Helsana

# Bearbeitungsreglement der Helsana-Gruppe

# 1. Zweck des Bearbeitungsreglements

Das Bearbeitungsreglement sorgt für die notwendige Transparenz im Umfeld sowohl der Systementwicklung als auch der Datenbearbeitung. Es wird in möglichst kurzer und verständlicher Form geführt, so dass die Systementwicklung und Datenbearbeitung auch von "Nicht-Experten" verstanden bzw. beurteilt werden können. Es gilt dabei den Grundsatz "so viel wie nötig, und so wenig wie möglich" reglementarisch zu erfassen.

In diesem Bearbeitungsreglement werden die Grundsätze der Datenbearbeitung für alle Datensammlungen der Versicherungsgesellschaften der Helsana-Gruppe (nachstehend auch «**Helsana**», «**wir**» oder «**uns**») festgehalten. Zu den Versicherungsgesellschaften der Helsana-Gruppe gehören die Helsana Versicherungen AG, die Helsana Zusatzversicherungen AG und die Helsana Unfall AG.

# 2. Datenbearbeitungen und Verfahren

## 2.1 Struktur

Die Datenbearbeitungen von Helsana sind in folgenden Datenaktivitäten aufgegliedert:

- Angebotsentwicklung Individualgeschäft (IG)
- Audit, Risk, Legal & Compliance
- Datensicherheitsmanagement
- Facility Management
- Gesundheitswissenschaften
- HR-Management
- In- und Exkasso, Finanzen, Aktuariat
- IT-Management
- Kundenservice IG
- Kundenservice Unternehmensgeschäft (UG)
- Leistungseinkauf IG
- Leistungsmanagement IG
- Leistungsmanagement UG
- Neugeschäft IG & UG
- Personalversicherung IG & UG
- Personalvorsorgestiftung
- Vertrauensärztlicher Dienst (VAD)
- Vertragsverwaltung IG
- Vertriebskanalmanagement IG
- Vertriebskanalmanagement UG
- Vertriebsunterstützung IG

Verschiedene Schnittstellen ermöglichen den direkten Kontakt mit externen Dienstleistern und Leistungserbringern, beispielsweise bei direkter Abrechnung des Leistungserbringers mit Helsana. Des Weiteren gibt es eine Schnittstelle, über welche bestimmte Leistungserbringer den Versicherungsschutz einer versicherten Person online prüfen können. Der Datenschutz und die entsprechende Datensicherheit werden mittels starker Authentifizierung sowie moderner Verschlüsselungs- und Übertragungstechnologie gewährleistet.

## 2.2 Datenbearbeitungsverfahren

Helsana hält in internen Reglementen fest, wie die Datenbearbeitungen zu inventarisieren und hinsichtlich Rechtmässigkeit zu prüfen sind (Compliance Checks). Die Verfahren zum Speichern, Bekanntgeben an Dritte, Aufbewahren, Archivieren, Pseudonymisieren, Anonymisieren, Löschen oder Vernichten der Daten sind in den jeweiligen Datenschutzkonzepten pro Datenbearbeitung festgehalten.

## 2.3 Benutzung und Datenzugriff

### 2.3.1 Zugriffsberechtigte

Zugriffsberechtigt auf die IT-Systeme von Helsana sind:

- Mitarbeitende von Helsana, soweit sie dies zur Ausübung ihres Auftrags «Abwicklung der Krankenversicherung» benötigen;
- Systemadministratoren von Helsana;
- Vertraglich mandatierte Dienstleister;

(alle zusammen Zugriffsberechtigte).

### 2.3.2 Verwaltung der Zugriffsberechtigten

Die Verwaltung der Zugriffsberechtigten wird zentral durch das Identity & Access Management von Helsana geführt. Interne und externe Mitarbeitende werden via HR-Schnittstelle gemeldet. Neue Identitäten inkl. Accounts werden nur erfasst, wenn ein gültiger Arbeitsvertrag oder Dienstleistungsvertrag existiert und eine entsprechende Freigabe der Rechte durch die linienvorgesetzte Person vorliegt.

### 2.3.3 Persönliche Zugriffsberechtigung

Mit dem Eintritt in Helsana erhalten alle Zugriffsberechtigten gemäss Rollenmodell, abgeleitet von der jeweiligen Funktion und ihrer organisatorischen Zugehörigkeit, ihre Zugriffsberechtigungen zu Informationen. Alle weiteren benötigten Rechte müssen via Berechtigungsportal individuell beantragt werden. Hierbei gilt, dass jeder Antrag durch die direkt vorgesetzte Person sowie, je nach Berechtigungsrolle, zusätzlich durch die rollengenehmigende Person bestätigt werden muss.

### 2.3.4 Aufhebung der Zugriffsberechtigung

Die Zugriffsberechtigten der IT-Systeme von Helsana sind nur so lange zugriffsberechtigt, als sie die Daten für die Ausübung ihrer Arbeitsfunktion benötigen. Bei Austritt sowie bei Aufgabenwechsel innerhalb von Helsana wird die Zugriffsberechtigung entzogen und die für den neuen Aufgabenbereich benötigten Zugriffsberechtigungen werden via Rollenmodell neu zugewiesen.

### 2.3.5 Ausbildung der Zugriffsberechtigten

Für die verschiedenen Applikationen und Subsysteme werden die Zugriffsberechtigten in Kursen geschult.

### 2.3.6 Handbücher und Bearbeitungsrichtlinien für die Zugriffsberechtigten

Zu den Subsystemen gibt es entsprechende Dokumente. Weiter wird in Weisungen, Reglementen und Leistungshandbüchern sowie in Listen die Datenbearbeitung festgelegt. Diese werden von den zuständigen Organisationseinheiten regelmässig aktualisiert.

Die zuständigen Organisationseinheiten schaffen mittels spezifischer Anweisungen einen für das gesamte Versicherungsgebiet der Schweiz gleichbleibenden Level der Leistungsbeurteilung nach Bundesgesetz über die Krankenversicherung (KVG).

### 2.3.7 IT-Dienstleister

Soweit der Betrieb von IT-Systemen von Helsana an externe IT-Dienstleister ausgelagert ist, folgen diese in ihrem Bereich analogen Regelungen.

# 3. Recht auf Auskunft, Berichtigung und Datenherausgabe

Die Betroffenen können gemäss Art. 25 des Bundesgesetzes über den Datenschutz (DSG) vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden, und diese Daten herausverlangen. Zudem haben sie das Recht, ihre Daten bei Helsana berichtigen zu lassen.

# 4. Technische und organisatorische Massnahmen zur Gewährleistung der Datensicherheit

## 4.1 Zugangskontrolle

Sämtliche Räumlichkeiten von Helsana in denen besonders schützenswerte Personendaten bearbeitet werden, sind entweder elektronisch oder manuell vor dem Zugang unbefugter Personen gesichert. Über die Schlüsselverwaltung und die elektronische Zutrittskontrolle wird durch die Verantwortlichen Protokoll geführt. Der Beauftragte für die physische Sicherheit kann jederzeit Einblick oder Auswertungen verlangen. Schutzzonen bestimmen die Sicherheitsvorkehrungen: Die Arbeitsplätze sind vor dem Zutritt unbefugter Dritter geschützt. Spezialräume und sensible Räume, wie die Technikräume und die Rechenzentren, sind wie folgt gesichert:

- Die IT-Systeme in den von der IT von Helsana betriebenen Rechenzentren und durch die IT von Helsana betriebenen dezentralen Server sind mit erhöhten physischen Sicherheitsanforderungen ausschliesslich für den Zugang spezifisch berechtigter Personen gesichert.
- Die IT-Systeme in dezentralen Servern, welche nicht durch die IT von Helsana betrieben werden, sind vergleichbaren Sicherheitsvorkehrungen unterstellt, wie diejenigen, die durch diese selbst betrieben werden.

Durch informationstechnische Vorkehrungen ist es ausschliesslich berechtigten Personen möglich, Daten zu bearbeiten. Nur berechtigte Personen erhalten Zugriff auf IT-Systeme von Helsana.

## 4.2 Authentifizierung der Zugriffsberechtigten

Der Zugriff auf IT-Systeme von Helsana wird durch die User-ID kombiniert mit einem zeitlich befristeten individuellen Autorisierungsmerkmal geschützt.

## 4.3 Bekanntgabekontrolle

Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, werden über die Schnittstellen identifiziert (z.B. Online-Deckungsabfragen durch Leistungserbringer im Zusammenhang mit dem Einsatz der Versichertenkarte).

## 4.4 Übermittlung von Daten

Die Übermittlung von Daten ist durch Verschlüsselungsverfahren geschützt.

## 4.5 Speicherkontrolle

Die Zugriffsberechtigten erhalten spezifische Berechtigungen für Mutationen in Datenfeldern, die sie für die Erfüllung der Aufgaben (z.B. gemäss KVG oder Bundesgesetz über die Unfallversicherung [UVG]) benötigen.

## 4.6 Technische Anforderungen an Endgeräte

Der Zugang zum internen Netzwerk von Helsana ist eingeschränkt, durch spezifische Kontrollmassnahmen geschützt und überwacht. Bei externen IT-Dienstleistern bestehen für deren Netzwerke analoge Vorkehrungen.

## 4.7 Massnahmen zum Schutz der Daten (Vertraulichkeit) im Bereich der Endgeräte

Sämtliche Datenendgeräte (Clients) sind mit technischen Sicherheitsmassnahmen mehrfach gegen Angriffe geschützt.

Ausgedruckte Daten werden so aufbewahrt, dass Drittpersonen (z.B. Raumpflegepersonal) diese nicht einsehen und/oder kopieren können. Diese Daten werden in Anwendung einer internen Weisung entweder in abschliessbaren Behältnissen aufbewahrt oder via Aktenvernichter oder Datarec entsorgt. Es gilt das Clean-Desk- sowie das Clear-Screen-Prinzip.

## 4.8 Protokollierung

Zusätzlich zur Kontrolle der Zugriffe auf IT-Systeme von Helsana über das Berechtigungsverfahren sowie den Schutz über die persönliche User-ID und Autorisierung, verfügen einzelne IT-Systeme über eine Protokollierung der automatisierten Bearbeitung, damit nachträglich festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben wurden. Die Protokollierung wird in Anwendung von Art. 4 der Verordnung über den Datenschutz (DSV) durchgeführt: Die Protokolle werden während 13 Monaten revisionsgerecht aufbewahrt. Sie sind ausschliesslich den Organen und Personen zugänglich, denen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung oder Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegt, und dürfen nur für diesen Zweck verwendet werden. Bei externen IT-Dienstleistern bestehen teilweise ähnliche, aber eigene Regelungen zur Protokollierung.

## 4.9 Entwicklung

Anfragen für die Weiterentwicklung des Systems werden zusammengefasst und als Maintenance oder Projekt definiert, budgetiert und realisiert. Das Verfahren sowie die Governance sind im Rahmen «Helsana-Projektvorgehen» geregelt.

## 4.10 Unterstützung der Zugriffsberechtigten und Meldepflicht

Fachlich werden die Zugriffsberechtigten durch die Fachführungen der jeweiligen Bereiche unterstützt. Die technische Unterstützung für die IT-Systeme und das Netzwerk wird durch die IT von Helsana erbracht oder in Auftrag gegeben.

Die Zugriffsberechtigten sind über den Schutzbedarf des IT-Systems von Helsana und die Vorschriften im Umgang mit dem IT-System und dessen Daten orientiert. Die Vorgaben sind in Weisungen und Sensibilisierungs-Merkblättern der Informationssicherheit beschrieben. Mögliche Sanktionen bei vorsätzlichen oder fahrlässigen Verletzungen der Informationssicherheit sind den Zugriffsberechtigten bekannt.

Sämtliche Verstösse sind gemäss dem Prozess Sicherheitsvorfall den Vorgesetzen oder gemäss Code of Conduct der Hinweisgeberstelle umgehend zu melden.

## 4.11 Aufsicht und Verantwortlichkeit

Die fachverantwortlichen Personen der IT-Systeme bzw. Applikationen beaufsichtigen, dass sich die Zugriffsberechtigten an die Weisungen sowie das vorliegende Bearbeitungsreglement und die externen IT-Dienstleister an ihre vertraglichen Vorgaben halten.

## 5. Version

Dieses Bearbeitungsreglement ist nicht Bestandteil eines Vertrags mit den Versicherten oder anderen Dritten. Wir können dieses Bearbeitungsreglement daher jederzeit anpassen. Die auf dieser Website veröffentlichte Version ist die jeweils aktuelle Fassung.

Letzte Aktualisierung: **September 2023**