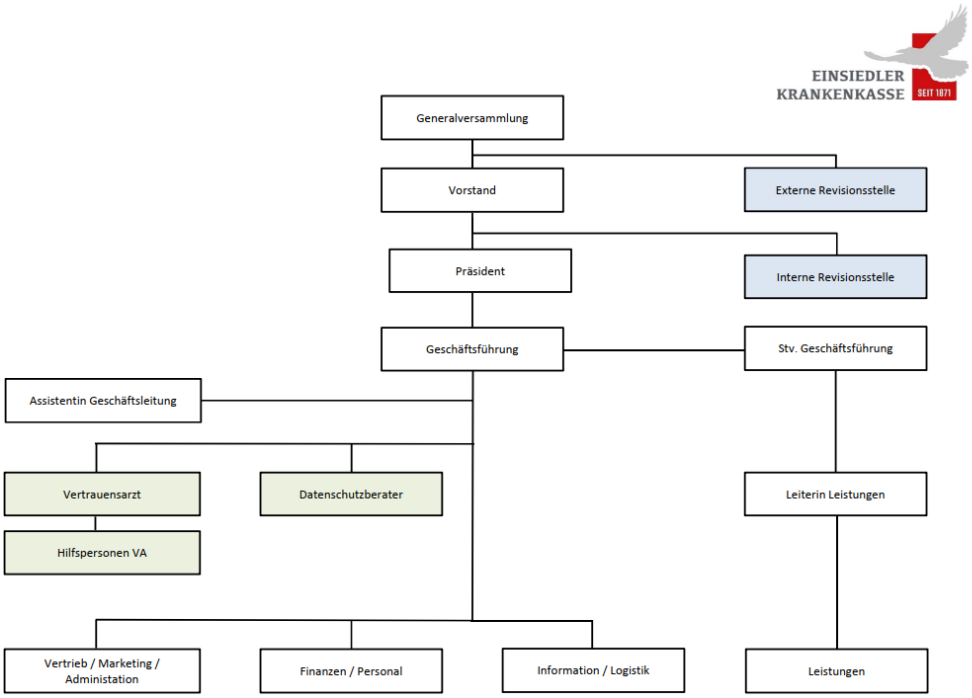
EKK	Einsiedler Krankenkasse
GEKVG	Gemeinsame Einrichtung KVG
GL	Geschäftsleitung
Inkl.	Inklusive
Kap.	Kapitel
KVG	Bundesgesetz über die Krankenversicherung
KVV	Verordnung über die Krankenversicherung
PV	Prozessverantwortliche Person
RVK	Dienstleistungen und Versicherungen für den Gesundheitsmarkt
SVK	Schweizerischer Verband für Gemeinschaftsaufgaben der Krankenversicherer
TOM	Technische und organisatorische Massnahmen
VAD	Vertrauensärztlicher Dienst
VDSZ	Verordnung über die Datenschutzzertifizierung
VVG	Bundesgesetz über den Versicherungsvertrag
zDAS	Zertifizierte Datenannahmestelle

2. Organisation

2.1 Verantwortlichkeiten

Die Gesamtverantwortung für den Datenschutz trägt der Vorstand der EKK. Diese Verantwortung ist nicht übertragbar. Die Geschäftsführung bzw. dessen Stellvertretung ist verantwortlich für die Umsetzung des Datenschutzes im Betrieb sowie IT-Themen wie das Betriebssystem, Anwendungen, die Datenbank, das Netzwerk und die Datensicherheit.

2.2 Organigramm interne Organisation



2.3 Verpflichtung Datenschutz

Die Mitarbeitenden der EKK unterzeichnen bei Stellenantritt eine Vertraulichkeits- und Schweigepflichterklärung. Die Mitarbeitenden sind in ihrer Funktion für die Schaffung der notwendigen und angemessenen Rahmenbedingungen für den Datenschutz verantwortlich. Die Mitarbeitenden werden periodisch über die Entwicklung im Datenschutzbereich informiert, geschult und sensibilisiert.

2.4 Schweigepflicht

Die Mitarbeitenden der EKK unterstehen während des Arbeitsverhältnisses und darüber hinaus der Schweigepflicht nach Art. 33 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) und Art. 62 des Bundesgesetzes über den Datenschutz (DSG).

2.5 Verzeichnis der Datenbearbeitungen

Die EKK führt ein Verzeichnis der Bearbeitungstätigkeiten, welches mindestens jährlich überprüft und bei Änderungen aktualisiert ist. Das Verzeichnis ist beim EDÖB gemeldet.

2.6 Datenschutzberater

Die EKK verfügt über einen beim EDÖB gemeldeten externen DSB. Der DSB kontrolliert die Einhaltung des Datenschutzes, berät und unterstützt die EKK bei der operativen Umsetzung des Datenschutzes im Betrieb.

3. Datenbearbeitungen

3.1 Zweck der Datenbearbeitungen

Die EKK bearbeitet Personendaten von versicherten Personen sowie von potenziellen Versicherungsnehmenden. Der Zweck ist in Art. 84 KVG geregelt. Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung des Gesetzes beauftragten Organe sind befugt, die Personendaten – einschliesslich der besonders schützenswerten Daten und Persönlichkeitsprofile – zu bearbeiten, um die ihnen nach dem Gesetz übertragenen Aufgaben ordnungsgemäss zu erfüllen.

3.2 Herkunft der Daten

Die Herkunft der Daten stammt in erster Linie von den Versicherten selbst oder von Versicherten ermächtigten Personen und Stellen, aus der Leistungsabwicklung von Leistungserbringern sowie von Amtsstellen.

3.3 Kategorien der Daten

Folgende Personendaten werden bearbeitet (Aufzählung ist nicht abschliessend):

- Identifikationsdaten (Name, Vorname, Versichertennummer, Familiennummer, Kartennummer, Information über Bevollmächtigte)
- Persönliche ID-Kennnummern (Passnummer, ID-Nummer, AHV-Nummer)
- Persönlichkeits- und Familiendaten (Geburtsdaten, Geburtsort, Geschlecht, Staatsangehörigkeit, Aufenthaltsbewilligung, Wohnsitz, Zivilstand, Heiratsdatum, Anzahl Kinder, Todesdatum, Berufliche Situation)
- Korrespondenzdaten (Postadresse, E-Mail)
- Daten im Zusammenhang mit dem Versicherungsantrag und dem Versicherungsvertrag (Gesundheitsfragebogen, Arztberichte, medizinische Informationen von Leistungserbringern oder anderen Versicherern, Vorbehalte, versicherte Risiken, Versicherungsmodelle und Versicherungsdeckung, Vertragsdauer)

- Daten zur Bearbeitung von Leistungen wie z.B.: Schadenmeldung, Rechnungen von Leistungserbringern, Arztberichte, Leistungsabrechnungen usw.
- Zahlungsdaten (Bank- oder Postverbindungen und Zahlungsart, Fakturierung und Prämienzahlung, ausstehende Beträge und Betreibungen, Kontoguthaben)
- Daten zur Bearbeitung auf der App/Homepage/Tracking
- IP-Adresse

Die Personendaten werden in folgende Kategorien eingeteilt:

1 allgemein zugänglich / öffentlich
2 intern
3 vertraulich / besonders schützenswert

3.4 Bekanntgabe an Dritte

Die Bekanntgabe an Dritte ist nur erlaubt, wenn diese aus rechtlichen Gründen und zwecks Erfüllung des Bearbeitungszwecks einen Anspruch auf Daten haben oder eine entsprechende schriftliche Einwilligung des Betroffenen vorliegt. Nach der Übertragung ist der Dritte als Datenempfänger für den Datenschutz und die Datensicherheit verantwortlich.

Daten können insbesondere bekannt gegeben werden für:

- Einhaltung der Versicherungspflicht
- Beurteilung von Leistungsansprüchen
- Verhinderung ungerechtfertigter Bezüge
- Koordination mit Leistungen anderer Sozialversicherungen
- Geltendmachung eines Rückgriffrechts gegenüber haftpflichtigen Dritten
- Zuweisung oder Verifikation der Sozialversicherungsnummer
- Führen von Statistiken

Die weitere Datenbekanntgabe ist abschliessend in Art. 84a KVG geregelt.

3.5 Aufbewahrung der Personendaten

Personendaten, welche zum Zweck der Bearbeitung nicht mehr erforderlich sind, werden vernichtet oder anonymisiert – vorbehältlich der gesetzlichen Aufbewahrungspflicht und Verjährungsfrist.

4. Technische und organisatorische Massnahmen

4.1 Physischer Zutritt

Der Zugang zu den Räumlichkeiten der EKK ist nur mit einem Schlüssel möglich. Der Zutritt für Dritte ist, ausgenommen im Empfangsbereich, nicht möglich. Ausserhalb der Arbeitszeiten werden die Räumlichkeiten der EKK abgeschlossen. Das Archiv ist nur Mitarbeitenden der EKK zugänglich. Vertrauliche Unterlagen, wie jene des Vorstandes, der Geschäftsleitung und des Vertrauensärztlichen Dienstes, werden separat archiviert und der Zugang ist jeweils nur für den verantwortlichen Mitarbeitenden möglich.

4.2 Elektronischer Zugriff

Die Zugriffsberechtigung bei der EKK erfolgt nach dem Need-to-know-Prinzip. Es werden nur Geräte ans interne Netzwerk geschlossen, die von der EKK zur Verfügung gestellt werden und entsprechend geschützt

sind. Es haben nur Mitarbeitende Zugriff auf Personendaten, die sie zwecks Erfüllung ihrer Aufgaben benötigen. Alle Mitarbeitende verfügen über ein persönliches Login. Die Zugriffsberechtigungen werden nur von autorisierten Personen vergeben und werden in einer Zugriffsmatrix dokumentiert. Nicht mehr benötigte Zugriffsrechte werden gesperrt oder gelöscht.

4.3 Bekanntgabekontrolle/Zusammenarbeit mit Partnern

Der Austausch von besonders schützenswerten Daten mit externen Partnern erfolgt in separat geschützten Bereichen. Die Übermittlung findet immer über einen verschlüsselten Kanal statt.

4.4 Vernichtung physischer oder elektronischer Daten/Geräte

Die Vernichtung von physischen und elektronischen Daten/Geräte erfolgt durch definierte Prozesse und zertifizierte Partner.

4.5 Datenschutzpolitik und Richtlinie Datenschutz und Datensicherheit

Die Mitarbeitenden der EKK sind zur Einhaltung der Datenschutzpolitik sowie der Richtlinie Datenschutz und Datensicherheit verpflichtet.

5. Kontrollverfahren

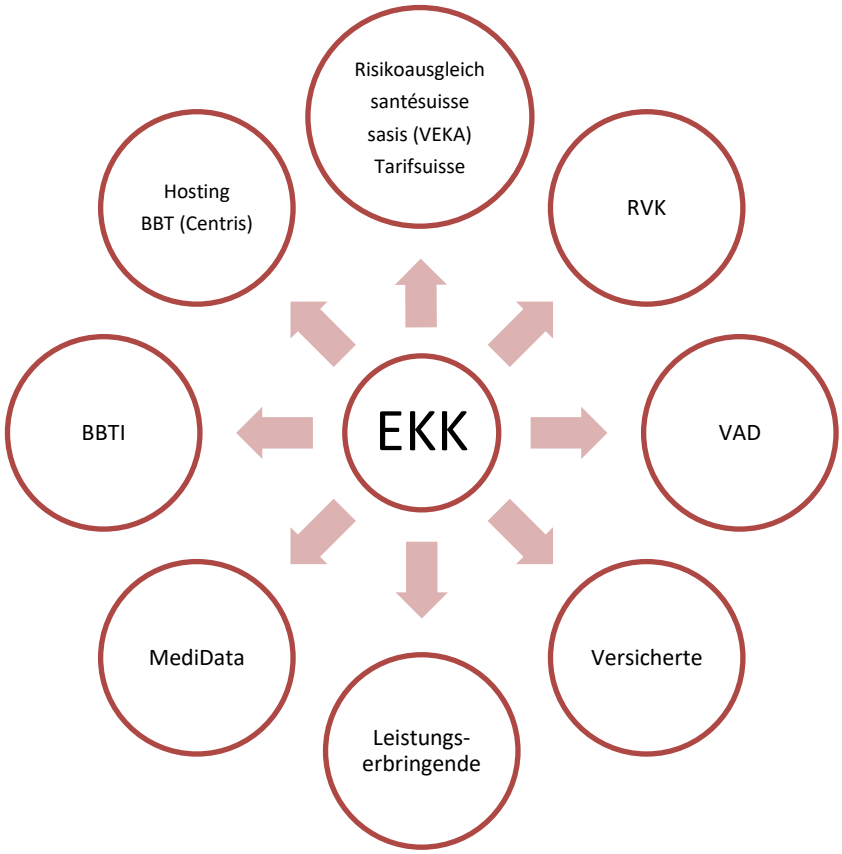
Folgende Kontrolle werden zwecks Gewährleistung Datenschutz und Datensicherheit umgesetzt:

- Periodische Kontrollen der Umsetzung der Datenschutzpolitik und der Richtlinien Datenschutz und Datensicherheit
- Periodische Kontrolle der Zugriffsrechte
- Halbjährliche Erneuerung der Passwörter
- Dokumentierte Prozesse bei Neu- und Austritten
- Jährliche Überprüfung der Dokumentationen und Weisungen
- Jährliche Schulung durch den externen DSB
- Jährliche Kontrolle der Massnahmen durch den externen DSB
- Jährliche interne Audits durch den externen DSB
- Jährliche Kontrolle durch die interne Revision
- Sorgfältige Auswahl, Instruktion und Kontrolle von externen Partnern
- Vertragliche Vorgaben mit externen Partnern zwecks Einhaltung der Vorschriften

6. Informationssystemstruktur

6.1 Übersicht System

Die nachfolgende Grafik zeigt die von der Datenbearbeitung betroffenen Systeme auf:



Die Kernapplikation für die Abwicklung der Krankenversicherung ist das BBTI. Die Kernapplikation wird über den Partner BBT Software AG betrieben. Die Verbindung zur internen IT-Infrastruktur erfolgt über Remote Access und über eine Multi-Faktor-Authentifizierung. Zusätzlich sind die Shared- und Kundensysteme durch eine Firewall getrennt.

6.2 Übersicht Sub- und Umsysteme

Nebst dem BBTI besteht das Informationssystem aus weiteren Sub- und Umsystemen, die entweder direkt das Krankenversicherungsgeschäft betreffen oder für den allgemeine Betrieb verwendet werden:

Sub- oder Umsystem	Bereich	Zweck
BBTI	Krankenversicherung	• Kernapplikation für die Durchführung des Kranken- und Unfallversicherungsgeschäfts
BBTP	Krankenversicherung	• Web-Portal für Kunden mit Einsicht in eigenes Dossier • Webrechner für Offerten
Sumex II	Krankenversicherung	• Austausch von elektronischen XML-Dokumenten zur schematischen und tariflichen Prüfung • Empfangen von elektronischen Rechnung direkt vom Leistungserbringer • Rechnungsprüfung anhand von aktuellen Tarif- und Referenzdaten
surplusReader	Krankenversicherung	• Erfasst Leistungsrechnungen als elektronisches XML • Nachbearbeitung und Weiterleitung ans BBTI oder zur Prüfung an Sumex II
Zertifizierte Datenannahmestelle	Krankenversicherung	• Entgegennahme, Prüfung und Weiterverarbeitung von DRG-Rechnungen
CaseNet (MediCasePool)	Krankenversicherung	• Webapplikation zum sicheren Austausch von vertrauensärztlichen Daten an den unabhängigen Vertrauensarzt
Veka	Krankenversicherung	• Versichertenkarte
Microsoft (RDP)	IT-Betrieb	• Einheitlicher Desktop für Mitarbeitende • Microsoft Office Produkte
Mitel	IT-Betrieb	• Software Übersicht telefonisch Erreichbarkeit
Infoniqa One 50	Finanz- und Rechnungswesen	• Führung der Finanz- und Lohnbuchhaltung
Schwyer Kantonalbank	Finanz- und Rechnungswesen	• Übermittlung Rechnungen
Six / Raiffeisen	Finanz- und Rechnungswesen	• Übermittlung LSV
Clicktime	HR-Management	• Zeiterfassungssoftware

Aufgrund von Sub- und Umsystemen ergeben sich weitere dokumentierte Schnittstellen.

6.3 Outsourcing

Voraussetzung für die Übertragung der Bearbeitung von Personendaten an externe Partner ist, dass die Daten nur so bearbeitet werden, wie das die EKK selbst tun würde und die Übertragung durch keine Geheimhaltungspflicht verboten ist. Diese Partner verpflichten sich mit Vertragsabschluss zur Einhaltung der Datenschutzbestimmungen für sich und ihre Hilfspersonen.

7. Prozessabläufe Datenschutz

Im Bereich Datenschutz sind folgende Prozesse wesentlich:

Prozess	Zuständig	Ablauf
Datenschutz-Folgeabschätzung (Art. 22 DSG)	GL	Kap. 7.1
Meldeprozess Verletzung Datensicherheit (Art. 24 DSG)	GL	Kap. 7.2
Auskunftsprozess (Art . 25 DSG)	GL	Kap. 7.3
Berichtigungsprozess (Art. 32 Abs. 1 DSG)	GL	Kap. 7.3

7.1 Datenschutz-Folgeabschätzung

Sofern ein hohes Risiko für die betroffene Person besteht, führt die EKK eine Datenschutz-Folgeabschätzung bei neuen Bearbeitungstätigkeiten und auch bei wesentlichen Weiterentwicklungen und Erweiterungen von Personendatenbearbeitungen.

7.2 Meldeprozess Verletzung Datensicherheit

Nr.	Inhalt	Beschreibung
1	Meldung	Eine mögliche Verletzung wird gemeldet. Die Meldung wird unverzüglich an die Geschäftsleitung weitergeleitet.
2	Prüfung intern	Die Geschäftsleitung überprüft den Vorfall, ob es sich um eine tatsächliche Verletzung handelt.
3	Dokumentation	Sämtliche relevanten Informationen werden dokumentiert.
4	Prüfung extern	Der externe Datenschutzberater wird miteinbezogen und es erfolgt ein erneute Triage der Verletzung.
5	Sofortmassnahmen	Es werden Sofortmassnahmen eingeleitet, um den Vorfall zu stoppen oder begrenzen. Falls erforderlich, wird die betroffene Person informiert.
6	Untersuchung	Der Vorfall wird zwecks Ursache und Auswirkungen untersucht.
7	Information EDÖB	Ist die Verletzung meldepflichtig, wird der EDÖB gemäss Anforderungen benachrichtigt.
8	Information betroffene Person	Die betroffene Person wird, sofern gesetzlich vorgeschrieben oder angemessen, über den Vorfall informiert. Die Person erhält Informationen über den Vorfall, getroffene Massnahmen
9	Massnahmen	Es werden Massnahmen zwecks Verhinderung zukünftiger Vorfälle umgesetzt.
10	Prävention	Um den Schutz und die Sicherheit von Personendaten zu erhöhen, wird ein kontinuierlicher Verbesserungsprozess eingeleitet.

7.3 Auskunfts- und Berichtigungsprozess

Nr.	Beschreibung	Zuständig
1	Eingang Begehren schriftlich per Mail oder Post inkl. Kopie amtlicher Ausweis wird der GL weitergeleitet.	PV
2	GL überprüft zusammen mit PV, ob betroffene Person bekannt und im System zu finden ist.	PV/GL
3	Der DSB wird miteinbezogen.	GL
4a	Bestehen kein Daten über die betroffenen Person, wird die betroffene Person entsprechend informiert.	GL
4b	Bestehen Daten über die betroffene Person, erfolgt eine Identifikationsprüfung der betroffenen Person	PV/GL
5	Ist die Identifikation erfolgreich, wird der betroffenen Person der Einfang des Begehren schriftlich bestätigt.	GL
6	Das Begehren wird bearbeitet.	PV
7	Das Begehren wird innerhalb der gesetzlichen Frist beantwortet.	GL

7.4 Auskunftsbegehren über die Gesundheit

Gesundheitsdaten der Person, die ein Auskunftsgesuch stellt, werden an den Vertrauensarzt der EKK übermittelt und nicht an die Person persönlich, die das Gesuch gestellt hat,.

8. Kontaktperson Datenschutz

Auskunfts- oder Berichtigungsbegehren können schriftlich, zusammen mit einer Kopie eines amtlichen Ausweises, an folgende Adresse und Kontaktperson gerichtet werden:

Einsiedler Krankenkasse
Betrieblicher Datenschutzverantwortlicher
Kronenstrasse 19
8840 Einsiedeln
datenschutz@kkeinsiedeln.ch

Wenn notwendig wird der externe Datenschutzberater zugezogen.

9. Abschliessende Bestimmungen

9.1 Aktualität

Das Reglement wird mindestens jährlich vom externen DSB überprüft und kann jederzeit geändert werden. Änderungen bedürfen der schriftlichen Form und Zustimmung durch die Geschäftsleitung.

9.2 Publikation

Die aktuelle Version des Bearbeitungsreglement ist auf der Homepage abrufbar.

Urs Kälin, Geschäftsührer

Mary Walker, Stv. Geschäftsführerin