

# Datenschutzerklärung und Bearbeitungsreglement Helsana Versicherungen AG

Version 1.01 vom 6.6.2018

## 1. Kurzüberblick

Die Grundversicherung für den Krankheitsfall ist für alle Einwohner der Schweiz obligatorisch. Die Helsana Versicherungen AG (**Helsana**) ist neben anderen Krankenkassen für die Abwicklung dieser obligatorischen Krankenversicherung verantwortlich und bietet dafür alle Leistungen an, die gesetzlich vorgeschrieben sind. Zur Abwicklung der obligatorischen Krankenversicherung, wozu als Beispiele die Ausrichtung von Leistungen oder das Prämieninkasso gehören, bearbeitet Helsana Personendaten. Unter Personendaten sind alle Angaben zu verstehen, die sich auf eine bestimmte oder bestimmbare (natürliche) Person beziehen. In erster Linie sind das Daten von Personen, die bei Helsana versichert sind und ihre Personendaten Helsana selber bekanntgeben. Zu diesen Daten gehören zum Beispiel Kontaktinformationen wie Name, Adresse oder Telefonnummer. Um ihren gesetzlichen Auftrag zu erfüllen, ist Helsana auf weitere persönliche Daten wie Geburtsdatum, AHV- und Versichertennummer sowie Angaben zur Gesundheit von Personen angewiesen.

Da Helsana grossen Wert auf den Schutz dieser zum Teil besonders schützenswerten Daten legt, wird in dieser Datenschutzerklärung darüber informiert:

- Wer für die Datenbearbeitung verantwortlich ist;
- Von welchen Personen welche Daten erhoben und bearbeitet werden;
- Wie und von wem die Daten erhoben und bearbeitet werden;
- Zu welchem Zweck die Daten bearbeitet werden und auf welcher rechtlichen Grundlage;
- Wem die Daten bekanntgegeben werden;
- Wie lange die Daten aufbewahrt werden;
- Was die Rechte der betroffenen Personen sind.

## 2. Anwendbarkeit der Datenschutzerklärung

Diese Datenschutzerklärung erläutert die Beschaffung und weitere Bearbeitungen von Personendaten durch Helsana. Sie dient gleichzeitig als Bearbeitungsreglement für die im Sinne von Art. 11 und Art. 21 der Verordnung zum Bundesgesetz über den Datenschutz (**VDSG**) in Verbindung mit Art. 84b des Bundesgesetzes über die Krankenversicherung (**KVG**).

Vorbehalten bleiben die Beschaffung und weitere Bearbeitungen von Personendaten, die durch andere Datenschutzerklärungen oder Nutzungsbedingungen abgedeckt sind, aus den Umständen hervorgehen oder gesetzlich geregelt sind.

### 3. Verantwortliche, Datenschutzbeauftragter

Für die Beschaffung und weitere Bearbeitungen von Personendaten im Zusammenhang mit der Abwicklung der obligatorischen Krankenversicherung ist Helsana die verantwortliche Stelle (so insbesondere im Sinne von Art. 4 Abs. 7 der europäischen Datenschutz-Grundverordnung [**DSGVO**] und des Bundesgesetzes über den Datenschutz, soweit die jeweiligen Bestimmungen im Einzelfall zur Anwendung gelangen).

Allfällige datenschutzrechtliche Anfragen, Ansprüche oder Auskünfte betreffend Helsana können unter Beilage einer Kopie eines amtlichen Ausweises an den Datenschutzbeauftragten von Helsana an folgende Kontaktadresse gerichtet werden:

Helsana Versicherungen AG  
Datenschutzbeauftragter  
Postfach  
8081 Zürich

Soweit Helsana in den Anwendungsbereich der DSGVO fällt, ist Active-Assets A<sup>2</sup> GmbH sowohl ihr Datenschutzbeauftragter im Sinne von Art. 37 DSGVO als auch ihr Vertreter nach Art. 27 DSGVO. Seine Kontaktdaten sind:

Active-Assets A<sup>2</sup> GmbH  
Gottlieb-Daimler-Str. 5  
78467 Konstanz  
Deutschland  
[privacy@helsana.ch](mailto:privacy@helsana.ch)

### 4. Erhebung, Bearbeitung und Nutzung von Personendaten

#### 4.1 Betroffene Personen

Helsana erhebt und bearbeitet Personendaten von

- Personen, die bei Helsana oder einem anderen Krankenversicherer der Helsana Gruppe versichert sind oder waren;
- Personen, welche als Familienvorstand, Zahler oder bevollmächtigte Person angegeben werden (diese müssen nicht zwingend über eine Versicherung bei Helsana verfügen).
- Personen, die Helsana oder einem anderen Krankenversicherer der Helsana Gruppe zur Einhaltung der Versicherungspflicht durch Kantone zugewiesen werden (vgl. Art. 6 KVG);
- Teilnehmern der von Helsana durchgeführten Marktforschungs-, Kundenzufriedenheits- und Meinungsumfragen;
- möglichen oder tatsächlichen Interessenten der Produkte und Dienstleistungen von Helsana

(alle zusammen **Kunden**).

Ferner erhebt und bearbeitet Helsana Daten von Leistungserbringern, Vertrauensärzten, Dienstleistern, Vertriebspartner und weiteren Geschäftspartnern von Helsana sowie von deren Mitarbeitenden und Kontakten (**Partner**);

Helsana bearbeitet namentlich folgende Kategorien von Personendaten von Kunden:

- **Persönliche Daten und Kontaktinformationen:** Dazu gehören insbesondere, aber nicht abschliessend, Vor- und Nachname, Geschlecht, Geburtsdatum, Alter, Zivilstand, AHV- und Versicherungsnummer, Sprachen, Nationalität, Kantons- und Gemeindezugehörigkeit, (E-Mail-)Adresse, Telefonnummer, Gesundheitsdaten, Familienangehörige, etc.;
- **Daten im Zusammenhang mit Kommunikation:** Darunter fallen Angaben wie bevorzugter Kommunikationskanal, Korrespondenz und Kommunikation mit Helsana per Brief, E-Mail, Telefon, Online-Kundenportal myHelsana oder andere Weise (einschliesslich Aufzeichnungen der Kommunikation), Kundenzufriedenheit, etc.;
- **Vertragsdaten:** Art der Versicherung und Deckung, Art und Umfang der Leistungen, Eintritts- und Austrittsdatum, Sistierung, Franchisen;
- **Daten im Zusammenhang mit Leistungsabwicklungen:** Dazu gehören unter anderem Leistungserbringer, Diagnosen, Arztberichte, Angaben von Vertrauensärzten, Leistungskosten, Bank- und Post-Verbindungen, Zahlungen, Daten von Drittversicherern, Angaben im Zusammenhang mit Rückfragen, Rechnungen des Leistungserbringers;
- **Daten im Zusammenhang mit der Prämienberechnung und -erhebung:** Dazu gehören namentlich Versicherungsprämie, Prämienfakturierung, Prämienverbilligung Kanton, Inkassodaten, etc.;
- **Daten im Zusammenhang mit Rechtsstreitigkeiten:** Darunter fallen insbesondere Daten betreffend Beschwerden und Differenzen zu Leistungen bzw. den dazu geschlossenen Verträgen wie etwa Regresse und Streitigkeiten sowie Daten aus Verfahrensakten von Behörden und Gerichten, etc.;
- **Daten im Zusammenhang mit der Nutzung des Online-Kundenportals myHelsana:** Dazu gehören insbesondere IP-Adresse und andere Identifikatoren (z.B., MAC-Adresse des Smartphone oder Computers, Cookies), Zugangsdaten (inklusive Passwörter), Datum und Dauer der Versicherungsvertragsbeziehung, Datum, Zeit und Anzahl der Besuche der Website, abgerufene Seiten und Inhalte, verweisende Webseiten;
- **Daten im Zusammenhang mit dem Marketing von Produkten und Dienstleistungen:** Dazu gehören Angaben wie Newsletter An-/Abmeldungen, erhaltene Unterlagen und spezielle Aktivitäten, persönliche Präferenzen und Interessen etc.;
- **Daten im Zusammenhang mit Case Management:** Angaben zu Gesundheit, Arbeitgeber und Arbeitsverhältnis, medizinischen, sozialen und arbeitsplatzspezifischen Gegebenheiten und entsprechendem Unterstützungsbedarf etc.

(alle zusammen **Kundendaten**).

Ferner bearbeitet Helsana namentlich folgende Kategorien von Personendaten von Partnern:

- **Daten von Leistungserbringern, Dienstleistern und weiteren Geschäftspartnern und Angaben zu deren Mitarbeitern und Kontakten,** so insbesondere Kontaktangaben, Angaben zur Funktion, Angaben zum bisherigen Verkehr mit diesen Personen, Angaben über Marketingaktivitäten (z.B. Erhalt von Newslettern), Angaben zu geschäftlichen Transaktionen, Anfragen, Of-

feren, Angebote, Konditionen und Verträge (insbesondere im Zusammenhang mit Tarifverträgen), Angaben zu Ausbildungen und beruflichen Tätigkeit, etc. (**Partnerdaten**);

Im Rahmen ihrer Geschäftsbeziehung werden Kunden diejenigen Kundendaten bereitstellen müssen, die für die Aufnahme und Abwicklung der Vertragsbeziehung und Erfüllung der damit verbundenen vertraglichen Pflichten notwendig oder gesetzlich vorgeschrieben sind. Ohne diese Daten wird Helsana in der Regel nicht in der Lage sein, den Vertrag mit dem jeweiligen Kunden zu schliessen oder diesen auszuführen. Dies gilt analog auch für die Partnerdaten, soweit es um Geschäftsbeziehungen zu Dienstleistern, Lieferanten und Geschäftspartnern von Helsana geht; diese können grundsätzlich ohne Angaben zu deren Mitarbeitern und anderen Kontakten grundsätzlich nicht abgeschlossen und abgewickelt werden. Zwingend ist auch die Protokollierung der Zugriffe auf die über die Website abrufbaren Dienstleistungen (insbesondere im Zusammenhang mit dem Kundenportal myHelsana), und die damit verbundene Erhebung der Verbindungsdaten (wie IP-Adresse); diese erfolgt automatisch bei der Benutzung und lässt sich nicht für einzelne Besucher bzw. Kunden abstellen.

## 4.2 Datenquellen

Die Personendaten werden in erster Linie bei der direkten Kommunikation mit den Kunden (Brief, Kontakt- und Antragsformulare, E-Mail, Telefon, oder auf andere Weise) sowie im Rahmen der Benutzung der Website erhoben.

Personendaten können aber auch indirekt erhoben werden, so namentlich durch

- von Kunden ermächtigte Personen und Stellen;
- andere (Kranken)-Versicherer innerhalb und ausserhalb der Helsana Gruppe (Art. 84a KVG);
- Leistungserbringer und Vertrauensärzte;
- Informationsaustausch im Rahmen der Amts- und Verwaltungshilfe (Art. 32 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrecht [ATSG]);
- öffentlich zugängliche Quellen (z.B. Internet, Presse, Medien, Register);
- Zukauf von ergänzenden Angaben von Datenquellen Dritter (z.B. Adresshändler).

## 4.3 Datenbearbeiter bzw. beteiligte Stellen

Die Abwicklung der obligatorischen Krankenversicherung wird in erster Linie von Mitarbeitenden der regionalen Kundenservices und Generalagenturen/Verkaufsstellen vorgenommen. Für diese Aufgabe bearbeiten sie Personendaten inkl. besonders schützenswerte Personendaten gemäss in der Datensammlung von Helsana (vgl. Ziff. 9).

Bei der Durchführung der obligatorischen Krankenversicherung haben die Mitarbeitenden im Rahmen der nachfolgend aufgeführten Datenbearbeitungsaktivitäten (die **Datenaktivitäten**) jeweils auf diejenigen Daten Zugriff, die für die jeweilige Aufgabenerfüllung erforderlich sind:

- Vertriebskanalmanagement und Vertriebsunterstützung;
- Angebotsentwicklung
- Neukundengeschäft;
- Kundenservice;
- Vertragsverwaltung;

- Leistungsmanagement;
- Leistungseinkauf;
- Personalversicherung;
- Vertrauensärztlicher Dienst;
- Gesundheitswissenschaften;
- Inkasso, Finanzen, Aktuariat;
- Risikoausgleich;
- Audit, Risk, Legal und Compliance;
- IT-Management und Datensicherheitsmanagement;
- Personalvorsorgestiftung;
- Einkauf.

Für die Einhaltung der Bestimmungen der Weisungen und Reglemente zur Datenbearbeitung im Zusammenhang mit den Datenaktivitäten bei Helsana sorgen sogenannte Prozessowner. Sie sind verantwortlich, dass ihre Applikationsdaten nur im gesetzlich definierten Rahmen zur Verfügung gestellt werden.

#### **4.4 Automatisierte Einzelentscheide**

Bei Helsana werden im Rahmen der Leistungsabwicklung automatisierte Einzelentscheide getroffen. Reichen Kunden oder Leistungserbringer der Helsana eine Rechnung ein, erfolgt die Prüfung, ob die beanspruchte Leistung unter den gesetzlichen Leistungskatalog (Art. 24 ff. KVG, Art. 33 ff. KVV und Krankenpflege-Leistungsverordnung KLV) fällt und damit auch Entscheidung, ob eine Anspruchsberechtigung besteht, automatisiert. Dabei erfolgt kein Profiling, da nur die Rechnungen anhand von Daten gemäss Verträgen und Tarifen überprüft werden (vgl. Ziff. 4.5). Soweit im Zusammenhang mit dem Inkasso ein Schuldbetreibungsverfahren eingeleitet worden ist, erfolgen die weiteren Schritte (Fortsetzungsbegehren, Konkursbegehren, Verwertungsbegehren etc.) insofern automatisiert, als sie nach Ablauf der entsprechenden Frist gestellt werden, soweit die Forderung noch nicht beglichen worden ist.

Solche automatisierten Einzelentscheide erfolgen, da sie für die Erfüllung des Versicherungsvertrags zwischen den Kunden und Helsana erforderlich sind und angemessene Massnahmen bestehen, dass die Rechte und berechtigten Interessen der betroffenen Personen gewahrt werden (vgl. Ziff. 11).

#### **4.5 Profiling**

Automatisierte Bearbeitungen von Personendaten zur Bewertung bestimmter persönlicher Aspekte, die sich auf natürliche Personen beziehen (Profiling), erfolgen bei Helsana namentlich in folgenden Bereichen bzw. zu folgenden Zwecken:

- Vertriebsaktivitäten und Kundenbefragungen sowie Angebotsmanagement;
- Zahlungsverhaltens- und Kostenanalyse.

Helsana wertet aus verschiedenen Quellen bezogene Daten nach bestimmten Kriterien aus. Dies tut sie insbesondere, um zu ermitteln, welche Produkte bestimmte Personen interessieren könnten oder um Produkte zu entwickeln, die auf die Bedürfnisse von gewissen Personen zugeschnitten sind.

## 5. Zweck und Rechtsgrundlagen der Datenbearbeitung

### 5.1 Kundendaten

Die Kundendaten werden in erster Linie für die ordentliche Durchführung der obligatorischen Krankenversicherung gemäss den nachfolgenden, gesetzlichen Zwecken erhoben (Art. 84 KVG):

- Einhaltung der Versicherungspflicht;
- Prämienberechnung und -erhebung;
- Beurteilung von Leistungsansprüchen sowie Leistungsberechnung, -gewährung und Koordination mit Leistungen anderer Sozialversicherungen;
- Beurteilung des Anspruchs auf Prämienverbilligungen nach Art. 65 KVG sowie Berechnung und Gewährung der Verbilligungen;
- Geltendmachung von Rückgriffsrechten gegenüber einem haftpflichtigen Dritten (Regress);
- Führung von Statistiken;
- Zuweisung und Verifizierung der Versichertennummer der Alters- und Hinterlassenenversicherung;
- Berechnung des Risikoausgleichs.
- Bekanntgaben an Dritte gemäss Art. 84a KVG.

Datenbearbeitungen dienen insbesondere und soweit gesetzlich zulässig darüber hinaus (auch) zu folgenden Zwecken:

- Schutz von Kunden, Mitarbeitern und anderer Personen insbesondere bei Bedrohungsfällen betreffend Mitarbeitende und Schutz der Daten, die Helsana anvertrauten Geheimnisse und Vermögenswerte, Sicherheit der Systeme und Gebäude von Helsana;
- Im Zusammenhang mit angebotenen Dienstleistungen, Vertragsabschluss, Abwicklung von Verträgen, Pflege und Entwicklung von Kundenbeziehungen, Kommunikation, Kundendienst und Support, Promotionen, Werbung und Marketing (inklusive Newsletter und Zusendung von Werbematerial);
- Verwaltung, Betrieb, und Weiterentwicklung der Website (einschliesslich der Bereitstellung von Funktionen, welche Identifikatoren oder andere Personendaten voraussetzen) und weiterer IT-Systeme, Identitätsprüfungen;
- Einhaltung der rechtlichen und regulatorischen Anforderungen und internen Regeln von Helsana, Verfolgung und Umsetzung von diversen Rechten, Abwehr von Rechtsansprüchen, Zivilprozess, Beschwerden, Missbrauchsbekämpfung, für die Zwecke von rechtlichen Untersuchungen oder Verfahren und zur Beantwortung von Anfragen von Behörden;
- Qualitätskontrolle, Marktforschung, Weiterentwicklung von Produkten und Dienstleistungen, Erstellung von Statistiken, Budgets, Aufzeichnungen und Managementinformationen und weiterer Berichte über Kunden, Transaktionen und Aktivitäten, Angebote und sonstige geschäftliche Aspekte von Helsana für die Zwecke der Geschäftsführung und Entwicklung des Unternehmens, seines Angebots und seiner Aktivitäten, Projektmanagement;
- Verkauf oder Kauf von Geschäftsbereichen, Gesellschaften oder Teilen von Gesellschaften und andere gesellschaftsrechtliche Transaktionen und damit verbunden die Übertragung von Kundendaten;

- Für andere Zwecke, soweit eine gesetzliche Pflicht die Bearbeitung erfordert oder diese zum Zeitpunkt der Datenerhebung aus den Umständen erkennbar oder angezeigt waren,

(zusammen der **Kundenbearbeitungszweck**).

Helsana verwendet die Kundendaten für den Kundenbearbeitungszweck aufgrund folgender Rechtsgrundlagen:

- Vertragserfüllung;
- Erfüllung einer rechtlichen Verpflichtung von Helsana;
- Einwilligung des Kunden (insbesondere soweit eine Bearbeitung auf konkrete Rückfrage erfolgt, die jederzeit zurückgezogen werden kann, so namentlich für den Empfang von Newslettern, für den sich der Kunde angemeldet hat);
- Berechtigte Interessen von Helsana, insbesondere
  - Effizienter und effektiver Schutz von Kunden, Mitarbeitern und anderen Personen und Schutz der Daten, Geheimnisse und Vermögenswerte von Helsana und die ihr anvertraut worden sind, Sicherheit der Systeme und Gebäude von Helsana;
  - Einhaltung der rechtlichen und regulatorischen Anforderungen und internen Regeln von Helsana;
  - Effiziente und effektive Kundenbetreuung, Kontaktpflege und sonstige Kommunikation mit Kunden auch ausserhalb der Vertragsabwicklung;
  - Aufrechterhaltung und sichere, effiziente und effektive Organisation des Geschäftsbetriebs, einschliesslich eines sicheren, effizienten und effektiven Betriebs und einer erfolgreichen Weiterentwicklung der Website und anderer IT-Systeme;
  - Verkauf und Lieferung von Produkten und Dienstleistungen, auch mit Bezug auf Personen, die nicht direkt Vertragspartner sind (wie z.B. begünstigte Personen);
  - Sinnvolle Unternehmensführung und -entwicklung;
  - Nachvollzug von Kundenverhalten, -aktivitäten, -vorliegen und -bedürfnisse, Marktstudien;
  - Effiziente und effektive Verbesserung der bestehenden Produkte und Dienstleistungen und Entwicklung neuer Produkte und Dienstleistungen;
  - Durchführung von Werbung und Marketing;
  - Betrieb der Website und sonstiger Systeme von Helsana;
  - Erfolgreicher Verkauf oder Kauf von Geschäftsbereichen, Gesellschaften oder Teilen von Gesellschaften und andere gesellschaftsrechtliche Transaktionen;
  - Interesse an der Verhinderung von Betrug, Vergehen und Verbrechen sowie an Untersuchungen im Zusammenhang mit solchen Delikten und sonstigem unangebrachten Verhalten, Behandlung von rechtlichen Klagen und Vorgehen gegenüber Helsana, Mitwirkung an Rechtsverfahren und Kooperation mit Behörden, und sonst die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

## 5.2 Partnerdaten

Helsana kann Partnerdaten soweit nach anwendbarem Datenschutzrecht zulässig insbesondere zu den folgenden Zwecken bearbeiten: des Abschlusses und der Abwicklung von Verträgen und sonstigen

Geschäftsbeziehungen mit Partner, Promotionen, Werbung und Marketing, Kommunikation, Einladung an Anlässe und Teilnahme an Aktionen für Partner, Durchführung gemeinsamer Aktivitäten, Einhaltung der rechtlichen und regulatorischen Anforderungen und internen Regeln von Helsana, Verfolgung und Umsetzung von diversen Rechten, Abwehr von Rechtsansprüchen, Zivilprozessen, Beschwerden, Betrugs- und Missbrauchsbekämpfung, für die Zwecke von rechtlichen Untersuchungen oder Verfahren und zur Beantwortung von Anfragen von Behörden, für den Verkauf oder Kauf von Geschäftsbereichen, Gesellschaften oder Teilen von Gesellschaften und andere gesellschaftsrechtliche Transaktionen und damit verbunden die Übertragung von Partnerdaten. Sie tut dies auf der derselben Basis wie oben für Kundendaten dargelegt.

## **6. Datenbekanntgabe an Dritte**

### **6.1 Schweigepflicht**

Sämtliche Mitarbeitenden von Helsana unterstehen der Schweigepflicht (Art. 33 ATSG). Bei Verletzungen der Schweigepflicht unterstehen Mitarbeitende einer spezialgesetzlichen Strafbestimmung (Art. 54 KVAG). Die Mitarbeitenden sind über die Sanktionen informiert und unterzeichnen mit Eintritt bei Helsana zudem eine Geheimhaltungs- und Schweigepflichterklärung.

### **6.2 Ausnahmen von der Schweigepflicht**

Die Ausnahmen von der Schweigepflicht sind gesetzlich geregelt (Art. 84, Art. 84a KVG und Art. 32 ATSG) und bestehen, sofern kein überwiegendes Privatinteresse entgegensteht, insbesondere für die Bearbeitung von Personendaten durch

- Dritte im Auftrag von Helsana;
- Weitere Dritte, sofern im Einzelfall eine schriftliche Einwilligung der betroffenen Person vorliegt, das Einholen einer Einwilligung nicht möglich ist, oder die Einwilligung nach den Umständen als im Interesse der versicherten Person vorausgesetzt werden darf;
- Andere Organe der Kranken- oder Sozialversicherung, sofern es für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist oder eine gesetzliche Pflicht zur Bekanntgabe besteht;
- Weitere Behörden, Gerichte und Amtsstellen (z.B. im Zusammenhang mit Quellensteuern, Bundesstatistik, Strafanzeige und Verbrechenabwehrung, Prämieninkasso).

Nicht personenbezogene Daten dürfen bekanntgegeben werden, sofern es einem überwiegenden Interesse entspricht. Sofern die Anonymität der betroffenen Personen gewahrt wird, dürfen Daten von allgemeinem Interesse veröffentlicht werden.

### **6.3 Kategorien von Dritten**

Helsana kann Kundendaten und Partnerdaten soweit nach anwendbarem (Datenschutz)-Recht zulässig an folgende Kategorien von Dritten weitergeben, welche die Personendaten für den jeweiligen Bearbeitungszweck im Auftrag von Helsana oder für eigene Zwecke bearbeiten:

- Betroffene Personen (insbesondere Versicherte) und von ihnen bevollmächtigte Dritte;
- Familienvorstand des Vertrags (falls angegeben) mit Bezug auf Daten von mitversicherten Familienmitgliedern;
- Weitere Gesellschaften der Helsana Gruppe (beispielsweise mit Helsana Zusatzversicherungen AG im Rahmen der Prüfung eines Versicherungsantrages für Zusatzversicherungen);



- Andere (Kranken-)Versicherer ausserhalb der Helsana Gruppe;
- Branchenorganisationen, Verbände, Organisationen und weitere Gremien;
- Leistungserbringer, Vertrauensärzte, Ombudsstelle;
- Dienstleister (innerhalb und ausserhalb der Helsana Gruppe); einschliesslich Auftragsbearbeiter;
- Lieferanten und sonstige Geschäftspartner;
- Erwerber oder Interessenten am Erwerb von Geschäftsbereichen, Gesellschaften oder sonstigen Teilen von Helsana;
- Medien;
- Öffentlichkeit, einschliesslich Besucher von Websites und sozialen Medien von Helsana;
- Lokale, nationale und ausländische Behörden und Amtsstellen (insbesondere Organe von Bund und Kantonen, IV-Stellen etc.);
- Andere Parteien in möglichen oder tatsächlichen Rechtsverfahren.

## **7. Datenübermittlung ins Ausland**

Helsana kann Kundendaten und Partnerdaten innerhalb von Helsana wie auch an Dritte in jedes Land der Erde übermitteln, insbesondere in alle Länder, in denen die Dienstleister von Helsana ihre Daten bearbeiten (so namentlich Niederlanden, Irland, Deutschland). Werden Daten in ein Land ohne angemessenen Datenschutz übermittelt, so gewährleistet Helsana einen angemessenen Schutz mittels Einsatz hinreichender vertraglicher Garantien, so namentlich auf Basis der EU-Standardvertragsklauseln, Binding Corporate Rules oder stützt sich auf die Ausnahmen der Einwilligung, der Vertragsabwicklung, der Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen, des überwiegenden öffentlichen Interesses, der vom Kunden, Besuchern oder Partnern veröffentlichten Daten oder weil es zum Schutz der Unversehrtheit dieser Personen nötig ist. Der Kunde, Besucher und Partner kann schriftlich unter Beilage einer Kopie eines amtlichen Ausweises an die oben genannte Kontaktadresse (vgl. Ziff. 3) eine Kopie der vertraglichen Garantien verlangen oder erfährt dadurch, wo eine solche Kopie eingeholt werden kann. Helsana behält sich vor, solche Kopien aus datenschutzrechtlichen Gründen oder aus Geheimhaltungsgründen zu schwärzen.

Datenübermittlungen ins Ausland erfolgen insbesondere gegenüber der gemeinsamen Einrichtung, die als gesetzliche Verbindungsstelle zwischen Helsana und Organen der Sozialversicherung von Staaten der EU dient, namentlich zur Koordination der Leistungsabrechnung (Art. 95a KVG und Art. 19 der Verordnung über die Krankenversicherung.)

## **8. Datenaufbewahrung**

Helsana speichert vertragsbezogene Kundendaten und Partnerdaten grundsätzlich für die Dauer des Vertragsverhältnisses und zehn Jahre über die Beendigung des Vertragsverhältnisses hinaus, soweit im Einzelfall keine kürzeren oder längeren gesetzlichen Aufbewahrungspflichten bestehen, dies aus Beweisgründen erforderlich ist oder ein anderer nach anwendbarem Recht gültiger Ausnahmegrund besteht, oder eine frühere Löschung angezeigt ist (namentlich weil die Daten nicht mehr benötigt werden oder Helsana zu deren Löschung verpflichtet ist).

Für betriebliche Daten, die Kundendaten oder Partnerdaten enthalten (z.B. Protokolle, Logs), gelten grundsätzlich kürzere Aufbewahrungsfristen von maximal 13 Monaten.

Geschäftliche Unterlagen, einschliesslich Kommunikation, werden so lange aufbewahrt, wie Helsana ein Interesse daran hat (so insbesondere ein Beweisinteresse im Falle von Ansprüchen, Dokumentation der Einhaltung bestimmter gesetzlicher und anderer Vorgaben, ein Interesse an nicht personenbezogenen Auswertung) oder dazu verpflichtet ist (vertraglich, gesetzlich oder aufgrund von anderen Vorgaben). Vorbehalten bleiben gesetzliche Pflichten etwa bezüglich Anonymisierung oder Pseudonymisierung von Daten.

## **9. Helsana-Datensammlung**

### **9.1 Struktur**

Die Datensammlung von Helsana ist nach Datenaktivitäten gegliedert und umfasst folgende Kategorien:

- Vertriebskanalmanagement und Vertriebsunterstützung;
- Angebotsentwicklung;
- Neukundengeschäft;
- Kundenservice;
- Vertragsverwaltung;
- Leistungsmanagement;
- Leistungseinkauf;
- Personalversicherung;
- Vertrauensärztlicher Dienst;
- Gesundheitswissenschaften;
- Inkasso, Finanzen, Aktuariat;
- Risikoausgleich;
- Audit, Risk, Legal und Compliance;
- IT-Management und Datensicherheitsmanagement;
- Personalvorsorgestiftung;
- Einkauf.

Verschiedene Schnittstellen, wie z.B. MediData, 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 eines Versicherten online prüfen können. Der Datenschutz und die entsprechende Datensicherheit werden mittels starker Authentifizierung, moderner Verschlüsselungs- und Übertragungstechnologie gewährleistet.

### **9.2 Benutzung und Datenzugriff**

#### **9.2.1 Zugriffsberechtigte**

Zugriffsberechtigt auf das Helsana-Informationssystem sind:

- Mitarbeitende von Helsana, soweit sie dies zur Ausübung ihres Auftrags "Abwicklung der Krankenversicherung" benötigen;

- Systemadministratoren von Helsana;
- Vertraglich mandatierte Dienstleister;

(alle zusammen **Zugriffsberechtigte**).

### **9.2.2 Verwaltung der Zugriffsberechtigten**

Die Verwaltung der Zugriffsberechtigten wird zentral von der IT der Helsana geführt. Interne Mitarbeiter werden via HR-Schnittstelle und externe Mitarbeiter über das jeweilige Sourcing gemeldet. Neue Identitäten inkl. Accounts werden nur erfasst, wenn ein gültiger Arbeitsvertrag oder Dienstleistungsvertrag existiert und eine entsprechende Freigabe der Rechte durch den Linienvorgesetzten vorliegt.

### **9.2.3 Persönliche Zugriffsberechtigung**

Mit dem Eintritt in die Helsana erhält jeder Zugriffsberechtigte gemäss Rollenmodell, ableitend von seiner Funktion, seine Zugriffsberechtigungen zu Informationen. Alle weiteren benötigten Rechte müssen via Berechtigungsportal individuell beantragt werden. Hierbei gilt, dass jeder Antrag durch den direkten Vorgesetzten sowie, je nach Berechtigungsrolle, zusätzlich durch den Rollengenehmiger bestätigt werden muss.

### **9.2.4 Aufhebung der Zugriffsberechtigung**

Die Zugriffsberechtigten des Helsana-Informationssystem 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.

### **9.2.5 Ausbildung der Zugriffsberechtigten**

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

### **9.2.6 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 spezifischen Anweisungen einen für das gesamte Versicherungsgebiet der Schweiz gleichbleibenden Level der Leistungsbeurteilung nach KVG.

### **9.2.7 IT-Dienstleister**

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

## **10. Technische und organisatorische Massnahmen**

### **10.1 Zugangskontrolle**

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

### **10.2 Personendatenträgerkontrollen**

Durch informationstechnische Vorkehrungen ist es ausschliesslich berechtigten Personen möglich, Daten auf den elektronischen Datenträgern zu bearbeiten. Nur berechtigte Personen erhalten Zugriff auf das Helsana-Informationssystem.

### **10.3 Authentifizierung der Zugriffsberechtigten**

Der Zugriff auf die Subsysteme des Helsana-Informationssystems wird durch die User-ID kombiniert mit einem zeitlich befristeten individuellen Passwort geschützt.

### **10.4 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).

### **10.5 Übermittlung von Daten**

Die Übermittlung von Daten zwischen den Datenendstationen und den Hostcomputern ist durch das Übertragungsprotokoll geschützt.

### **10.6 Speicherkontrolle**

Die Zugriffsberechtigten erhalten spezifische Berechtigungen für Mutationen in Datenfeldern, die sie für die Erfüllung der Aufgaben gemäss KVG benötigen.

## **10.7 Technische Anforderungen an Endgeräte**

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

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

Die Datenendgeräte sind in geschützten Zonen platziert. Mobile Datenendgeräte enthalten Datenspeicher, die durch ein starkes, passwortabhängiges Verschlüsselungsverfahren geschützt sind.

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.

## **10.9 Protokollierung**

Zusätzlich zur Kontrolle der Zugriffe auf das Helsana-Informationssystem über das Berechtigungsverfahren sowie den Schutz über die persönliche User-ID und Passwort-Erkennung, verfügen einzelne Subsysteme 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. 10 VDSG durchgeführt: Die Protokolle werden während 13 Monaten revisionsgerecht aufbewahrt. Sie sind ausschliesslich den Organen zugänglich, denen die Überwachung der Datenschutz- und Datensicherheitsvorschriften obliegt und dürfen nur für diesen Zweck verwendet werden. Bei externen IT-Dienstleistern bestehen teilweise ähnliche, aber eigene Regelungen zur Protokollierung.

## **10.10 Entwicklung**

Anfragen für die Weiterentwicklung des Systems werden zusammengefasst und als Maintenance, Kleinvorhaben oder Projekt definiert, budgetiert und realisiert. Das Verfahren ist im Rahmen "Helsana-Projektvorgehen" geregelt.

## **10.11 Unterstützung der Zugriffsberechtigten und Meldepflicht**

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

Die Zugriffsberechtigten sind über die Sicherheitseinstufung des Helsana-Informationssystems und die Vorschriften im Umgang mit dem System und dessen Daten orientiert. Die Bestimmungen sind in Betriebshandbüchern unter Informationssicherheit beschrieben. Mögliche Sanktionen bei vorsätzlichen oder fahrlässigen Verletzungen der Informationssicherheit sind den Zugriffsberechtigten bekannt.

Sämtliche Zugriffsberechtigten sind verpflichtet, folgende Feststellungen dem Prozessowner oder Vertreter der Zugriffsberechtigten zu melden:

- Beobachtete oder vermutete Schwachstellen bzw. Sicherheitsmängel des Systems;
- Nicht umgesetzte oder nicht eingehaltene Sicherheitsmassnahmen;

- Unvorhergesehene Ereignisse, die eine Auswirkung auf die Informationssicherheit haben können.

## **10.12 Aufsicht und Verantwortlichkeit**

Die Prozessowner der Subsysteme beaufsichtigen, dass sich die Zugriffsberechtigten an die Weisungen, das vorliegende Bearbeitungsreglement und die externen IT-Dienstleister an ihre vertraglichen Vorgaben halten.

## **11. Rechte der Kunden, Besucher und Partner**

Jede betroffene Person, Kunde, Besucher und Partner, hat gegenüber Helsana ein Auskunftsrecht über sie betreffende Personendaten. Zudem hat sie das Recht, von Helsana die Berichtigung, Löschung und Einschränkung von sie betreffende Personendaten zu verlangen sowie einer solchen Bearbeitung von Personendaten zu widersprechen. Falls die Bearbeitung der Personendaten auf einer Einwilligung beruht, kann die Einwilligung durch die betroffene Person jederzeit widerrufen werden. In Staaten der EU bzw. dem EWR hat die betroffene Person in gewissen Fällen das Recht, die bei der Nutzung von Online-Diensten generierten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, das die weitere Nutzung und Übermittlung ermöglicht. Anfragen im Zusammenhang mit diesen Rechten sind schriftlich unter Beilage einer Kopie eines amtlichen Ausweises an die Kontaktadresse (vgl. Ziff. 3) zu richten. Helsana behält sich vor, die Rechte der betroffenen Person im Rahmen des jeweils anwendbaren Rechts einzuschränken und z.B. keine vollständige Auskunft zu erteilen oder Daten nicht zu löschen.

Wenn Helsana automatisiert eine einzelne Person betreffende Entscheidung vornimmt, die gegenüber der betroffenen Person rechtliche Wirkungen entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, kann die betroffene Person bei Helsana mit einer zuständigen Person sprechen und von ihr eine Wiedererwägung des Entscheids verlangen, oder von vornherein die Beurteilung durch eine Person verlangen, soweit das anwendbare Recht dies vorsieht. In diesem Fall kann die betroffene Person gewisse automatisierte Dienstleistungen unter Umständen nicht mehr nutzen. Die Person wird über solche Entscheide nachfolgend oder separat vorgängig informiert.

Jede betroffene Person hat das Recht, bei der zuständigen Datenschutzbehörde eine Beschwerde einzureichen. In der Schweiz ist dies der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte (<http://www.edoeb.admin.ch>).

## **12. Änderung der Datenschutzerklärung**

Helsana kann die vorliegende Datenschutzerklärung jederzeit ohne Vorankündigung und Mitteilung anpassen. Es gilt die jeweils aktuelle, auf der Website publizierte Fassung.

Soweit die Datenschutzerklärung Teil einer Vereinbarung mit Kunden und Partnern ist, kann Helsana diese im Falle einer Aktualisierung über die Änderung per E-Mail oder auf andere geeignete Weise informieren. Erfolgt innert 30 Tagen kein Widerspruch, so gilt die neue Datenschutzerklärung als vereinbart. Wird widersprochen, kann Helsana die Vereinbarung ausserordentlich und fristlos auflösen.

\* \* \* \* \*