SLKK

vernünftig versichert: die
ehemalige Schweizerische
Lehrerkrankenkasse

Bearbeitungsreglement zur Sicherstellung des Datenschutzes

2023

KRANKENKASSE SLKK

Dokumentenstatus

Dokumententyp:	Reglement
Klassifizierung:	Public
Editor:	Datenschutzberaterin
Editiert am:	09.08.2023
Prüfer:	Geschäftsleitung
Freigegeben am:	25.08.2023
Version:	1.3
Status:	publiziert

Dokumentenhistorie

Version	Datum	Autor	Änderung	Begründung	Seite
1.0	2013	stm	Initialisierung		
1.1	10.10.2016	stm	Aktualisierung	Prozesse, Organigramm, Partner haben geändert	div.
1.2	10.10.2021	stm	Aktualisierung und Ergänzungen	Zertifizierung Oktober 2021	div.
1.3	09.08.2023	zay	Ergänzungen	Anpassung gemäss revDSG (Stand am 1. September 2023)	div.

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

1.1 Rechtliche Grundlage

Gestützt auf Art. 6 der Verordnung über den Datenschutz (DSV) i. V. m. Artikel 84b des Bundesgesetzes über die Krankenversicherung (KVG) hat die KRANKENKASSE SLKK (SLKK) für die Bearbeitung von Personendaten natürlicher Personen das vorliegende Bearbeitungsreglement (Reglement) erstellt.

1.2 Ziel des Bearbeitungsreglements

Das Bearbeitungsreglement umschreibt insbesondere die Datenbearbeitungs- und Kontrollverfahren der Personendaten bei der SLKK. Das Reglement enthält Angaben über die für den Datenschutz und die Datensicherheit verantwortlichen Organe, über die Herkunft der Daten und die Zwecke, für welche sie regelmässig bekannt gegeben werden. Im Weiteren beschreibt es das Verfahren für die Erteilung der Zugriffsberechtigungen auf die entsprechenden Informationssysteme und Datensammlungen.

1.3 Zweck der Datenbearbeitung

Der Zweck der Datenbearbeitung ist im Bundesgesetz über die Krankenversicherung (KVG) und in der Verordnung zum Bundesgesetz über die Krankenversicherung (KVV) geregelt. Die mit der Durchführung der Kontrolle oder der Beaufsichtigung der Durchführung des Gesetzes beauftragten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten (Art. 84 KVG + Art. 5 lit. c DSG), zu bearbeiten, um die ihren nach dem Gesetz übertragenen Aufgaben zu erfüllen.

Die Personendaten, die die SLKK im Rahmen der Durchführung der Kranken- und Unfallversicherung im Bereich der obligatorischen Krankenpflegeversicherung nach dem Bundesgesetz über die Krankenversicherung (KVG) einschliesslich der Datenbearbeitungen durch den Vertrauensarzt und die Datenannahmestelle (Art. 59a KVV) rechtmässig bekommt, werden mit dem Zweck der Durchführung der Kranken- und Unfallversicherung im Bereich der obligatorischen Krankenpflegeversicherung erhoben und bearbeitet.

Zur Bearbeitung von Daten zählt jeder Umgang mit Personendaten, z. B. die Beschaffung, Speicherung, Nutzung, Bekanntgabe, Veränderung, Archivierung oder Löschung von Daten. Die Bearbeitung der Personendaten durch die SLKK beruht auf den Grundsätzen von Treu und Glauben, der Rechtmässigkeit, der Verhältnismässigkeit, der Transparenz, der Zweckbindung, der Datenrichtigkeit und der Datensicherheit.

1.4 Personendaten

Alle Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Keine Personendaten sind anonymisierte oder aggregierte Daten, welche nicht mehr zur Identifizierung einer bestimmten Person verwendet werden können.

1.5 Verantwortliche Stelle der Datenbearbeitung

Die SLKK ist verantwortlich für die Abwicklung der obligatorischen Krankenpflegeversicherung nach KVG und somit Inhaberin der Verzeichnisse der Bearbeitungstätigkeiten der Personendaten. Mit den in diesem Reglement vorgesehenen Massnahmen sorgt die SLKK für die Einhaltung der gesetzlichen Vorschriften.

Die Datenbearbeitungen der SLKK sind in folgenden Hauptaktivitäten aufgegliedert:

- Datenannahmestelle
- Abwicklung des Krankenversicherungsvertrages
- Vertrauensärztlicher Dienst

Bei direkter Abrechnung mit dem Leistungserbringer nutzt die SLKK verschiedene Schnittstellen.

1.6 Richtlinien Datenschutz- und Datensicherheit

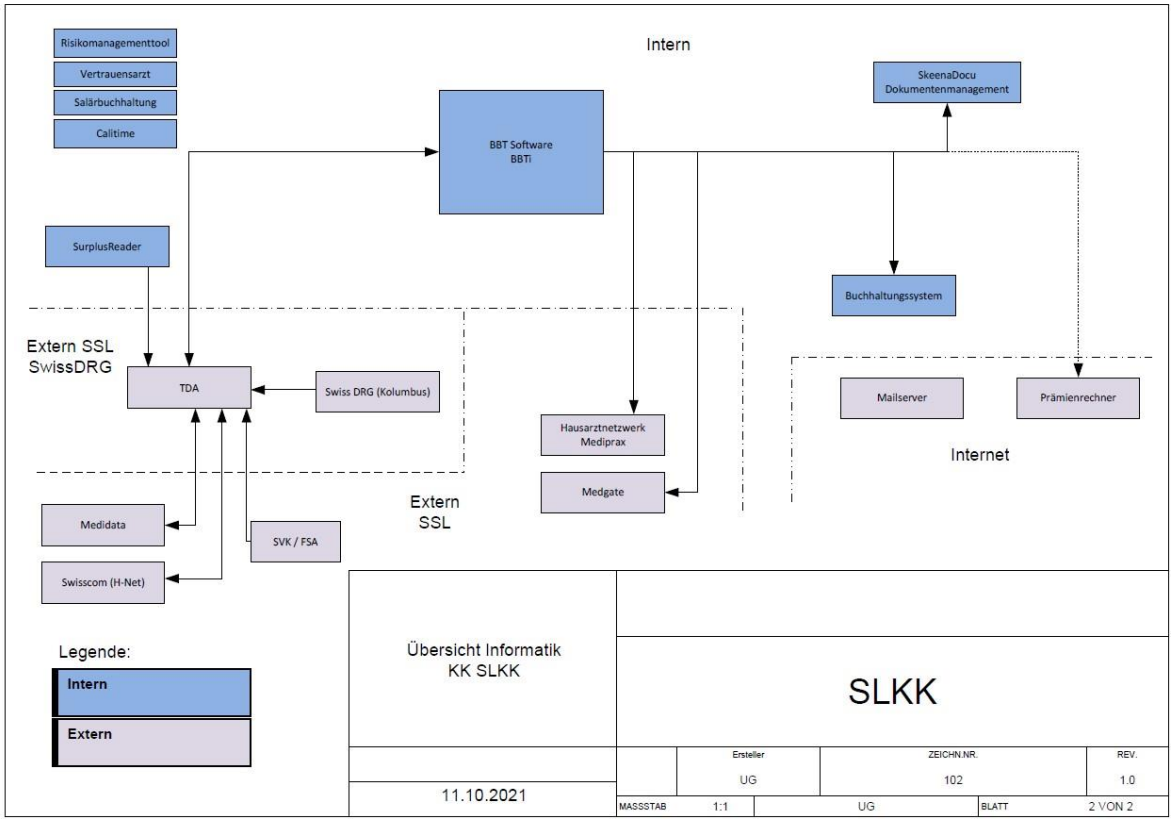
Die Richtlinien Datenschutz und Datensicherheit (Richtlinien) bzw. die entsprechende Datenschutz- und Datensicherheitsverpflichtung werden bei Stellenantritt durch die Mitarbeitenden unterzeichnet und sind Bestandteil des Arbeitsvertrages. Anlässlich von periodischen Schulungen werden die Mitarbeitenden über die Entwicklung im Datenschutzbereich informiert und sensibilisiert. Die Mitarbeitenden sind in ihrer Funktion für die Schaffung der notwendigen und angemessenen Rahmenbedingungen für den Datenschutz und die Datensicherheit verantwortlich.

1.7 Schweigepflicht nach Art. 33 ATSG

Sämtliche Mitarbeitende unterstehen während und über das Arbeitsverhältnis hinaus der Schweigepflicht nach Art. 33 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG). Die Schweigepflicht bildet Bestandteil der unter Ziff. 1.6. erwähnten Richtlinien. Bei Verletzung der Schweigepflicht gelten die strafrechtlichen Bestimmungen von Art. 92 KVG.

2 Eingesetzte Informatik-Infrastruktur

2.1 Übersicht



2.2 Kernsystem

SLKK arbeitet mit der ERP-Lösung BBTindividual (BBTi), welche Inhouse gewartet und betrieben wird. In diesem System werden folgende versicherungsrelevanten Daten bearbeitet:

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

2.3 Schnittstellen

- Leistungserbringer

Leistungserbringern haben keinen Zugriff auf den Server oder auf andere Systeme der SLKK. Die Deckungsabfrage mittels Versichertenkarte findet beim Veka-Center (Sasis AG) über eine zertifizierte Schnittstelle statt.

- Hausarztnetzwerk Arztmap

Die SLKK erhält vom jeweiligen Netzwerk der MCO-Ärzte diejenigen Personendaten, die sie benötigt, um die ihm nach dem Bundesgesetz über die Krankenversicherung übertragenen Aufgaben zu erfüllen, insbesondere um die korrekte Abwicklung der SLKK-HomeCare-Versicherung zu gewährleisten. Zwischen den Partnern, der SLKK und den verschiedenen Ärztenetzwerken bestehen Verträge, welche die Datenübermittlung regeln. Die SLKK übermittelt dem Hausarztnetzwerk über HIN verschlüsselte E-Mails regelmässig Listen mit den SLKK-HomeCare-Versicherten sowie die Versichertenangaben der versicherten Kunden.

- Medgate

Im Zusammenhang mit den alternativen Versicherungsmodellen SLKK-TelCare und SLKK-SmartMed arbeiten wir mit Medgate, dem Zentrum für Telemedizin, zusammen. Medgate hat keinen Zugriff auf unsere Systeme, bekommt aber die versicherungstechnisch notwendigen Daten von der SLKK über eine sichere Linie (SFTP) geliefert. Die Daten benötigt Medgate um mit den Versicherten, welche Kontakt zu Medgate aufnehmen, zu kommunizieren und sie gemäss Versicherungsdeckung zu beraten.

- Swiss DRG Control GmbH

Elektronische Rechnungen des Typs SwissDRG- und TarPsy-Rechnungen werden durch die zertifizierte Datenannahmestelle der SLKK empfangen und geprüft. Die Datenannahmestelle für elektronische SwissDRG-Rechnungen und Tarpsy-Rechungen wird von der Swiss DRG Control GmbH betrieben. Diese prüft die Daten für die stationären Behandlungen, welche in einem Spital, in einer psychiatrischen Institution oder in einer Reha-Klinik erbracht wurden gemäss den Prozessen in Ziff. 6. Die SLKK hat die Datenannahmestelle der SwissDRG Control GmbH dem EDÖB gemeldet und sie ist im Verzeichnis des EDÖB bei der SLKK mit aufgeführt.

Schw. Verband für Gemeinschaftsaufgaben der Krankenversicherer SVK / FSA SLKK hat die vertrauensärztlichen Leistungen betreffend spezieller Medikamente, Transplantationen, Dialyse, künstliche Ernährung zu Hause und mechanische Heimventilation inkl. Beurteilungen und Abklärungen an den SVK ausgelagert. Die zertifizierte Datenannahmestelle des SVK/FSA prüft im Auftrag der SLKK die SwissDRG-Rechnungen, welche Transplantationen und Dialysen betreffen und leitet diese visiert an die SLKK zur abschliessenden Bearbeitung und Bezahlung weiter. Die SLKK hat die SVK Datenannahmestelle für Spezialaufgaben (Bereiche, Transplantationen und Dialyse) dem EDÖB gemeldet und sie ist im Verzeichnis des EDÖB bei der SLKK mit aufgeführt.

- Vertrauensarzt

Die SLKK hat vertragliche Vereinbarungen mit externen Vertrauensärzten und Vertrauenszahnärzten. Der Vertrauensarzt hat über einen SSL-Tunnel Zugriff auf einen dezidierten Terminalserver. Dort sind jedoch nur diejenigen Daten abgelegt, welche der VA für

die Beurteilung eines Falles benötigt. Diese Daten werden dort nicht gespeichert. Auf alle anderen Daten oder Systeme hat er keinen Zugriff.
Der Vertrauenszahnarzt hat keinen Zugriff auf die Daten und Systeme der SLKK. Anfragen zu Abklärungen werden schriftlich gestellt und mit der Post versandt.
Der vertrauensärztliche Dienst VAD arbeitet im Haus und ist räumlich und technisch von den anderen Organisationseinheiten abgegrenzt.

- Medicall

Medicall hilft unseren Versicherten im Notfall im Ausland weiter. Sämtliche Anfragen von Medicall an die SLKK und unsere Rückmeldungen zur Versicherungsdeckung einzelner Personen werden verschlüsselt über E-Mail versandt. Medicall hat keinen Zugriff auf unser Daten und Systeme.

- BBT Software AG

Die BBT Software AG ist der Hersteller des Kernsystems BBTi. Der Support von BBTi hat keinen Zugriff auf das ERP-System. Systemfehler werden auf einer externen Testdatenbank in einer völlig unabhängigen Umgebung durch die Mitarbeitenden von BBTi eruiert und behoben. Updates und Fehlerbehebungen werden über Releases und Hotfixes gelöst. Der Systemadministrator der SLKK importiert die Datenbank vor Ort.
Mit Authentifizierung, Verschlüsselungs- und modernen Übertragungstechnologien werden in Bezug auf diese und allfällige weitere Schnittstellen der Datenschutz und die Datensicherheit gewährleistet.

- Mitarbeitende

Die Mitarbeitenden der SLKK können via ihren Computer (Client) auf die Daten auf dem Applikations- und auf den Dateiserver zugreifen, die sie für die Erbringung ihrer Aufgaben brauchen. Alle Daten werden auf einem Backup-Server sicherheitsgespeichert (dupliziert). Lediglich die IT-Abteilung kann auf die Backups zugreifen. Alle Clients sowie die Drucker sind ans Netz angeschlossen. Die User haben nicht auf alle Laufwerke und Ordner Zugriff.
Die Zugriffsberechtigungen werden gemäss unserer Security verteilt.
Sofern die Mitarbeitenden der SLKK ausserhalb der Räumlichkeiten der SLKK arbeiten, gelten die Bestimmungen der Richtlinie Telearbeit, um die Vertraulichkeit sowie den Datenschutz sicherzustellen.

2.4 Outsourcing

Zwischen allen Partnern und der SLKK bestehen Zusammenarbeitsverträge und Datenschutzvereinbarungen. Mit Vertragsunterzeichnung wird die Einhaltung des Datenschutzes bestätigt.

3 Organisation

3.1 Geschäftsstellen, Filialen

Die SLKK betreut Versicherte in der deutschsprachigen Schweiz in der obligatorischen Krankenpflegeversicherung. Die SLKK hat weder Geschäftsstellen noch Filialen. Der Hauptsitz befindet sich in 8050 Zürich.

3.2 Organisationsstruktur

Die Genossenschaft KRANKENKASSE SLKK ist eine Genossenschaft mit Sitz in Zürich. Der Vorstand besteht aus vier Personen.
Die interne und externe Revision sowie der Compliance Officer sind dem Vorstand direkt unterstellt. Die Geschäftsleitung besteht aus drei Personen und ist für die operative Geschäftsführung zuständig. Die SLKK beschäftigt 22 Mitarbeitende.

Die SLKK ist in folgende Bereiche aufgeteilt

- Vertrieb
- Leistungsabteilung (ambulant und stationär)
- vertrauensärztlicher / vertrauenszahnärztlicher Dienst
- zertifizierte Datenannahmestelle
- Finanzen
- Informatik
- Dienste
- Compliance / Risikomanagement und Datenschutz

3.3 Verantwortlichkeiten

Die Gesamtverantwortung für den Datenschutz tragen der Vorstand und die Geschäftsleitung. Diese Aufgabe und Verantwortung ist nicht übertragbar.
Alle weiteren Aufgaben, Kompetenzen und Verantwortlichkeiten betreffend Datenschutz und Sicherheit sind in den entsprechenden Stellenbeschreibungen festgehalten. Der Datenschutzberatende berät das Unternehmen in der Umsetzung und Einhaltung des Datenschutzes und nimmt die entsprechenden Kontrollen vor. Er trägt jedoch nicht die Verantwortung für die Einhaltung der Bestimmungen des Datenschutzes, diese liegt in jedem Fall beim Inhaber der Daten (SLKK), bzw. bei den entsprechenden Abteilungen.

4 Benutzer und Datenzugriff

4.1 Benutzer

Folgende Rollen sind zugriffsberechtige auf die IT-Systemen der SLKK:

- Mitarbeitende der SLKK, um die Abwicklung des Krankenversicherungsvertrages zu gewährleisten
- IT-Dienstleister (vertraglich mandatiert)

Abhängig von Funktion und Rolle, die ein Mitarbeitender wahrnimmt, wird die Zugriffsberechtigung (Einsichts- und/oder Mutationsrecht) erteilt und dokumentiert. Für Wartung und Problemlösung erhält die IT-Outsourcing-Partner Zugriff auf die betroffenen Systeme.

4.2 Benutzerverwaltung

Die Benutzerverwaltung erfolgt zentral durch den internen IT-Koordinator. Die Geschäftsleitung und die Personalabteilung sind für die Vergabe/Zuteilung der IT-Zugriffsrechte der einzelnen Mitarbeitenden zuständig. Für jeden Mitarbeitenden wird ein Zugriffsprotokoll erstellt, jährlich überprüft und im Mitarbeiterdossier aufbewahrt.

4.3 Aufhebung der Zugriffsrechte

Die Benutzer sind nur so lange und in dem Umfang zugriffsberechtigt, als sie die Daten für die Ausübung ihrer Funktion benötigen. Bei Austritt wird die Zugriffsberechtigung beendet.

4.4 Ausbildung der Benutzer

Die Benutzer werden auf BBTi resp. auf den für den Betrieb notwendigen Applikationen intern geschult.

4.5 Prozessabläufe, interne Richtlinien

Die Arbeitsprozesse werden im Intranet oder in Handbüchern abgebildet und umschrieben und sind für alle Mitarbeitende zugänglich. Die Prozesse werden von der internen Kontrollstelle und der internen Revision regelmässig auf ihre Aktualität überprüft.

5 Bearbeiten von Daten

5.1 Datenbeschaffung

Die Daten stammen in erster Linie von unseren Versicherten selbst sowie von den von Versicherten ermächtigten Personen und Stellen (Leistungserbringer, Versicherungen, Amtsstellen etc.), aus der Leistungsabwicklung von Leistungserbringern sowie von Amtsstellen (Prämienverbilligung, Sozialamt, Asylwesen).

5.2 Datenbearbeitungsverfahren

Die Datenverarbeitung (insbesondere das Speichern, Bekanntgabe an Dritte, Archivieren, Aufbewahren, Anonymisieren, Pseudonymisieren, Berichten oder Löschen) wird in diesem Reglement beschrieben.

5.3 Datenkategorien

Dazu gehören persönliche Informationen und Kontaktdaten, Antragsdaten, Finanz- und Zahlungsdaten, allfällige Schaden-, Leistungs-, Rechtsfalldaten, Gesundheitsdaten, besonders schützenswerte Personendaten.
Es werden folgende wesentliche Datenkategorien im System geführt:

- Name, Vorname
- Geburtsdatum
- AHV-Nummer
- Sozialversicherungsnummer
- Versichertennummer
- Adresse
- Nationalität
- Zahladresse
- Vertragsdaten
- Leistungsdaten
- Prämiendaten
- Mahndaten
- Vollmachten
- Unterschrifts-Berechtigungen
- Vorversicherer
- Einwilligungserklärungen

5.3 Bekanntgabe von Daten an Dritte

Eine Bekanntgabe von Daten an Dritte ist gemäss Art. 84a in Verbindung mit Art. 84 KVG nur erlaubt, wenn diese aus rechtlichen Gründen einen Anspruch auf diese Daten haben oder eine

entsprechende schriftliche Einwilligung des Betroffenen vorliegt. Nach dem Versand der Daten ist der Empfänger für den Datenschutz und die Datensicherheit verantwortlich.
Daten können insbesondere bekannt gegeben werden für die Datenbearbeitung zur

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

5.4 Weitere Datenweitergabe nach Art. 84a KVG

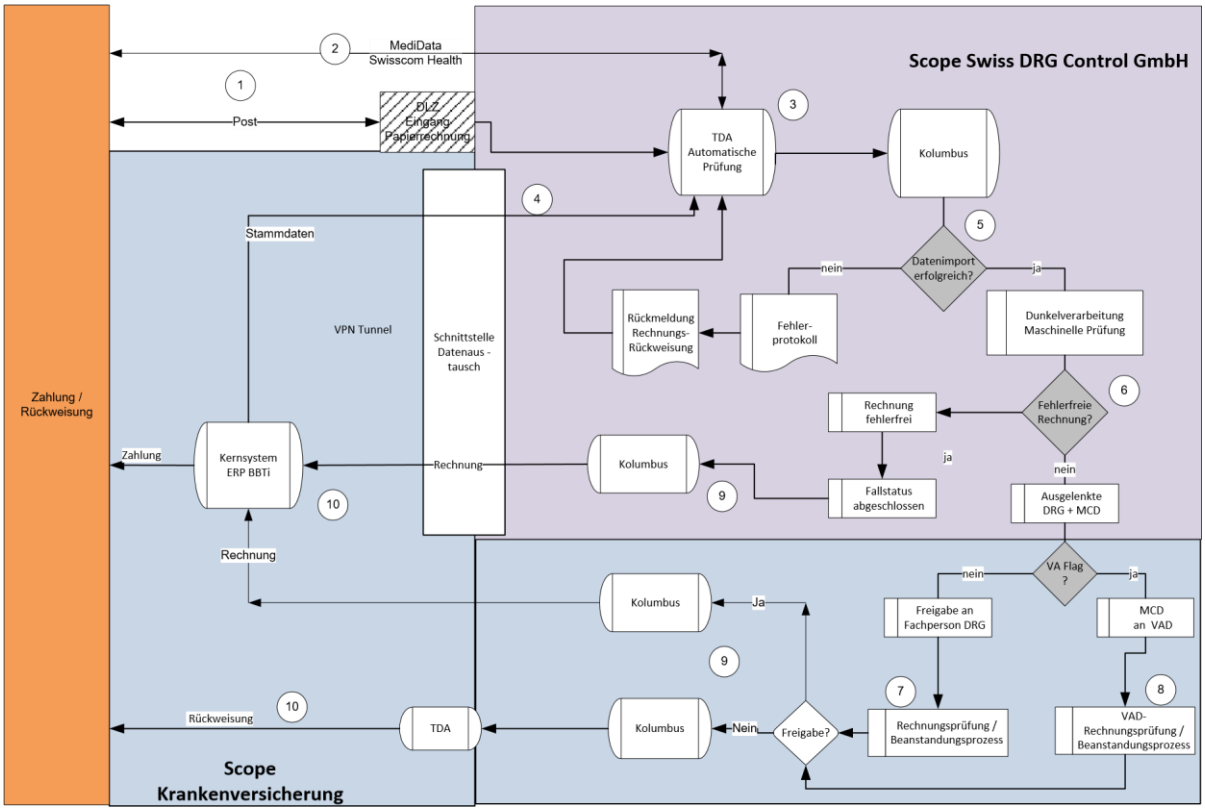
Die weitere Datenbekanntgabe ist abschliessend in Art. 84a KVG geregelt. So können im Einzelfall und auf schriftlich begründetes Gesuch hin Daten gemäss den spezifischen Anforderungen an Sozialhilfebehörden, Zivilgerichte, Strafgerichte und Strafuntersuchungsbehörden, Betreibungsämter sowie mit schriftlicher Einwilligung der betroffenen Person an Dritte weitergegeben werden.

5.5 Anmeldung der Verzeichnisse der Bearbeitungstätigkeiten beim EDÖB

Die SLKK verfügt über einen dem EDÖB gemeldeten, betrieblichen Datenschutzberatenden nach Art. 10 DSG . Die SLKK ist verpflichtet nach Art. 12 DSG ein Verzeichnis ihrer Bearbeitungstätigkeiten zu führen.

6 Datenannahmestelle

6.1 Prozessübersicht



6.2 Eingang elektronischer SwissDRG /Tarpsy-Rechnungen

Die DRG und die Tarpsy-Daten (Rechnung + MCD) werden von den Leistungserbringern elektronisch an die DAS der Swiss DRG Control GmbH übermittelt. Die elektronische Datenübermittlung zwischen den Leistungserbringern und der DAS erfolgt mittels Intermediär, namentlich Swisscom Health AG und MediData. Die Datenübermittlung erfolgt verschlüsselt mittels ssl (secure socket layer).

Durch den Eingang im Tarif and Distribution Adviser (TDA) als XML-File gelangen die DRG und Tarpsy-Rechnungen sowie das MCD in den Scope der durch die Swiss DRG Control GmbH betriebenen DAS.

6.3 Eingang physischer SwissDRG/Tarpsy-Rechnungen

Der Leistungserbringer versendet die SwissDRG- oder die Tarpsy Rechnung als Papierdokument an die SLKK. Das Couvert wird im physischen Dienstleistungscenter (DLZ) der SLKK geöffnet, als SwissDRG- oder TarPsy-Rechnung erkannt und separiert, gescannt und so in den Standard XML 4.5 überführt.

Diese Aufgaben gehören in den Scope der datenschutzzertifizierten DAS, werden jedoch nicht auf die Swiss DRG Control GmbH übertragen. Vielmehr liegt die Entgegennahme und Bearbeitung von Papierrechnungen im Aufgabenbereich der SLKK. Sobald die Rechnung als

Standard XML 4.5 im TDA empfangen wird, befinden sie sich im Scope der durch die Swiss DRG Control GmbH betriebenen DAS.

6.4 Rechnungsprüfung im TDA

Im TDA) der Swiss DRG Control GmbH werden alle XML-Files eingelesen und nach folgenden Kriterien geprüft:

- Kennt der TDA die aufgeführte Person?
- Ist der DRG-Tarife 010, 011, 012 und für Tarpsy 030 vorhanden?
- Durchführung einer Schemavalidierung gemäss elektronischem Datenaustausch.

Sind diese Voraussetzungen nicht erfüllt, geht die Rechnung über denselben Intermediär zurück, welcher die Daten eingeliefert hat. Die Daten verlassen damit wieder den Scope der datenschutzzertifizierten DAS der Swiss DRG Control GmbH. Sind die Voraussetzungen hingegen erfüllt, werden die DRG- und Tarpsy-Rechnungen Daten in das System Kolumbus überführt.

6.5 Prüfung in Kolumbus

In Kolumbus wird die SwissDRG-Rechnung bzw. die Tarpsy-Rechnung einschliesslich MCD anhand von vordefinierten Auslenkungsregeln einer Dunkelprüfung unterzogen. In Kolumbus ist ein administratives und ein medizinisches Regelwerk hinterlegt.

Sofern eine Auslenkungsregel anschlägt, werden die SwissDRG- und Tarpsy-Daten ausgelenkt, und zwar entweder an die Fachstelle DRG oder, sofern die Rechnung einen VA-Flag vorweist, an den Vertrauensarzt bzw. den Vertrauensärztlichen Dienst (VAD). Mit dieser Auslenkung verlassen die DRG- und Tarpsy-Daten den Scope der zertifizierten Datenannahmestelle der Swiss DRG Control GmbH.

Ist die Rechnung fehlerfrei, das heisst das Regelwerk schlägt nicht an und die Rechnung wird nicht ausgelenkt, dann erhält sie den Status abgeschlossen, wird freigegeben und verlässt den Scope der DAS, um im Scope der SLKK bis zum Exkasso weiter verarbeitet zu werden.
Die MCDs werden in der Datenannahmestelle in Kolumbus archiviert und dürfen nur vom Vertrauensarzt freigegeben werden.

Die Auslenkungsregeln in Kolumbus werden von der SLKK vorgegeben. Die SLKK darf der SwissDRG Control GmbH keine Weisungen bezüglich der Datenweitergabe in Bezug auf einzelne Rechnungen erteilen (Art. 59a Abs. 4 KVV).

6.6 Prüfung der ausgelenkten Rechnungen

DRG-Rechnungen und Tarpsy-Rechungen mit VA-Flag werden nur an den VA / VAD ausgelenkt. Die übrigen ausgelenkten Rechnungen werden (ohne Zugriff auf das MCD) an die Fachpersonen mit besonderen Kenntnissen ausgelenkt.

USER-ID:	Vertrauensarzt	Vertrauensärztlicher Dienst VAD	Fachperson mit besonderen Kenntnissen (ohne MA SLKK)	Fachperson mit besonderen Kenntnissen (mit MA SLKK)	Administrator SWISS DRG Control	Administrator Kolumbus
Kolumbus						
MCD mit VAD-Flag	Zugriff	Zugriff	kein Zugriff	Kein Zugriff	kein Zugriff	Zugriff
MCD ohne VAD-Flag	Zugriff	Zugriff	Zugriff	Zugriff	kein Zugriff	Zugriff
Ausgelenkte DRG Rech'g	Zugriff	Zugriff	Zugriff	Zugriff	Kein Zugriff	Zugriff
Abgeschlossene Rech'g	Zugriff	Zugriff	Kein Zugriff	Kein Zugriff	kein Zugriff	kein Zugriff
Kolumbus Einstellungen	kein Zugriff	kein Zugriff	kein Zugriff	Kein Zugriff	kein Zugriff	Zugriff
Swiss DRG Control Terminal-Server						
Systemeinstellungen	kein Zugriff	kein Zugriff	kein Zugriff	Kein Zugriff	Zugriff	kein Zugriff
Netzwerkeinstellungen	kein Zugriff	kein Zugriff	kein Zugriff	Kein Zugriff	Zugriff	kein Zugriff
RDP Swiss DRG Control Verbindung	Zugriff	Zugriff	Zugriff	Zugriff	Zugriff	Zugriff
RDP Swiss DRG Control Einstellungen	kein Zugriff	kein Zugriff	kein Zugriff	Kein Zugriff	Zugriff	Kein Zugriff
Firewall	kein Zugriff	kein Zugriff	kein Zugriff	Kein Zugriff	Zugriff	kein Zugriff
Datenbank	kein Zugriff	kein Zugriff	kein Zugriff	Kein Zugriff	Zugriff	kein Zugriff

7 Archivierung und Vernichtung

7.1 Aufbewahrungspflicht

Archivierungspflichtige Dokumente werden während der gesetzlichen verlangten Dauer archiviert und vor Veränderungen oder unbefugten Zugriffen geschützt. Für Daten der sozialen Krankenversicherung nach KVG gilt eine Aufbewahrungspflicht von zehn Jahren (Art. 958 f OR).

7.2 Vernichtung physisch vorhandener Daten

Bei der Vernichtung von vertraulichen oder besonders schützenswerter Daten in physischer Form muss der Datenschutz gewährleistet sein, d. h. die Unterlagen dürfen nicht in öffentlich zugänglichen Behältern der Vernichtung zugeführt werden. Die SLKK hat mit dieser Aufgabe eine zertifizierte Firma beauftragt.

7.3 Vernichtung elektronisch gespeicherter Daten

Elektronische Datenträger müssen vor der Vernichtung unlesbar gemacht werden oder die Vernichtung durch ein für die Entsorgung von elektronischen Datenträgern zertifiziertes Unternehmen erfolgen. Die elektronisch gespeicherten Daten werden nach Ablauf der Aufbewahrungspflicht endgültig gelöscht.

8 Technische und organisatorische Massnahmen (TOMs)

8.1 Zutrittskontrolle

Die Büroräumlichkeiten der SLKK sind ausserhalb der Öffnungszeiten mit einer Alarmanlage gesichert. Zu Räumen mit erhöhten Datensicherheitsbedürfnissen wie z. B. der Serverraum kennt nur ein beschränkter Kreis von Mitarbeitenden den Zugangscode.

8.2 Authentifizierung der Benutzer - Zugriffskontrolle

Der Zugriff auf die ERP-Lösung und auf die anderen Systeme in der SLKK ist durch die USER-ID geschützt. Das Login auf den Rechner kann nur mittels Fingerprint erfolgen. Für den Zugriff auf Umsysteme muss sich der Mitarbeitende mittels Passwort identifizieren.
Folgende Massnahmen sind darauf ausgerichtet, dass die Benutzung von automatisierten Datenbearbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen verhindert wird:

- Protokollierungen
- Anti-Viren-Software
- Anti-Spyware-Software
- Blockierung USB-Schnittstellen für Datenträger
- Regelmässige Kontrolle der Berechtigungen
- Regelmässige Kontrolle der Zugriffe / Logfiles
- Sensibilisierung des Personals
- Protokollierung durch Anti-Virenschutz Server

8.3 Zugangskontrolle

Massnahmen die unbefugten Personen den Zugang zu Räumlichkeiten und Anlagen, in denen Personendaten bearbeitet werden, verwehren. Folgende Massnahmen zur Zugangskontrolle existieren bei der SLKK:

- Automatisches Zugangskontrollsystem
- Alarmsystem
- Abschliessbare Serverschränke
- Sicherheitsschlösser
- Personenidentifikation
- Protokollierung der Zutritte
- Sorgfältige Auswahl von Personal

8.4 Verfügbarkeit und Integrität

Die SLKK ergreift die Massnahmen, die unbefugten Personen das Lesen, Kopieren, Verändern, Verschieben, Löschen oder Vernichten von Datenträger verunmöglichen. Dazu gehören auch die technischen und organisatorischen Massnahmen, die für die Speicherkontrolle, Transportkontrolle, Wiederherstellung, Systemsicherheit und Datenintegrität ergriffen werden.
Folgende Massnahmen zur Verfügbarkeit und Integrität existieren bei der SLKK (nicht abschliessend):

- Serverraum mit Eintrittspasswort
- Protokollierungen
- Zugriffsberechtigungen für Daten, Anwendungen, Betriebssysteme
- Verschlüsselung von Datenträgern
- Dokumentation der regelmässigen Abruf- und Übermittlungsvorgängen
- Schutz gegen Feuer, Rauch, Überflutungen, Feuchtigkeit, usw.
- Software- und Anwendungs-Updates
- Sicherheitsaktualisierungen
- Behebung von Schwachstellen

8.5 Zusammenarbeit mit Partnern

Der Datenaustausch von besonders schützenswerten Daten mit unseren externen Partnern erfolgt in einem geschützten Bereich.

8.6 Weitere Massnahmen

Sowohl die Firewall als auch das Antivirus-Programm werden regelmässig automatisch aktualisiert. Die IT wird jährlich durch die externe Revision einer Prüfung unterzogen.

9 Rechte der Versicherten

9.1 Informationspflicht beim Beschaffen von Personendaten

Art. 19 DSG verlangt die Information der betroffenen Person über jede Beschaffung von Personendaten. Aufgrund des gesetzlichen Auftrages nach KVG zur Bearbeitung von aller Art der Personendaten gilt die Ausnahmeregelung nach Art. 20 Abs. 1 lit. b DSG, wonach die Informationspflicht des Inhabers des Verantwortlichen entfällt, wenn die Bearbeitung ausdrücklich durch das Gesetz vorgesehen ist.

9.2 Auskunftsrecht nach Art. 25 DSG

Jede Person kann von der SLKK schriftlich Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Das Auskunftsrecht richtet sich nach Art. 25ff DSG sowie Art. 9 und 17 DSV.
Die Auskunftsgesuche sind unter Beilage einer amtlichen Ausweiskopie an die KRANKENKASSE SLKK, zu Handen des Datenschutzberatenden, Hofwiesenstrasse 370, 8050 Zürich zu richten.

9.2 Datenherausgabe- oder Datenübertragungsrecht nach Art. 28 DSG

Jede Person kann von der SLKK die Herausgabe ihrer Personendaten, die sie ihm bekanntgegeben hat, in einem gängigen elektronischen Format schriftlich verlangen Das Recht auf Datenherausgabe oder –übertragung richtet sich nach Art. 28 und 29 DSG sowie Art. 9. Art. 21 und 22 DSV.

9.3 Berichtigungs- und Löschungsrechte

Die betroffenen Personen können gemäss Art. 41 und Art. 32 Abs. 4 DSG verlangen, dass ihre Daten berichtigt, vernichtet, bearbeitet oder die Bekanntgabe an Dritte gesperrt werden. Die entsprechenden Gesuche sind an die KRANKENKASSE SLKK, zu Handen des Datenschutzberatenden, Hofwiesenstrasse 370, 8050 Zürich zu richten.

10 Abschliessende Bestimmungen

10.1 Änderung des Reglements

Das Bearbeitungsreglement wird in Ergänzung zu den Richtlinien Datensicherheit bei Bedarf aktualisiert. Dieses Reglement kann jederzeit geändert werden. Änderungen bedürfen der Schriftform und der Zustimmung der Geschäftsleitung. Die Verantwortung für die Aktualisierung trägt der Datenschutzberatende der SLKK. Die aktualisierte Version dieses Reglements wird dem EDÖB gemäss Art. 84b KVG zugestellt.

10.2 Inkrafttreten

Dieses Reglement wurde von der Geschäftsleitung genehmigt und ist per 1. September 2023 gültig. Es ersetzt das Bearbeitungsreglement Ausgabe 2021.

KRANKENKASSE SLKK

Roland Kleiner	Yanina Zawisla
Direktor	Datenschutzberaterin

Glossar

ATSG	Bundesgesetz über den Allgemeiner Teil des Sozialversicherungsrechts
BAG	Bundesamt für Sozialversicherungen
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
KVG	Bundesgesetz über die Krankenversicherung
VVG	Bundesgesetz über den Versicherungsvertrag
DSG	Bundesgesetz über den Datenschutz
VDSG	Verordnung zum Bundesgesetz über den Datenschutz
BAG	Bundesamt für Gesundheit
IV	Invalidenversicherung
AHV	Alters- und Hinterlassenenversicherung
Santésuisse	Branchenverband der Krankenversicherer
Sasis AG	Aktiengesellschaft für die Versichertenkarten (Veka)
Medgate	Schweizer Zentrum für Telemedizin
Medicall	Notruf- und Dienstleistungszentrale
SVK	Dienstleistungsbetrieb für angeschlossene Versicherer