2401-02

KUNDENINFORMATION ZU DEN DATENBEARBEITUNGEN NACH KVG

Ausgabe 2024

BEARBEITUNGSREGLEMENT NACH ARTIKEL 84B KVG IN VERBINDUNG MIT ARTIKEL 6 DSV

INHALTSVERZEICHNIS

1 Allgemeine Bestimmungen

2 Bearbeitungszweck der Kundendaten bei Atupri

3 Datensammlungen von Atupri

4 IT-Infrastruktur

5 Datenbearbeitung

6 Aufbewahrung von Personendaten

7 Interne Organisation

8 Technische und organisatorische Massnahmen von Atupri

9 Zugriffsberechtigungen

10 Massnahmen zur Datenminimierung

11 Angaben zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung

12 Publikation

BEARBEITUNGSREGLEMENT NACH ARTIKEL 84B KVG
IN VERBINDUNG MIT ARTIKEL 6 DSV

INHALTSVERZEICHNIS

1 ALLGEMEINE BESTIMMUNGEN
1.1 Abkürzungen
1.2 Ausgangslage

2 BEARBEITUNGSZWECK DER KUNDENDATEN BEI ATUPRI

3 DATENSAMMLUNGEN VON ATUPRI
3.1 Datensammlung der Datenannahmestelle gemäss Artikel 59*a* KVV
3.2 Datensammlung vertrauensärztlicher Dienst (VAD)
3.3 Datensammlung Versicherte KVG

4 IT-INFRASTRUKTUR
4.1 Kernsysteme
4.2 Schnittstellen
4.3 Aufgabenübertragung

5 DATENBEARBEITUNG
5.1 Herkunft der Personendaten
5.2 Kategorien betroffener Personen
5.3 Kategorien von Personendaten
5.4 Datenbekanntgabe an Dritte

6 AUFBEWAHRUNG VON PERSONENDATEN

7 INTERNE ORGANISATION
7.1 Geschäftsleitung
7.2 Datenschutzberater
7.3 Risikomanagement
7.4 ICT Security Officer
7.5 Datenannahmestelle
7.6 Datenschutzkoordinatoren
7.7 Bereiche und Mitarbeitende

8 TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN VON ATUPRI

9 ZUGRIFFSBERECHTIGUNGEN

10 MASSNAHMEN ZUR DATENMINIMIERUNG

11 ANGABEN ZUM VERFAHREN ZUR AUSÜBUNG DES AUSKUNFTSRECHTS UND DES RECHTS AUF DATENHERAUSGABE ODER -ÜBERTRAGUNG

12 PUBLIKATION

1 ALLGEMEINE BESTIMMUNGEN

Diese Kundeninformation KVG enthält Angaben zur Bearbeitung von Personendaten, zur Aufbewahrung und Archivierung der Personendaten, zur Datensicherheit sowie zu den Betroffenenrechten. Insgesamt zeigt die Kundeninformation KVG nebst der internen Organisation von Atupri die Datenbearbeitungs- und Kontrollverfahren von Atupri im Bereich der Krankenversicherung nach KVG auf.

Die Kundeninformation KVG stellt das nach Artikel 84*b* des Bundesgesetzes über die Krankenversicherung (KVG) in Verbindung mit Artikel 6 der Verordnung zum Bundesgesetz über den Datenschutz (DSV) zu erlassende Bearbeitungsreglement dar.

1.1 Abkürzungen

Abkürzung	Bedeutung
Abs.	Absatz
AG	Aktiengesellschaft
AHV	Alters- und Hinterlassenenversicherung
Art.	Artikel
ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts
BAG	Bundesamt für Gesundheit
CD	Compact Disc
DAS	Datenannahmestelle
DRG	Diagnosis-Related Groups
DSG	Bundesgesetz über den Datenschutz
DSV	Verordnung zum Bundesgesetz über den Datenschutz
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
HMO-Partner	Health-Maintenance-Organization-Partner
i. V. m.	in Verbindung mit
ID	Identitätskarte
IT	Informationstechnik
KOBE	Kostenbeteiligung
KVAG	Bundesgesetz betreffend die Aufsicht über die soziale Krankenversicherung (Krankenversicherungsaufsichtsgesetz)
KVG	Bundesgesetz über die Krankenversicherung
KVV	Verordnung über die Krankenversicherung
lit.	Litera
OR	Obligationenrecht
RCG	Recht, Compliance und Generalsekretariat
SVK	Schweizerischer Verband für Gemeinschaftsaufgaben der Krankenversicherer
TOMS	technische und organisatorische Massnahmen
usw.	und so weiter
VA	Vertrauensarzt
VAD	vertrauensärztlicher Dienst
VEKA	Versichertenkarte
VVG	Bundesgesetz über den Versicherungsvertrag
VVK	Verordnung über die Versichertenkarte für die obligatorische Krankenpflegeversicherung
z. B.	zum Beispiel
ZSR	Zahlstellenregister
ZVR	Zentrales Vertragsregister

1.2 Ausgangslage

Atupri bearbeitet als Krankenversicherer die Personendaten ihrer Versicherten, wie insbesondere deren Gesundheitsdaten, welche als besonders schützenswert gelten. Atupri bearbeitet diese Daten, um ihren gesetzlichen Auftrag, namentlich die Abwicklung der Kranken- und Unfallversicherung im Bereich des Bundesgesetzes über die Krankenversicherung (KVG), zu erfüllen (Art. 84 KVG).

Die Bearbeitung von Personendaten ist in Artikel 33 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) und in den Artikeln 84 und 84*a* KVG geregelt. Nebst den Anforderungen des KVG zum Datenschutz gelten das Bundesgesetz über den Datenschutz (DSG) sowie die Verordnung zum Datenschutzgesetz (DSV). Atupri muss sich bei der Bearbeitung von Personendaten an die allgemeinen Bearbeitungsgrundsätze halten.

Atupri hat für die Datensammlung, welche besonders schützenswerte Personendaten beinhalten, basierend auf Artikel 84*b* KVG in Verbindung mit Artikel 6 der Verordnung zum Bundesgesetz über den Datenschutz (DSV), die vorliegende Kundeninformation KVG erstellt.

2 BEARBEITUNGSZWECK DER KUNDENDATEN BEI ATUPRI

Atupri bearbeitet als Gesundheitsversicherer im KVG-Bereich Personendaten, einschliesslich besonders schützenswerter Daten, die sie benötigt, um die ihr nach dem KVG und dem KVAG übertragenen Aufgaben zu erfüllen (Art. 84 KVG i. V. m. Art. 34 Abs. 2 lit. a KVG).

Insbesondere sind dies folgende Bearbeitungszwecke:
- Für die Einhaltung der Versicherungspflicht sorgen
- Die Prämien berechnen und erheben
- Leistungsansprüche beurteilen
- Leistungen berechnen und gewähren
- Leistungen mit anderen Sozialversicherungen koordinieren
- Anspruch auf Prämienverbilligung nach Artikel 65 KVG beurteilen

- Verbilligungen berechnen und gewähren
- Rückgriffsrechte gegenüber haftpflichtigen Dritten geltend machen
- Die Aufsicht über die Durchführung des KVG ausüben
- Erhebung von Statistiken gemäss KVAG
- Erfüllung von gesetzlichen Aufbewahrungspflichten
- Überwachungsmassnahmen zum Schutz von IT-Infrastruktur, Gebäuden und Anlagen (beispielsweise Zutrittskontrollen, Netzwerk- und E-Mail-Scanner, Telefonaufzeichnungen, Überwachung von E-Mail und Internet)

3 DATENSAMMLUNGEN VON ATUPRI

Im Zusammenhang mit den Dienstleistungen von Atupri als Kranken- und Unfallversicherer nach KVG bezwecken die Datensammlungen von Atupri die Durchführung der obligatorischen Kranken- und Unfallversicherung nach KVG.

Atupri führt drei Datensammlungen: die Datensammlung der Datenannahmestelle gemäss Artikel 59*a* KVV, die Datensammlung des Vertrauensarztes sowie die Datensammlung zu den Personendaten von Versicherten nach KVG.

3.1 Datensammlung der Datenannahmestelle gemäss Artikel 59a KVV

Funktionsweise der zertifizierten Datenannahmestelle (DAS)

Bei Rechnungen für stationäre Aufenthalte (Somatik, Psychiatrie und Rehabilitationen) hat der Gesetzgeber festgelegt, dass der Empfang und die Prüfung der elektronischen Datensätze (Rechnungen) aus Datenschutzüberlegungen über eine zertifizierte Datenannahmestelle abgewickelt werden müssen.

Atupri hat die Centris AG und – für stationäre Spezialdiagnosen – den Schweizerischen Verband für Gemeinschaftsaufgaben der Krankenversicherer (SVK) als zertifizierte Datenannahmestellen dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gemeldet. Nur speziell berechtigte Mitarbeitende des vertrauensärztlichen Dienstes haben Zugriff auf die zu prüfenden Daten. Die jährlich überprüften Zertifizierungen stellen sicher, dass insbesondere die Anforderungen des Datenschutzes gewährleistet und die Persönlichkeitsrechte der Betroffenen sichergestellt werden. Die detaillierte Organisation und die Abläufe der DRG-Prüfung bei Atupri sind in einer separaten Arbeitsanleitung des vertrauensärztlichen Dienstes festgehalten.

3.2 Datensammlung vertrauensärztlicher Dienst (VAD)

Vertrauensärzte und Vertrauensärztinnen beraten die Versicherer in medizinischen Fachfragen sowie in Fragen der Vergütung und der Tarifanwendung. Sie prüfen insbesondere die Voraussetzung der Leistungspflicht des Versicherers (Art. 57 Abs. 4 KVG). Die Leistungserbringer müssen den Vertrauensärzten die zur Erfüllung dieser Aufgaben notwendigen Dokumente und Daten liefern (Art. 57 Abs. 6 KVG). Dabei kann es sich um Daten von Kunden handeln, die dem Datenschutz unterliegen. Die an den Vertrauensarzt gerichteten Dokumente gelangen unabhängig von ihrem Eingangskanal und ungeöffnet an den VAD von Atupri.

Detaillierte Prüfung von DRG-Rechnungen durch den vertrauensärztlichen Dienst

Lediglich Rechnungen, welche von der DAS als auffällig taxiert werden, gehen zur detaillierten Prüfung an den VAD von Atupri. Detaillierte Ausführungen zu Prozessen und die Vergabe der Berechtigungen sind in der Arbeitsanleitung des vertrauensärztlichen Diensts geregelt.

3.3 Datensammlung Versicherte KVG

Atupri verwendet Kernsysteme für die Verwaltung von Versichertendaten, für die Versichertenbetreuung und die Leistungsabwicklung. Eines der Kernsysteme wird zur elektronischen Dokumentenarchivierung eingesetzt. Bei den Kernsystemen sind Berechtigungsregeln hinterlegt, welche garantieren, dass die Mitarbeitenden nur auf diejenigen Personendaten zugreifen können, die für die Erfüllung der Aufgaben notwendig sind.

Berechtigung Kernsysteme

Wer auf die Kernsysteme Zugriff hat, ist in einem separaten Berechtigungskonzept festgehalten. Siehe auch Kapitel 9.

Speicherung der Kernsystem-Daten

Die Personendaten unserer Kunden, auf die die Kernsysteme zugreifen, sind auf den Servern einer Firma in der Schweiz gespeichert. Die Firma selbst hat ihren Sitz ebenfalls in der Schweiz.

4 IT-INFRASTRUKTUR

4.1 Kernsysteme

Atupri bearbeitet die Daten in Kernsystemen. Folgende versicherungsrelevante Daten werden bearbeitet:

- Vertragsdaten (Vorname, Name, Versicherten-Nr., Adresse, AHV-Nummern, SV-Nummer, Versichertendeckung, Prämienverbilligung)
- Leistungsverarbeitung (Leistungsdaten, die für die Abrechnung notwendig sind)
- Inkasso – Mahnwesen
- Archiv

4.2 Schnittstellen

Im Rahmen der Durchführung und Abwicklung der Krankenversicherung im KVG-Bereich unterhält Atupri Schnittstellen zu Datenbezügern und -lieferanten, welche nachfolgend beschrieben werden:

EMPFÄNGER/LIEFERANT	ZWECK	BESONDERS SCHÜTZENSWERTE PERSONENDATEN	AUSLÖSER
Banken/Finanzdienstleister	Zahlungsverkehr	Nein	Automatisch/manuell
Behörden/Gerichte	Art. 82 KVG / Art. 84a KVG	Ja	Manuell
Datendrehscheibe	Leistungsverarbeitung KVG	Ja	Automatisch
Externe Druckerei	Versand Kundenmagazin	Nein	Automatisch
Gemeinsame Einrichtung KVG	Risikoausgleich	Nein	Manuell
HMO-Partner	Gatekeeping, Einhaltung Vertrag	Ja	Automatisch
Informatikanbieter	Service und Betrieb der Informatikinfrastruktur	Ja	Automatisch
Kantone	Individuelle Prämienverbilligung	Ja	Manuell
Leistungserbringer	Art. 84a KVG	Ja	Automatisch/manuell
Partner telemedizinische Dienstleistung	Gesundheitsbetreuung	Ja	Automatisch
Partner Regress	Regress	Ja	Automatisch
Santésuisse	Auskünfte, ZSR, Datenpool	Nein	Automatisch
Sozialversicherer	Art. 84a KVG	Ja	Manuell
SVK	Seltene VAD-Dienstleistungen	Nein	Manuell
VEKA/Vicard	Versichertenkarte (Art. 42a KVG, VVK)	Ja	Automatisch
Versicherte	Auskunft	Ja	Automatisch/manuell
Vertrauensärzte	VAD-Aufgaben	Ja	Manuell
ZVR	Auskunft	Nein	Manuell

4.3 Aufgabenübertragung

Atupri darf von Gesetzes wegen als Krankenversicherer einem Dritten Aufgaben übertragen (Art. 6 Abs. 1 KVAG). Zwischen den externen Dienstleistungsunternehmen und Atupri existieren Zusammenarbeitsverträge, in denen auch der Datenschutz geregelt wird.

5 DATENBEARBEITUNG

Atupri bearbeitet die Personendaten, die sie für die Durchführung der sozialen Krankenversicherung nach KVG benötigt (Art. 84 KVG).

5.1 Herkunft der Personendaten

Atupri bearbeitet jene Personendaten, die sie im Rahmen der ihr nach Artikel 84 KVG zugewiesenen Aufgaben einholen muss. Gewisse Personendaten erhält Atupri auch bei der Abwicklung ihrer Aufgaben. Sie erhält diese beispielsweise direkt von den versicherten Personen, von Behörden oder von Leistungserbringern, die stationäre Leistungen nach DRG erbringen. Die Kategorien betroffener Personen und die Kategorien der bearbeiteten Personendaten sind in Kapitel 5.2 und 5.3 beschrieben.

5.2 Kategorien betroffener Personen

Atupri bearbeitet verschiedene Kategorien von betroffenen Personen. Es sind dies:

- Versicherte Personen
- Potenzielle Kunden
- Ehemalige Kunden
- Behörden (Ansprechpersonen)
- Dienstleister (Ansprechpersonen)
- Personen, die als Familienvorstand, Prämienzahler oder bevollmächtigte Person angegeben werden und nicht über eine Versicherung bei Atupri verfügen
- Auftragnehmer
- Partner
- Leistungserbringer
- Vertrauensärzte

5.3 Kategorien von Personendaten

Atupri bearbeitet namentlich, aber nicht abschliessend die folgenden Kategorien von Personendaten:

- Persönliche Identifikation und Anredeeigenschaften (Vorname, Name)
- Persönliche Datumsangaben und Familiendaten (Geburtsdatum, Heiratsdatum, Todesdatum, Geburtsdatum [Ehe] Partner*in, Zivilstand [inkl. Datum], Anzahl Kinder, Geburtsort, Staatsangehörigkeit bei der Geburt, Wohnsitzland/-länder [Ländercode], [Nationalitätscode/]Nationalität, andere Nationalitäten [Nationalitätscode], Heimatort)
- Persönliche Merkmale (Alter, Geschlecht, Lebenszyklusphase [z. B. in Ausbildung, Renten, erwerbstätig, arbeitslos], Aufenthaltsstatus, Mitgliedschaften)
- Kontaktangaben (Korrespondenz- und Kommunikationsdaten)

- Persönliche ID-Nummer in öffentlichen Registern/ Verzeichnissen (Nummern auf amtlichen Ausweisen, z. B. Passnummer, Identitätskartennummer, AHV-Nummer)
- Kunden-Identifikatoren (Familiennummer, Versichertennummer, Debitorennummer, Kartennummern, myAtupri Teilnehmernummer, Information [Name, Adresse] über Bevollmächtigte, IBAN/BIC, Benutzer-IDs [Log-in-IDs], Passwörter, Bankdetails Kunde bei Dritten)
- Referenznummern zu Produkten (Fakturanummer)
- Referenznummern zu Dienstleistungen (Rechnungsnummern Dritter [Arzt, Spital usw.])
- Identifikatoren zur Kundenbeziehung (Name/ Abkürzung des internen Kundenkontakts, Marktsegment, Status Beziehung [aktiv/inaktiv], Kontowährung)
- Informationen zur Bonität (Prämien, Prämienausstände, KOBE-Ausstände, Leistungsausstände, Betreibungsbetrag, Betreibungsnummer, Pfändungsnummer, Dossiernummer)
- Daten betreffend Leistungsabwicklung
- Daten betreffend Website/Apps und Tracking
- ID- oder Pass-Informationen
- IP-Adresse

5.4 Datenbekanntgabe an Dritte

Atupri darf Daten in Abweichung von Artikel 33 ATSG bekannt geben, sofern kein überwiegendes Privatinteresse entgegensteht und zudem die in Artikel 84*a* Absatz 1 Bst. a bis h KVG abschliessend geregelten Voraussetzungen erfüllt sind. Während nach Artikel 84*a* Absatz 1 Bst. a bis g^{bis} KVG die Datenbekanntgaben ohne vorgängiges schriftliches Gesuch erfolgen können, dürfen gemäss Bst. h dieser Bestimmung Daten an Sozialhilfebehörden, Zivilgerichte, Strafgerichte, Strafuntersuchungsbehörden, Betreibungsämter und Kindes- und Erwachsenenschutzbehörden nur im Einzelfall und auf schriftlich begründetes Gesuch hin bekannt gegeben werden.

6 AUFBEWAHRUNG VON PERSONENDATEN

Das DSG sieht keine konkreten Aufbewahrungsfristen vor. Aus dem Bearbeitungsgrundsatz der Verhältnismässigkeit kann abgeleitet werden, dass Daten, die nicht mehr benötigt werden, zu vernichten sind. Atupri stellt im Alltag in der Regel auf die allgemeine Verjährungsfrist von 10 Jahren ab (Art. 958*f* OR).

Archivierung und Aufbewahrung der Datensammlung der Datenannahmestelle
Die Daten werden bei der Centris AG gespeichert. Die Aufbewahrungsdauer richtet sich nach den spezifischen gesetzlichen Bestimmungen. Die Aufbewahrung erfolgt maximal während 10 Jahren (Art. 958*f* OR), sofern dem kein überwiegendes Interesse von Atupri entgegensteht. Danach werden die Daten gelöscht. Wenn die medizinischen Angaben nach Artikel 59 Absatz 1 KVV nicht verschlüsselt aufbewahrt werden müssen, so werden die Personalien der Versicherten zur Aufbewahrung dieser Angaben pseudonymisiert. Die Aufhebung der Pseudonymisierung oder Verschlüsselung darf nur durch die Vertrauensärzte erfolgen (Art. 59*a*^{ter} Abs. 2 KVV).

Archivierung und Aufbewahrung der Datensammlung des vertrauensärztlichen Dienstes
Auf die physische Ablage und Aufbewahrung von Dokumenten im vertrauensärztlichen Dienst wird grundsätzlich verzichtet. Nach der Fallbearbeitung respektive nach Abschluss der Beurteilung werden die Unterlagen entweder vernichtet oder in elektronischer Form auf den zugriffsgeschützten Systemen und Ablagen aufbewahrt. Während der Fallbearbeitung und soweit eine physische Aufbewahrung in Einzelfällen notwendig ist (z. B. Fotodokumentation auf CD, Röntgenbilder), werden die vertraulichen Unterlagen in abschliessbaren Schränken aufbewahrt. Für die Aufbewahrung der Schlüssel sind Schlüsselschränke mit Zugangscode montiert.

Archivierung und Aufbewahrung der Datensammlung KVG
Die Daten werden auf den Atupri-Servern bei einer Firma in der Schweiz gespeichert. Die Firma hat ihren Sitz ebenfalls in der Schweiz. Die Aufbewahrungsdauer richtet sich nach den spezifischen gesetzlichen Bestimmungen und beträgt maximal 10 Jahre (Art. 958*f* OR). Nach dem Ablauf dieser Frist werden die Personendaten in den Kernsystemen gelöscht, sofern dem kein überwiegendes Interesse von Atupri entgegensteht.

Telefonaufzeichnungen
Die Gesprächsinhalte von ein- und ausgehenden Telefonanrufen werden zur Qualitätsmessung und zu Beweiszwecken aufgezeichnet. Die Daten werden während einer Dauer von 12 Monaten aufbewahrt, sofern dem kein überwiegendes Interesse von Atupri entgegensteht.

E-Mail-Aufzeichnungen
E-Mails werden während einer Dauer von 10 Jahren aufbewahrt, sofern dem kein überwiegendes Interesse von Atupri entgegensteht. E-Mail-Korrespondenz zwischen Atupri und den KVG-Kunden wird ins Kernsystem abgelegt. Diese wird während der gesetzlich vorgesehenen Archivierungsdauer von 10 Jahren aufbewahrt.

Chat-Aufzeichnungen
Atupri stellt für den Kundenkontakt den Atupri Chat zur Verfügung. Der Kunde oder interessierte Personen können auf der Website von Atupri ihre Frage auch via Chat an den Kundendienst stellen. Die Chatnachrichten werden während einer Dauer von 10 Jahren aufbewahrt, sofern dem kein überwiegendes Interesse von Atupri entgegensteht. Die Chat-Korrespondenz zwischen Atupri und den KVG-Kunden wird ins Kernsystem abgelegt. Diese wird während der gesetzlich vorgesehenen Archivierungsdauer von 10 Jahren aufbewahrt.

7 INTERNE ORGANISATION

7.1 Geschäftsleitung

Die Verantwortung für den Datenschutz trägt die Geschäftsleitung. Diese Verantwortung ist nicht übertragbar.

7.2 Datenschutzberater

Der Leiter RCG ist Datenschutzberater gemäss Artikel 25 DSG. Er trägt die Koordinationsverantwortung für den unternehmensweiten Datenschutz.

Die Rolle des Datenschutzberaters nimmt bei Atupri wahr:

Silvio Alonso
Leiter Recht, Compliance und Generalsekretariat
Zieglerstrasse 29, Postfach
3001 Bern

silvio.alonso@atupri.ch

7.3 Risikomanagement

Risikomanagement bewertet und analysiert die Risiken im Bereich Datenschutz, namentlich gemäss den Anforderungen des BAG, des DSG und der DSV.

7.4 ICT Security Officer

Der ICT Security Officer ist zuständig für die Datensicherheit auf Stufe Unternehmen. Seine Aufgaben, Kompetenzen und Verantwortlichkeiten sind in der Weisung Cybersecurity geregelt. Der ICT Security Officer hat im Zusammenhang mit dem Datenschutz namentlich folgende Aufgaben:

- Unterstützen der Bereiche bei technischen Einschätzungen zur Datensicherheit im Rahmen der Datenschutz-Folgenabschätzungen

- Unterstützen des Datenschutzberaters und der Geschäftsleitung bei der Einschätzung von Datensicherheitsverletzungen im Hinblick auf Meldungen von Verletzungen der Datensicherheit an den EDÖB.

7.5 Datenannahmestelle

vgl. Ziff. 3.1

7.6 Datenschutzkoordinatoren

Atupri hat Datenschutzkoordinatoren in den Bereichen. Die Datenschutzkoordinatoren haben im Zusammenhang mit dem Datenschutz die Aufgabe, den Datenschutzberater bei seinen Aufgaben zu unterstützen.

7.7 Bereiche und Mitarbeitende

Atupri legt die Anforderungen an den Datenschutz in internen Vorgaben fest, schult und kontrolliert die interne Einhaltung des Datenschutzes durch die Bereiche und Mitarbeitende.

Die internen Prozessabläufe im Bereich der Bearbeitung von Personendaten werden von Atupri dokumentiert und diese Dokumentationen werden laufend geprüft und sofern notwendig aktualisiert. Die technische Dokumentation der Systemkomponenten erfolgt in entsprechenden Betriebshandbüchern. Die Planung und die Realisierung von Aktualisierungen (Lifecycle) und Weiterentwicklungen werden über das Projektmanagement geführt und dokumentiert.

8 TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN VON ATUPRI

Atupri hat technische und organisatorische Massnahmen (TOMS) umgesetzt, um die Personendaten der Atupri Kunden vor unberechtigten Zugriffen, Änderungen und Löschungen zu schützen. Insbesondere hat Atupri die von Artikel 59*a*[ter] Absatz 1 KVV geforderten TOMS implementiert.

Zugriffskontrolle/Benutzerkontrolle
Atupri verfügt über eine mehrstufige Sicherheitsinfrastruktur für den Zugriff auf Informationssysteme. Alle Mitarbeitenden verfügen über ein persönliches Log-in für die Benutzung der Systeme. Die Zugriffsrechte werden mittels rollenbasierter Zugriffsberechtigungen erteilt und in entsprechenden Berechtigungskonzepten mit Zugriffsmatrix definiert. Durch die Definition und Umsetzung der Berechtigungskonzepte wird der Zugriff auf Daten nach dem Need-to-know-Prinzip eingeschränkt. Damit wird sichergestellt, dass keine unbefugte Einsichtnahme, Veränderung oder Löschung erfolgen kann.

Zugangskontrolle
Der Zugang zu den Räumlichkeiten von Atupri ist nur mit Schlüssel oder nach Anmeldung an der Loge möglich. Besucherinnen und Besucher müssen sich beim Empfang ausweisen und registrieren. Sie werden durch Atupri Mitarbeitende am Empfang abgeholt und dürfen sich nur in Begleitung in den Gebäuden bewegen. Somit ist der direkte Zugang durch Dritte, mit Ausnahme der Schalterbereiche, nicht möglich. Ausserhalb der Arbeitszeiten werden die Räumlichkeiten von Atupri abgeschlossen. Der Zutritt zu Datenräumen beim IT-Provider ist nur berechtigten Personen möglich.

Datenträgerkontrolle/Speicherkontrolle
Die Verwendung von externen Datenträgern für die Speicherung von Daten ist untersagt und technisch eingeschränkt. Für mittels Datenträger eingelieferte Daten stehen dedizierte Geräte mit eingeschränkten Berechtigungen zur Verfügung.

Transportkontrolle
Atupri stellt organisatorisch und technisch sicher, dass Personendaten bei der elektronischen Übermittlung angemessen geschützt sind. Der physische Transport von Personendaten ausserhalb der Räumlichkeiten von Atupri ist nicht erlaubt.
Eingabekontrolle
Alle Zugriffe auf Systeme von Atupri werden nachvollziehbar protokolliert.

Bekanntgabekontrolle
Der Empfänger von Personendaten muss vor der Übermittlung manuell oder durch technische Hilfsmittel verifiziert werden.

Wiederherstellung
Sämtliche Daten werden regelmässig an mehreren Standorten gesichert. Die Wiederherstellung wird periodisch geprüft.

Verfügbarkeit, Zuverlässigkeit, Datenintegrität
Die Systeme von Atupri stellen sicher, dass die Datenintegrität jederzeit gewährleistet ist. Sie werden in georedundanten Datenzentren in der Schweiz betrieben.

9 ZUGRIFFSBERECHTIGUNGEN

Es erhalten nur jene Atupri Mitarbeitende Zugriff auf die Personendaten, die dies zur Erfüllung ihrer Aufgaben benötigen (Need-to-know-Prinzip). Damit wird verhindert, dass die Personendaten von Unberechtigten eingesehen oder verändert werden können.

Art und Umfang der Zugriffsberechtigungen
Sämtliche Anträge an die Benutzerverwaltung wie Neuanlagen, Anpassungen in den Benutzerberechtigungen oder Löschungen müssen schriftlich oder elektronisch durch autorisierte Personen genehmigt werden. Im Falle der Berechtigungsvergabe ist zu spezifizieren, welche Berechtigungen der Benutzer erhalten soll. Im Falle einer Anpassung in den Benutzerberechtigungen ist zu spezifizieren, welche Berechtigungen gelöscht werden sollen bzw. welche Berechtigungen neu vergeben werden sollen.

Personendaten und Auftragsbearbeiter
Personendaten sind für Auftragsbearbeiter eingeschränkt abrufbar. Diese Daten können nur von befugten Personen eingesehen werden. Sie sind mit einer starken Authentifizierungsmethode geschützt.

Erteilung und Aufhebung von Zugriffsberechtigungen
Die Benutzer sind nur so lange zugriffsberechtigt, als sie die Daten für die Ausübung ihrer Arbeitsfunktion benötigen. Bei Austritt sowie bei Funktionsänderungen innerhalb von Atupri werden die bisherigen Zugriffsberechtigungen entzogen und die für die neue Funktion benötigten Zugriffsberechtigungen müssen neu beantragt werden. Die Aufhebung der Zugriffe erfolgt analog der Erteilung der Zugriffsberechtigung durch die Vorgesetzten mittels eines formalisierten Prozesses.

10 MASSNAHMEN ZUR DATENMINIMIERUNG

Atupri bearbeitet nur die gemäss KVG verlangten Personendaten. Dabei achtet sie auf folgende Datenminimierungsmöglichkeiten:

- Minimierung der Personendaten durch Pseudonymisierung und Anonymisierung – anstatt die Kunden mit Namen und Vornamen zu bearbeiten, sollte lediglich die Versichertennummer verwendet werden.
- Datenminimierung durch Zugriffsbeschränkung – nur jene Mitarbeitende, die die Personendaten zur Erfüllung ihrer Aufgaben benötigen, sollen Zugriff darauf erhalten.
- Datenminimierung durch zeitliche Beschränkung – die Personendaten sollen nur bis zur Zweckerreichung oder bis maximal zur Archivierungsdauer von 10 Jahren einsehbar sein.

11 ANGABEN ZUM VERFAHREN ZUR AUSÜBUNG DES AUSKUNFTSRECHTS UND DES RECHTS AUF DATENHERAUSGABE ODER -ÜBERTRAGUNG

Die betroffenen Personen können bei Atupri das Auskunftsrecht (Art. 8 DSG), das Recht auf Löschung sowie das Recht auf Berichtigung geltend machen. Atupri kann die in Artikel 9 DSG erwähnten Einschränkungen geltend machen.

Die betroffene Person kann ihr Begehren (Art. 8 DSG) schriftlich (per Post oder als E-Mail) zusammen mit einer Kopie der ID oder des Passes an folgende Adresse senden:

Atupri Gesundheitsversicherung AG, RCG,
Zieglerstrasse 29, Postfach, 3001 Bern
rcg@atupri.ch

Atupri beantwortet ein Betroffenenrecht innert 30 Tagen. Atupri sendet der betroffenen Person ein Antwortschreiben mit den verlangten Dokumenten als Beilage. Atupri kann die Person auffordern, einen Arzt zu bezeichnen, welcher die Daten von Atupri empfangen soll, der Person die Daten übergibt und erklärt.

Nach Artikel 42 Absatz 5 KVG ist der Leistungserbringer in begründeten Fällen berechtigt und auf Verlangen der versicherten Person in jedem Fall verpflichtet, medizinische Angaben nur dem Vertrauensarzt oder der Vertrauensärztin des Versicherers nach Artikel 57 KVG bekannt zu geben.

12 PUBLIKATION

Atupri aktualisiert dieses Dokument regelmässig.
Die Datenschutzerklärung ist auf der Website www.atupri.ch abrufbar.

Atupri verfügt über einen Datenschutzberater, was sie von der Pflicht zur Anmeldung der Datensammlungen beim EDÖB befreit (Art. 12*a* VDSG). Atupri erfüllt die Vorlagepflicht an den EDÖB gemäss Artikel 84*b* KVG.