Bearbeitungsreglement der KLuG Krankenversicherung

Inhalt

1 Interne Organisation

1.1 Verantwortlichkeiten

Die Gesamtverantwortung für den Datenschutz trägt das Leitungsorgan. Diese Verantwortung ist nicht übertragbar.

Für die Umsetzung des Datenschutzes im Betrieb sowie IT-Themen wie das Betriebssystem, Anwendungen, die Datenbank, das Netzwerk und die Datensicherheit. ist Yvonne Dempfle, Geschäftsführerin verantwortlich.

KLuG verfügt über einen externen Datenschutzberater (DSB). Dieser kontrolliert die Einhaltung des Datenschutzes, berät und unterstützt die KLuG Krankenversicherung bei der operativen Umsetzung des Datenschutzes im Betrieb.

KLuG ist verantwortlich für die Abwicklung der obligatorischen Krankenpflegeversicherung nach KVG und somit Inhaberin der Verzeichnisse der Bearbeitungstätigkeiten der Personendaten. Diese Verzeichnisse sind dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet.

Kontaktstelle bezüglich datenschutzrechtlicher Fragen:

Fragen in Zusammenhang mit dem Datenschutz sind an folgende Stelle zu richten:
RVK
Haldenstrasse 25
6006 Luzern
datenschutz@rvk.ch

1.2 Datenschutzpolitik resp. Datenschutzleitbild

1.2.1 Ausgangslage

Das Bundesgesetz über den Datenschutz (DSG) verfolgt das Ziel, die Persönlichkeit und die Grundrechte von Personen zu schützen, deren Daten bearbeitet werden. Als schweizweit tätige Krankenversicherung im Bereich der Kranken- und Unfallversicherung ist die KLuG Krankenversicherung auf die Bearbeitung von Personendaten angewiesen. Der rechtskonforme Umgang mit diesen Daten hat für die KLuG höchste Priorität.
Auch im Rahmen ihrer Tätigkeit als Arbeitgeberin trägt die KLuG Verantwortung für den Schutz der Integrität ihrer Mitarbeitenden. Insbesondere in administrativen Prozessen sowie bei Führungsaufgaben werden regelmässig besonders schützenswerte Personendaten bearbeitet. Datenschutzverletzungen würden das Vertrauen von Versicherten und Mitarbeitenden erheblich beeinträchtigen. Die KLuG begegnet diesem Risiko mit einer konsequent datenschutzkonformen Praxis.

Als Krankenversicherer untersteht die KLuG den einschlägigen Bestimmungen des:

- Bundesgesetzes über den allgemeinen Teil des Sozialversicherungsrechts (ATSG),
- Bundesgesetzes über die Krankenversicherung (KVG),
- Bundesgesetzes über den Datenschutz (DSG) sowie deren zugehörigen Verordnungen.

Alle Mitarbeitenden der KLuG sind verpflichtet, diese gesetzlichen Grundlagen einzuhalten.

Die KLuG verfügt über ein internes Bearbeitungsreglement, das die Organisation der Datenbearbeitung beschreibt und darlegt, wie Datensammlungen sowie automatisierte Bearbeitungsprozesse strukturiert sind. Im Rahmen ihrer Tätigkeit bearbeitet die KLuG personenbezogene und gesundheitsbezogene Daten, die gemäss Art. 5 lit. c DSG besonders schützenswert sind. Diese Daten werden ausschliesslich im Rahmen der gesetzlichen Vorgaben gespeichert, bearbeitet und – sofern notwendig – weitergegeben.

Gemäss Art. 59 KVV ist die KLuG verpflichtet, Spitalrechnungen und zugehörige Minimal Clinical Datasets (MCD), die besonders schützenswerte Daten beinhalten, über eine zertifizierte Datenannahmestelle (DAS) zu übermitteln. Die Datenannahmestelle der KLuG ist VDSZ zertifiziert. Die KLuG stellt sicher, dass alle datenschutzrechtlichen Vorgaben eingehalten und die Datenschutzsysteme laufend überprüft und verbessert werden. Die KLuG wird durch einen betrieblichen Datenschutzverantwortlichen begleitet.

Zentral ist für die KLuG das Prinzip der Verhältnismässigkeit gemäss Art. 6 Abs. 2 DSG: Es werden nur jene Daten bearbeitet, die zur Aufgabenerfüllung notwendig und rechtlich abgestützt sind. Die Daten werden nur so lange aufbewahrt, wie dies gesetzlich vorgeschrieben oder für die Zweckerfüllung erforderlich ist. Darüber hinaus trifft die KLuG alle erforderlichen technischen und organisatorischen Massnahmen zum Schutz der Daten vor unberechtigtem Zugriff, Verlust, Zerstörung oder anderweitiger Schädigung.

1.2.2 Gesetzliche Grundlagen

Die Datenbearbeitung der KLuG Krankenversicherung richtet sich nach folgenden Gesetzen und Verordnungen:

- Bundesgesetz über den allgemeinen Teil des Sozialversicherungsrechts (ATSG)
- Verordnung über den allgemeinen Teil des Sozialversicherungsrechts (ATSV)
- Bundesgesetz über die Krankenversicherung (KVG)
- Verordnung über die Krankenversicherung (KVV)
- Bundesgesetz über den Datenschutz (DSG)
- Verordnung über den Datenschutz (DSV)
- Bundesgesetz betreffend die Aufsicht über die soziale Krankenversicherung (KVAG)
- Verordnung betreffend die Aufsicht über die soziale Krankenversicherung (KVAV)
- Verordnung über die Versichertenkarte für die obligatorische Krankenversicherung (VKK)
- Verordnung des EDI über die Leistungen in der obligatorischen Krankenpflegeversicherung (KLV)

Die KLuG erhebt und bearbeitet Personendaten rechtmässig im Rahmen der Durchführung der obligatorischen Krankenpflegeversicherung gemäss KVG. Dies umfasst auch Bearbeitungen durch Vertrauensärzte sowie die Datenannahmestelle gemäss Art. 59a KVV. Daten werden ausschliesslich zweckgebunden bearbeitet, um unnötige Datenverarbeitungen zu vermeiden und das Risiko von Datenschutzverstössen zu minimieren.

1.2.3 Schutz der Persönlichkeit der Versicherten

Der Schutz der Persönlichkeit und der informationellen Selbstbestimmung der Versicherten ist ein zentrales Anliegen der KLuG. Die Einhaltung und laufende Optimierung der Datenschutz- und Informationssicherheitsvorgaben bilden dabei eine verbindliche Grundlage.

1.2.4 Umsetzung in Bezug auf den Datenschutz

Zur Gewährleistung eines hohen Datenschutzstandards trifft die KLuG folgende Massnahmen:

- **Verantwortung der Führungskräfte:** Die Führungsebene trägt die Verantwortung für die datenschutz- und sicherheitskonforme Umsetzung in ihren jeweiligen Bereichen.
- **Sensibilisierung und Schulung:** Mitarbeitende werden regelmässig zu Datenschutz und Informationssicherheit geschult und sensibilisiert.
- **Transparenz gegenüber betroffenen Personen:** Die KLuG informiert Betroffene umfassend über Art, Umfang und Zweck der Datenbearbeitung sowie über ihre Rechte. Anfragen werden zeitnah bearbeitet.
- **Organisatorische Rahmenbedingungen:** Es bestehen geeignete personelle, technische und organisatorische Voraussetzungen für eine gesetzeskonforme Datenbearbeitung.

- **Kontinuierliche Überprüfung:** Die Einhaltung der Datenschutzbestimmungen wird laufend kontrolliert – sowohl durch interne als auch durch externe Audits.
- **Datenschutzmanagementsystem (DMS):** Das DMS gewährleistet die systematische Überwachung und Dokumentation aller datenschutzrelevanten Prozesse.

1.2.5 Datensicherheit

Die KLuG setzt umfassende technische und organisatorische Massnahmen ein, um die Sicherheit der Personendaten zu gewährleisten:

- **IT-Sicherheit:** Der Einsatz aktueller Sicherheitssoftware (z. B. Virenschutz, Firewalls, etc.) verhindert unbefugten Zugriff. Mitarbeitende werden im Umgang mit IT-Risiken geschult und für Gefahren durch unsicheren E-Mail-Verkehr sensibilisiert.
- **E-Mail-Kommunikation:** Für die Kommunikation via E-Mail besteht ein Konzept und es wurden verbindliche Richtlinien verfasst. KLuG versendet besonders schützenswerte Personendaten mit HIN- Verschlüsselung und überprüft, dass die Versendung nur an berechtigte Empfänger erfolgt. Im Zweifelsfall werden Informationen per Briefpost verschickt.
- **Datensicherheitsmassnahmen:** Die implementierten technischen und organisatorischen Vorkehrungen werden regelmässig überprüft und bei Bedarf aktualisiert, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sicherzustellen.
- **Meldesystem für Datenschutzverletzungen:** Ein interner Prozess gewährleistet, dass bei Datenschutzverstössen umgehend reagiert und geeignete Massnahmen ergriffen werden.

1.3 Registrierung des Verzeichnisses der Bearbeitungstätigkeiten

Die KLuG hat ihr Verzeichnis der Bearbeitungstätigkeiten im datareg.ch des Bundes erfasst.

1.4 Dokumentierte Prozessabläufe

Alle Prozessabläufe inkl. Angaben zu Verantwortlichkeiten sind in den Handbüchern definiert und dokumentiert. Einsichtnahmen in Prozesse können bei folgender Person vereinbart werden:

KLuG Krankenversicherung
Leiterin Leistungen
Gubelstrasse 22
6300 Zug
041 724 64 00
team.klug@klug.ch

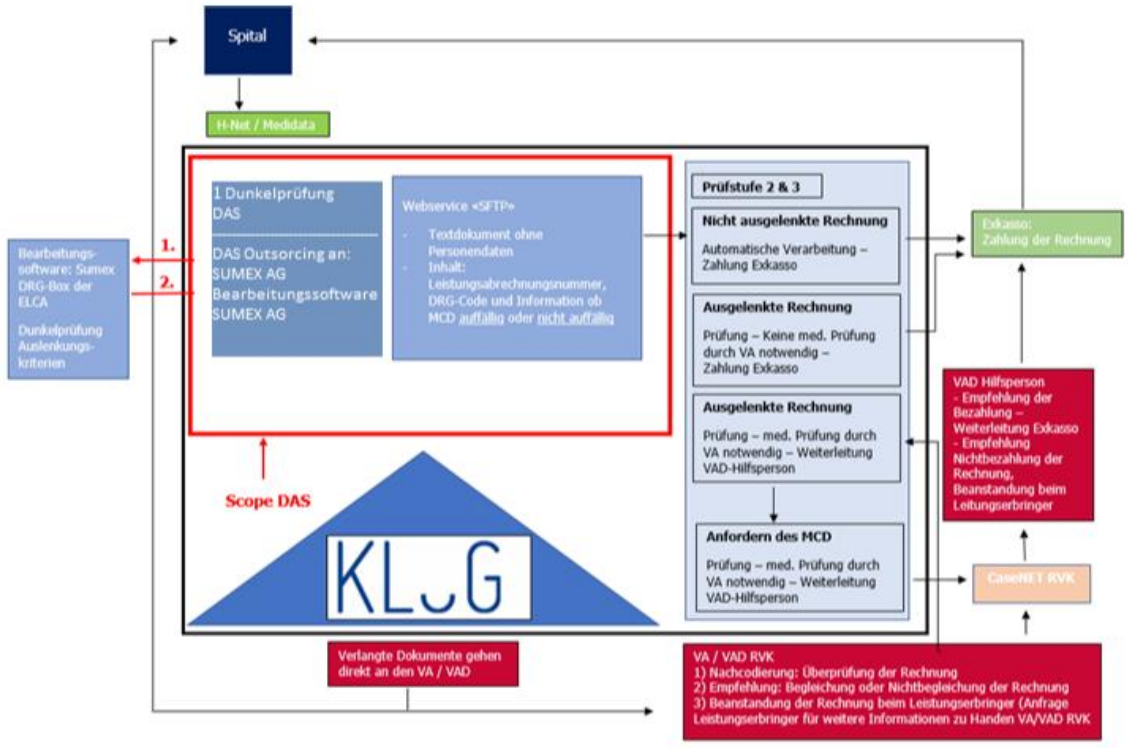
1.5 Datenfluss

Der Datenfluss wird im Konformitätsnachweis über die Felder „Herkunft" und „Empfänger" dokumentiert.

2 IT-Struktur

2.1 Struktur Datenbearbeitungssystem

Die nachfolgende Grafik zeigt die IT-Struktur auf, in welche das automatisierte Datenbearbeitungssystem eingegliedert ist.



Die Mitarbeitenden können via ihren Computer (Client) auf die Daten auf dem Server zugreifen, die sie für die Erfüllung ihrer Aufgaben brauchen. Alle Daten werden auf einem Back-up-Server sicherheitsgespeichert (dupliziert). Der Vertrauensarzt kann auf die Daten zugreifen, die er für die Erfüllung seiner Aufgabe braucht. Ausser den beiden vertrauensärztlichen Hilfspersonen können keine Mitarbeitenden der Krankenkasse auf die Daten des Vertrauensarztes zugreifen. Weder die Patienten noch die Ärzte resp. Spitäler können auf die Daten zugreifen.

2.2 Eingesetzte Informatikmittel

KLuG benutzt die Systemsoftware Siddhartha zur Verwaltung der Versichertendaten, Versicherten-betreuung und Leistungsabwicklung. Zusätzlich wird das System Therefore zur elektronischen Dokumentenarchivierung eingesetzt. Bei beiden Systemen sind Berechtigungsregeln hinterlegt, welche garantieren, dass jeder Mitarbeiter nur auf diejenigen Daten zugreift, die für die Erfüllung der Aufgaben notwendig sind.

2.3 Datenannahmestelle gemäss Art. 59a KVV

KLuG besitzt eine zertifizierte Datenannahmestelle für die Bearbeitung von elektronischen DRG-Rechnungen nach Art. 59a KVV, sowie für die Bearbeitung von DRG-Rechnungen in Papierform.

Die Geschäftsleitung der KLuG versichert, dass die Datenannahmestelle und der VA/VAD weisungsunabhängig handeln und nur die für eine weitere Prüfung notwendigen Daten an den Versicherer (KLuG) weitergeben.

Die MCD-Prüfung geschieht bei der Sumex AG, wobei die anonymisierten MCD-Daten mit der SUMEX-Dienstleistung der SUVA bei der SUVA durchgeführt wird.

Die MCD-Daten werden bei der Sumex AG verschlüsselt gespeichert. Nur der VA/VAD der KLuG kann auf diese Daten zugreifen, wenn dieser das verlangt (Art. 59a KVV).

Die versicherungstechnischen Prüfungen geschehen im System Siddhartha der KLuG. Das Regelwerk für die versicherungstechnischen Prüfungen wird nach einem vorgegebenen Prozess definiert, eingeführt, überprüft und angepasst. Die Regeländerung wird vor ihrer Umsetzung mit dem Datenschutzberater der Sumex AG auf Konformität und Machbarkeit überprüft.

DRG-Rechnungen bei denen sowohl die MCD-Prüfung (Sumex AG/SUVA) und der Prüfung auf der Basis des KLuG Regelwerks (in Siddhartha) keine weiteren Prüfungen notwendig sind, werden automatisch zur Zahlung freigegeben.

Die MCD-Daten, die nicht ausgelenkt werden, sind nicht im Zugriff der Mitarbeitenden der KLuG.

Sollte ein Leistungserbringer DRG Rechnungen in Papierform an KLuG senden, dann werden diese durch die Mitarbeitende der Datenannahmestelle (Posteingang) zurückgewiesen und nicht bearbeitet. Ein Brief mit dem Hinweis, dass der Leistungserbringer die Rechnungsstellung in elektronischer Form vornehmen soll, wird versandt, mit dem auch die Rechnungsunterlagen zurückgesendet werden. Im Normalfall erfolgt die Umstellung auf elektronische Übermittlung. Sollte der Leistungserbringer noch nicht in der Lage sein die Leistungsabrechnung elektronisch zu übermitteln – was sehr selten bis gar nicht vorkommt - dann wird diese DRG-Rechnung zur Prüfung „ausgelenkt".

Die Mitarbeitende der Datenannahmestelle (Posteingang) ist unabhängig von der Leistungsabrechnung und dem VA/VAD.

2.4 Outsourcing

Zwischen allen externen Dienstleistungsunternehmen und KLuG bestehen Zusammenarbeitsverträge. Diese Partner bestätigen mit der Vertragsunterzeichnung die Einhaltung der Datenschutzbestimmungen für sich und deren Hilfspersonen.

Für die elektronische Rechnungsprüfung vom Typus DRG (Art. 59a KVV) hat KLuG die Sumex AG als Dienstleister für die Prüfung der MCD's beauftragt. Die Sumex AG ist für diese Dienstleistung nach VDSZ zertifiziert.

Die Prüfung der anonymisierten MCD-Daten erfolgt bei der SUVA.

Dienstleister:

- **HELSANA:** Anbieter der Zusatzversicherungen von KLuG, Dienstleistungen wie Rechtsdienst, Vertrauensarzt etc.
- **RVK:** Anbieter von Zusatzversicherungen und Schnittstelle zu Verstössen im Rahmen des Hausarztsystems DOCMED, Medcase Pool
- **SUMEX**: Betreibt die Software Siddhartha und ist Provider der elektronischen Datenannahmestelle.
- **CENT**: Wandelt TARMED und LABOR-Rechnungen in elektronische XML-Files (4.4) um. Übermittelt die Daten an SECON.
- **SSS (Schaden Service Schweiz)**: Prüft die Unfall-Anzeigen auf Regressmöglichkeit.
- **CANON**: Betreiber der Software Therefore welche zur elektronischen Dokumentenarchivierung eingesetzt wird.
- **Corebit**: Externer IT-Dienstleister von KLuG
- **SVK**: Spitalrechnungen in den Bereichen Dialyse und Transplantation

Die nachfolgende grafische Übersicht zeigt die Partner der Dienstleistungen:

3 Zugriffe

3.1 Zugriffsdifferenzierung

Es werden nur die notwendigsten Zugriffsrechte auf Netzwerke, Programme und Daten an Benutzer vergeben. Jeder Mitarbeitende erhält nur Zugriff auf genau diejenigen Daten, die er zur Erfüllung seiner Aufgabe unbedingt braucht.

Die Geschäftsführerin entscheidet über die Vergabe und den Umfang der Zugriffsrechte. Sie entscheidet anhand der in der Weisung bezüglich Vergabe und Umfang der Zugriffsrechte definierten Regeln. Die Zugriffrechte sind auf die Funktion und Tätigkeitsfelder jeder Person zugeschnitten. Des Weiteren wird für jede Berechtigung entscheiden, ob eine Leseberechtigung genügt, oder Änderungsberechtigungen vergeben werden müssen.

Die Zugriffsrechte sind im Detail in der Zugriffsliste pro Mitarbeitenden festgehalten. Die Liste wird regelmässig durch das Management überprüft.

3.2 Authentisierung durch Passwörter

Der Mitarbeitende hat eine persönliche Identifikation (Benutzername) und ein Passwort. Die Weitergabe des persönlichen Passworts ist untersagt.

Die Weisung bezüglich der Zusammensetzung der Passwörter (Anzahl Stellen, Sonderzeichen etc.) liegt schriftlich vor und ist allen Mitarbeitenden bekannt.

4 Datensicherheit

Für die Gewährleistung der Datensicherheit, d.h. dem Schutz von Daten während der Datenverarbeitung, -speicherung oder -transport vor Verlust, Zerstörung, Verfälschung, unbefugter Kenntnisnahme und unberechtigter Verarbeitung, werden folgende Massnahmen angewendet:

4.1 Organisatorische Massnahmen

- Erstellung von Sicherheitskopien auf einem separaten Speichermedium.
- Getrennte Aufbewahrung der Sicherheitskopien.
- Alle Computer sind passwortgeschützt.
- Das Kennwort darf nicht den Kontonamen des Benutzers oder mehr als zwei Zeichen enthalten, die nacheinander im vollständigen Namen des Benutzers vorkommen. Es muss mindestens 8 Zeichen lang sein und Zeichen aus drei der folgenden Kategorien enthalten:
  - Großbuchstaben (A bis Z)
  - Kleinbuchstaben (a bis z)
  - Zahlen zur Basis 10 (0 bis 9)
  - nicht alphabetische Zeichen (zum Beispiel !, $, #, %)
- Automatische Bildschirmsperrung nach 15 Minuten ohne Aktivität.
- Alle Mitarbeitenden werden jährlich auf die Themen Datenschutz und Datensicherheit geschult.
- Die Mitarbeitenden der IT bilden sich regelmässig in Security Themen weiter.

4.2 Technische Massnahmen

- Es besteht ein Back-up-Konzept.
- Eine Firewall ist eingerichtet und wird regelmässig aktualisiert.
- Virenprüfung: die IT-Abteilung ist verantwortlich, dass alle Computer immer über den aktuellen Virenschutz verfügen.
- Zutrittskontrollen zum Serverraum und Dokumentation der Zutritte.

5 Interne und externe Kontrollen

In Ergänzung zu Kapitel 4 „Datensicherheit" sind folgende Massnahmen und Kontrollen im Unternehmen implementiert:
Die Einhaltung der datenschutzrechtlichen Bestimmungen wird **intern** folgendermassen sichergestellt und kontrolliert:

5.1 Massnahmen auf Unternehmungsebene

- schriftlich festgehaltene Datenschutzpolitik, die allen Mitarbeitenden bekannt ist
- Datenschutz- und Datensicherheitsrichtlinien resp. -konzept
- Regelungen von Aufgaben, Verantwortlichkeiten und Kompetenzen bezüglich Datenschutzes und Datensicherheit in den Pflichtenheften der Mitarbeitenden.
- Thematisierung des Datenschutzes und der Datensicherheit in allen Stellenbeschreibungen und Arbeitsverträgen.
- Die Zugänge zu den Büros sind gesichert.
- Jährliche Schulung aller Mitarbeitenden bezüglich Datenschutzes und Datensicherheit.
- Weisungen betreffend Umgang mit E-Mail und Telefon.
- Das System zeichnet die Zugriffe auf Daten, den Zeitpunkt sowie den Umfang der Zugriffe (lesen, verändern etc.) auf.

5.2 Kontrollen durch das Management

Das Leitungsorgan und die Geschäftsleitung nehmen ihre Führungs- und Überwachungsaufgaben durch folgende Kontrollen wahr:

- Prüfen der Bereiche der internen Kontrolle und Ableiten von Massnahmen.
- Prüfung der Umsetzung der Datenschutzpolitik.
- Sorgfältige Auswahl und Instruktion aller externer Dienstleister, die auf Daten zugreifen können oder denen Daten weitergegeben werden.
- Verfassen von Datenschutz- und Datensicherheits-Vertragsklauseln mit allen Dienstleistern, die auf Daten zugreifen können oder denen Daten weitergegeben werden sowie Kontrolle, ob die Dienstleister die Vorschriften bezüglich Datenschutzes und Datensicherheit einhalten.
- Periodische Prüfung der Zugriffsrechte sowie des Umfangs der Zugriffsrechte jedes Mitarbeitenden anhand der Zugriffsliste.
- Auswertung der Systemaufzeichnungen bezüglich Zugriffe auf Daten, Zeitpunkt sowie Umfang der Zugriffe und Abgleich mit der Zugriffsliste.

Des Weiteren lebt das Management seine Vorbildfunktion aktiv und täglich und stellt die notwendigen Mittel für die kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit bereit.

5.3 Kontrollen auf Prozessebene

- Prüfung der Konformität vor Einrichtung einer Datenbearbeitung im Verzeichnis der Bearbeitungstätigkeiten.
- Jährliche Kontrolle des Verzeichnisses der Bearbeitungstätigkeiten (Vollständigkeit, Korrektheit, ist die Datenbearbeitung immer noch zweckmässig? Ist der Empfänger der Daten noch korrekt etc.).

5.4 IT-Kontrollen

Der Grossteil der IT-Kontrollen wurde bereits unter „Datensicherheit" erläutert. Hier sind nur noch die ergänzenden aufgelistet.

- Protokollierung der Eingaben und Veränderungen
- Regelmässige IT-Audits durch externen Auditor gemäss IT-Strategie

5.5 Interne Audits

- Jährliche Kontrolle durch die Interne Revision und den Datenschutzberater

Diese Kontrollen sind in das umfassende interne Kontrollsystem des Unternehmens integriert.

6 Betroffenenbegehren

6.1 Form, Inhalt und Anschrift

Geregelt in: Art. 25 ff DSG und Art. 16 ff DSV (Auskunft), Art. 32/41 DSG und Art. DSV (Berichtigung), Art 6 Abs. 5 DSG, Art. 32 Abs. 2 lit. c und Abs. 4 DSG, Art. 4 Abs. 1, 3 und 4 DSV (Löschung), Art. 28 DSG, Art. 20 DSV (Recht auf Datenherausgabe und -übertragung).

Betroffenenbegehren sind schriftlich zusammen mit einer Kopie der ID oder des Passes an folgende Adresse und Kontaktperson zu senden:

RVK
Haldenstrasse 25
6006 Luzern
041 417 05 50
datenschutz@rvk.ch

6.2 Auskunftsbegehren über die Gesundheit

Daten über die Gesundheit des Gesuchstellers werden an einen vom Gesuchsteller bestimmten Arzt übermittelt, nicht an den Gesuchsteller persönlich.

6.3 Prozessablauf

Der interne Prozessablauf ist in Prozess-Dokumentation detailliert geregelt.

7 Archivierung und Vernichtung

Archivierungspflichtige Dokumente werden während der gesetzlich verlangten Dauer archiviert und vor Veränderungen oder unbefugten Zugriffen geschützt.

Die Zutritte zum Archiv werden sehr restriktiv vergeben und protokolliert. Die Protokolle werden aufbewahrt.

Nach Ablauf der gesetzlichen Archivierungsfrist werden die Dokumente vernichtet, da die rechtliche Grundlage (Zweckmässigkeit) wegfällt.

Der Ablauf der Aufbewahrung, Archivierung und Vernichtung ist im Konzept: *Datenaufbewahrungs- und -löschung sowie Archivierung* festgehalten.

Die Aufbewahrungsdauer für jede Datensammlung ist im Anhang 1 des Konzeptes *Datenaufbewahrungs- und -löschung sowie Archivierung* festgehalten.

8 Verfahren, wenn eine betroffene Person die Bekanntgabe oder Bearbeitung ihrer Daten verbietet,

Die betroffene Person kann die Bekanntgabe oder die Bearbeitung ihrer Daten verbieten.
Beide Begehren sind an folgende Kontaktperson zu richten:

KLuG Krankenversicherung
Leiterin Leistungen
Gubelstrasse 22
6300 Zug
041 724 64 00
team.klug@klug.ch

Diese Person resp. sein Stellvertreter trägt die Verantwortung für eine termingetreue Bearbeitung des Antrags. Diese Person resp. sein Stellvertreter trägt die Verantwortung für eine termingetreue Bearbeitung des Antrags.

Die internen Prozessabläufe sind in den Prozess-Dokumentationen in Prozessdokumentationen geregelt.