SLKK

vernünftig versichert: die ehemalige Schweizerische Lehrerkrankenkasse

Bearbeitungsreglement zur Sicherstellung des Datenschutzes 2025

KRANKENKASSE SLKK

Dokumentenstatus

Dokumententyp:	Reglement
Klassifizierung:	Public
Editor:	Datenschutzberaterin
Editiert am:	26.02.2025
Prüfer:	Geschäftsleitung
Freigegeben am:	27.03.2025
Version:	2.0
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.
1.4	11.10.2024	zay	Aktualisierung	ERP- und Datenannahmestellewechsel per 01.01.2025	div.
2.0	26.02.2025	zay	Überarbeitung	ERP- und Datenannahmestellewechsel per 01.01.2025	div.

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

1.1 Rechtliche Grundlage

Gemäss Art. 6 der Verordnung über den Datenschutz (DSV) in Verbindung mit Art. 84b des Bundesgesetzes über die Krankenversicherung (KVG) hat die KRANKENKASSE SLKK (SLKK) dieses Bearbeitungsreglement erstellt.

1.2 Zweck des Bearbeitungsreglements

Dieses Reglement definiert die Datenbearbeitungs- und Kontrollverfahren der KRANKENKASSE SLKK. Es enthält Informationen über die verantwortlichen Organe für Datenschutz und Datensicherheit, die Herkunft der Daten, das Verfahren zur Erteilung von Zugriffsberechtigungen auf Informationssysteme und Datensammlungen. Das Reglement beschreibt auch den Zweck der Datenbekanntgabe und die Empfänger.

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 Bearbeitung von Personendaten erfolgt gemäss den Bestimmungen des KVG und der dazugehörigen Verordnung (KVV). Die KRANKENKASSE SLKK bearbeitet Personendaten, einschliesslich besonders schützenswerter Daten, zur Erfüllung ihrer gesetzlichen Aufgaben im Rahmen der Kranken- und Unfallversicherung.

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

Personendaten sind alle Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Anonymisierte oder aggregierte Daten, die nicht zur Identifizierung einer Person verwendet werden können, gelten nicht als Personendaten.

1.5 Verantwortliche Stelle der Datenbearbeitung

Die KRANKENKASSE SLKK 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.

Die Datenbearbeitungen der SLKK sind in folgenden Hauptaktivitäten aufgegliedert:

- Datenannahmestelle
- Abwicklung des Krankenversicherungsvertrages
- Vertrauensärztlicher Dienst
- Rekrutierung

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

1.6 Richtlinien Datenschutz- und Datensicherheit

Die Krankenkasse SLKK ist verantwortlich für die Schaffung und Aufrechterhaltung angemessener Rahmenbedingungen für Datenschutz und Datensicherheit. In ihrer Datenschutzpolitik verpflichtet sie sich zur Einhaltung aller geltenden Datenschutzvorschriften sowie branchenspezifischer Bestimmungen. Zudem setzt sich die SLKK aktiv für eine kontinuierliche Verbesserung und Wirksamkeit des Datenschutzes ein.

Die Krankenkasse SLKK stellt intern Weisungen und Richtlinien zu Datenschutz und Datensicherheit bereit. Diese sind fester Bestandteil des Arbeitsvertrags und werden von den Mitarbeitenden bei Stellenantritt unterzeichnet. Regelmässige Schulungen gewährleisten, dass alle Mitarbeitenden über aktuelle Entwicklungen im Datenschutz informiert und dafür sensibilisiert werden.

1.7 Schweigepflicht nach Art. 33 ATSG

Alle Mitarbeitenden unterliegen während und nach dem Arbeitsverhältnis der Schweigepflicht gemäss Art. 33 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG). Bei Verletzung der Schweigepflicht gelten die strafrechtlichen Bestimmungen von Art. 92 KVG.

1.8 Scope und Geltungsbereich

Dieses Bearbeitungsreglement umfasst die Tätigkeit der Datenannahmestelle (DAS) der KRANKENKASSE SLKK, welche von der SUMEX AG zur Verfügung gestellt wird. Die SUMEX AG ist für die DAS zuständig; die KRANKENKASSE SL bleibt jedoch verantwortlich. Die SUMEX AG ist VDSZ:2023 zertifiziert.

Der Geltungsbereich umfasst folgende Bereiche und Schnittstellen:

- Eingehende elektronische Post und deren Bearbeitung über Schnittstellen zur KRANKENKASSE SL.
- Empfang von Rechnungen, medizinischen Codierdaten (MCD) und weiteren Dokumenten direkt von Leistungserbringern an die DAS der SUMEX AG.
- Bearbeitung von Papierrechnungen durch die KRANKENKASSE SLKK, sofern solche noch eingehen. Mit der Systemumstellung werden Rechnungen, sofern seitens des Leistungserbringers möglich, nur noch elektronisch empfangen.

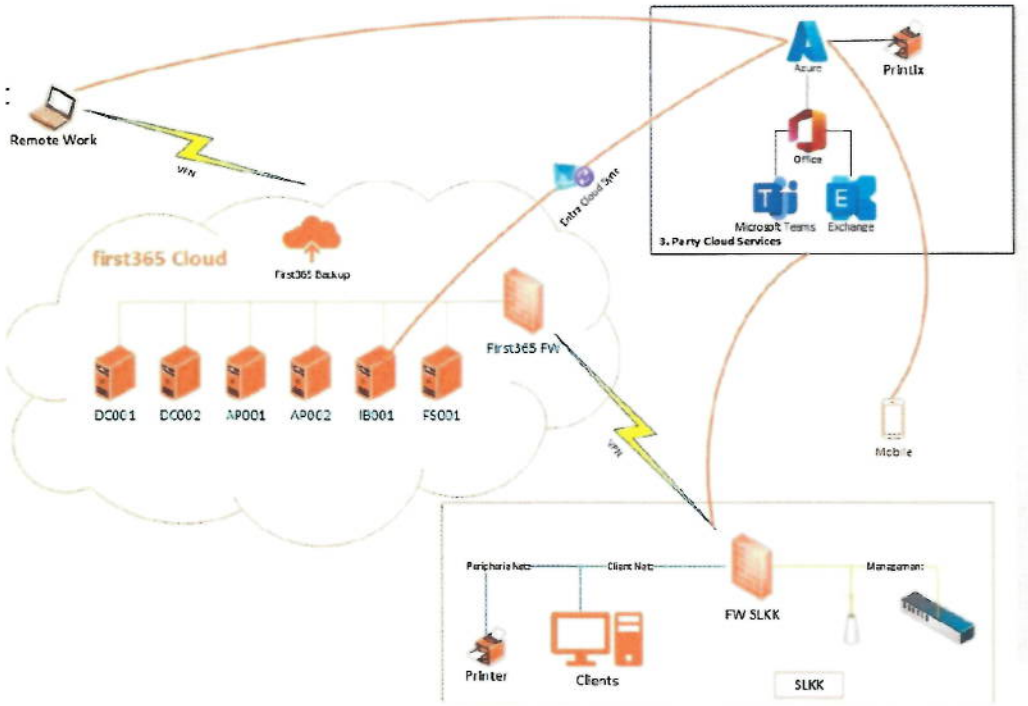
Die Einstufung einer Rechnung als auffällig oder unauffällig ergibt sich durch die Dunkelprüfung der DAS der SUMEX AG und durch hinterlegte Auslenkungskriterien. Es existieren Kriterien, bei denen Rechnungen automatisch ausgelenkt und direkt vom System abgewiesen werden.

1.9 Zugriff auf die Unterlagen

Dokumente, die nur der Vertrauensarzt (VA) einsehen darf (auffällige MCD), werden automatisch markiert und direkt dem VA zugestellt.

Mitarbeitende der KRANKENKASSE SLKK, die im Bereich des vertrauensärztlichen Dienstes (VAD) arbeiten, haben sich vertraglich als Hilfspersonen des VA verpflichtet und verfügen über entsprechende Zugriffsrechte. Andere Mitarbeitende der KRANKENKASSE SLKK und der ausgelagerten Stelle haben keine Einsicht in diese Dokumente.

2 Eingesetztes IT-System



Quelle: ffn für SLKK

Beschreibung der IT-Infrastruktur der SLKK

Die IT-Infrastruktur der SLKK wurde modernisiert und optimiert gemäss Vorgaben der , um Sicherheit, Effizienz und Skalierbarkeit zu gewährleisten.

- **Konsolidierung der Serverlandschaft**: Reduktion und Zentralisierung der Server zur besseren Ressourcennutzung und Wartung.
- **Intune Endpoint Management**: Zentrale Verwaltung und Absicherung aller Endgeräte zur Gewährleistung eines einheitlichen Sicherheitsstandards.
- **Defender Security Stack**: Implementierung eines umfassenden Sicherheitskonzepts mit Microsoft Defender für Schutz vor Bedrohungen und Angriffen.
- **Cloud Mail Migration**: Umstellung der E-Mail-Kommunikation in die Cloud für höhere Verfügbarkeit und Sicherheit.

Diese Massnahmen tragen zur erhöhten IT-Sicherheit, besseren Kontrolle über die IT-Umgebung und einer effizienteren Verwaltung der Infrastruktur bei.

Die SLKK nutzt die ERP-Lösung «Siddhartha» der SUMEX AG, die von SUMEX gewartet und betrieben wird. In diesem System werden folgende versicherungsrelevanten Daten verarbeitet:

- Vertragsdaten (z. B. Name, Geburtsdatum, Adresse, Versicherungsnummer, Gesundheitsdaten)
- Leistungsdaten für die Abrechnung
- Inkasso und Mahnwesen

- Archivierung

2.4 Schnittstellen

Leistungserbringer

Leistungserbringer haben keinen direkten Zugriff auf die Systeme der SLKK. Deckungsanfragen mittels Versichertenkarte erfolgen über das Veka-Center (Sasis AG) via zertifizierte Schnittstelle.

Medgate

Für die alternativen Versicherungsmodelle SLKK-TelCare und SLKK-SmartMed arbeitet die SLKK mit Medgate zusammen. Medgate erhält über eine sichere SFTP-Verbindung nur versicherungstechnisch relevante Daten, um Versicherte beraten zu können. Ein direkter Zugriff auf SLKK-Systeme besteht nicht.

SVK (Schweizerischer Verband für Gemeinschaftsaufgaben der Krankenversicherer)

Der SVK bearbeitet im Auftrag der SLKK vertrauensärztliche Leistungen zu speziellen Medikamenten, Transplantationen, Dialysen, künstlicher Ernährung zu Hause und mechanischer Heimventilation. Zudem prüft die SVK-Datenannahmestelle SwissDRG-Rechnungen zu Transplantationen und Dialysen und leitet sie zur finalen Bearbeitung an die SLKK weiter. Die SVK-Datenannahmestelle wurde beim EDÖB gemeldet.

Vertrauensarzt

Externe Vertrauensärzte und Vertrauenszahnärzte haben gesicherten Zugriff für die Beurteilung benötigten Daten. Daten werden nicht dauerhaft gespeichert. Der Vertrauenszahnarzt erhält keine direkten Zugriffsrechte; Anfragen erfolgen schriftlich. Der vertrauensärztliche Dienst (VAD) arbeitet intern, ist aber räumlich und technisch von anderen SLKK-Einheiten getrennt.

SUMEX AG

Die SUMEX AG stellt das Kernsystem bereit, wobei der SUMEX-Support keinen Zugriff auf das ERP-System hat. Fehleranalysen werden ausschliesslich in einer externen Testumgebung durchgeführt. Updates und Fehlerbehebungen erfolgen über Releases und Hotfixes, die vom SLKK-Systemadministrator vor Ort implementiert werden. Der Schutz von Daten und Systemen wird durch starke Authentifizierungsverfahren, Verschlüsselung und moderne Übertragungstechnologien sichergestellt.

Mitarbeitende

SLKK-Mitarbeitende greifen über ihre Clients auf benötigte Daten in den Applikations- und Dateiservern zu. Alle Daten werden durch Backups gesichert, die nur die IT-Abteilung einsehen kann. Netzwerkkontrolle regelt den Zugriff auf Laufwerke und Ordner. Bei Telearbeit gelten besondere Datenschutzrichtlinien.

2.5 Externe Schnittstellen

Medicall

Medicall unterstützt Versicherte im Ausland in Notfällen. Der Datenaustausch mit der SLKK erfolgt verschlüsselt per E-Mail. Medicall hat keinen direkten Zugriff auf SLKK-Daten oder Systeme.

Hausarztnetzwerk Arztmap

SL erhält von Ärztenetzwerken nur die für die SLKK-HomeCare-Versicherung relevanten Personendaten. Der Datenübermittlungsprozess ist vertraglich geregelt. SL übermittelt verschlüsselte E-Mails über HIN mit Versichertenlisten.

Dokumentenbearbeitung und Umsysteme des ERP-Tools

Für die Bearbeitung, Speicherung und Archivierung von Unterlagen nutzt die SLKK neben dem ERP-System der SUMEX AG folgende ergänzende Applikationen:

- **OLE**: Modul zur Digitalisierung und Bearbeitung von papierbasierten Leistungsabrechnungen sowie zur Korrektur oder Ergänzung unvollständig oder fehlerhaft digitalisierter Belege.
- **Therefore**: Dokumentenmanagement-System zur Erstellung und Verwaltung von Kundenkorrespondenz. Es wird für die Erstellung von Briefen und weiteren Mitteilungen genutzt, die nach dem Scannen direkt ins ERP-Tool weitergeleitet und dort archiviert werden.
- **Datawarehouse**: Zentrales Datenspeichersystem bei der SUMEX AG, in dem relevante Daten für Analyse- und Reporting-Zwecke strukturiert abgelegt werden.

Diese Umsysteme gewährleisten eine effiziente und sichere Bearbeitung von Dokumenten sowie eine reibungslose Integration in die bestehenden Prozesse der SLKK.

2.6 Outsourcing

Mit allen Partnern bestehen Datenschutzvereinbarungen. Durch Vertragsunterzeichnung bestätigen alle Beteiligten die Einhaltung der Datenschutzvorschriften.

3 Organisation

3.1 Geschäftsstellen, Filialen

Die SLKK betreut Versicherte in der Schweiz im Rahmen der obligatorischen Krankenpflegeversicherung. Sie unterhält keine Geschäftsstellen oder Filialen. Der Hauptsitz befindet sich in **8050 Zürich**.

3.2 Organisationsstruktur

Die Genossenschaft KRANKENKASSE SLKK ist eine Genossenschaft mit Sitz in Zürich.

Der **Vorstand** (die Verwaltung) besteht aus vier Personen. Die **Geschäftsleitung** besteht aus drei Personen und ist für die operative Geschäftsführung verantwortlich. Die SLKK beschäftigt insgesamt **22 Mitarbeitende**.

Die **interne und externe Revision** sowie der **Compliance Officer** sind dem Vorstand direkt unterstellt.

Die Organisation gliedert sich in folgende Bereiche:

- Vertrieb
- Leistungsabteilung (ambulant und stationär)
- Vertrauensärztlicher / Vertrauenszahnärztlicher Dienst
- Zertifizierte Datenannahmestelle (ausgelagert)
- Finanzen
- Informatik (ausgelagert)
- Compliance, Risikomanagement und Datenschutz
- Interne Revision (ausgelagert)

3.3 Verantwortlichkeiten

Die Gesamtverantwortung für den Datenschutz liegt beim Vorstand und der Geschäftsleitung. Diese Verantwortung kann nicht delegiert werden.

Alle weiteren Aufgaben, Kompetenzen und Verantwortlichkeiten im Bereich Datenschutz und Sicherheit sind in den jeweiligen Stellenbeschreibungen festgehalten.

Der Datenschutzbeauftragte berät das Unternehmen bei der Umsetzung und Einhaltung der Datenschutzrichtlinien und führt regelmässige Kontrollen durch. Die Verantwortung für die Einhaltung der Datenschutzvorgaben verbleibt jedoch bei der SLKK bzw. den jeweiligen Abteilungen.

4 Benutzer und Datenzugriff

4.1 Benutzer

Folgende Benutzergruppen haben Zugriff auf die IT-Systeme der SLKK:

- Mitarbeitende der SLKK, um die Abwicklung der Krankenversicherungsverträge zu gewährleisten.
- IT-Dienstleister (vertraglich beauftragt) zur Wartung und Fehlerbehebung.

Die Zugriffsberechtigung (Leserecht / Bearbeitungsrecht) wird abhängig von der jeweiligen Funktion und Rolle erteilt und dokumentiert.

4.2 Benutzerverwaltung

Die Benutzerverwaltung erfolgt zentral durch den internen IT-Koordinator.
Die Geschäftsleitung und die Personalabteilung sind für die Vergabe und Zuteilung der IT-Zugriffsrechte zuständig.

Für jede/n Mitarbeitende/n wird ein Zugriffsprotokoll geführt, das:

- Jährlich überprüft wird.
- Im Mitarbeiterdossier dokumentiert bleibt.

4.3 Aufhebung der Zugriffsrechte

Zugriffsrechte werden nur für die Dauer und in dem Umfang gewährt, wie sie für die Erfüllung der jeweiligen Aufgaben erforderlich sind.
Bei Austritt eines Mitarbeitenden wird die Zugriffsberechtigung unverzüglich deaktiviert und dokumentiert.

4.4 Schulung der Benutzer

Alle Benutzer werden intern auf das ERP-System und die für den Betrieb notwendigen Applikationen geschult.

4.5 Prozessabläufe und interne Richtlinien

- Die Arbeitsprozesse sind im Intranet und in Handbüchern dokumentiert und für alle Mitarbeitenden zugänglich.
- Die interne Kontrollstelle und die interne Revision überprüfen regelmässig die Aktualität dieser Prozesse.

5 Bearbeiten von Daten

5.1 Datenbeschaffung

Die Daten stammen in erster Linie von den 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
- Gesundheitsdaten

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

Die Ausnahmen gemäss Art. 17 DSG bleiben vorbehalten.

5.4 Weitere Datenweitergabe nach Art. 84a KVG

Die Weitergabe von Daten ist abschliessend in Art. 84a KVG geregelt. Im Einzelfall und auf schriftlich begründetes Gesuch hin können Daten gemäss den gesetzlichen Vorgaben an Sozialhilfebehörden, Zivilgerichte, Strafgerichte, Strafuntersuchungsbehörden und Betreibungsämter weitergegeben werden. Zudem ist eine Datenweitergabe an Dritte nur mit der schriftlichen Einwilligung der betroffenen Person zulässig.

5.5 Anmeldung der Verzeichnisse der Bearbeitungstätigkeiten beim EDÖB

Die SLKK verfügt über eine dem EDÖB gemeldete betriebliche Datenschutzberatung gemäss Art. 10 DSG. Nach Art. 12 DSG ist die SLKK verpflichtet, ein Verzeichnis ihrer Bearbeitungstätigkeiten zu führen. Dieses Verzeichnis wird erfasst und jährlich auf Aktualität überprüft.

6 Datenannahmestelle

Die SLKK betreibt eine zertifizierte Datenannahmestelle zur Verarbeitung elektronischer DRG-Rechnungen gemäss Art. 59a KVV sowie zur Bearbeitung von DRG-Rechnungen in Papierform (falls solche noch eingehen). Die Geschäftsleitung der SLKK versichert, dass sowohl die Datenannahmestelle als auch der VA/VAD unabhängig handeln und ausschliesslich die für eine weitere Prüfung erforderlichen Daten an den Versicherer (SLKK) weitergeben.

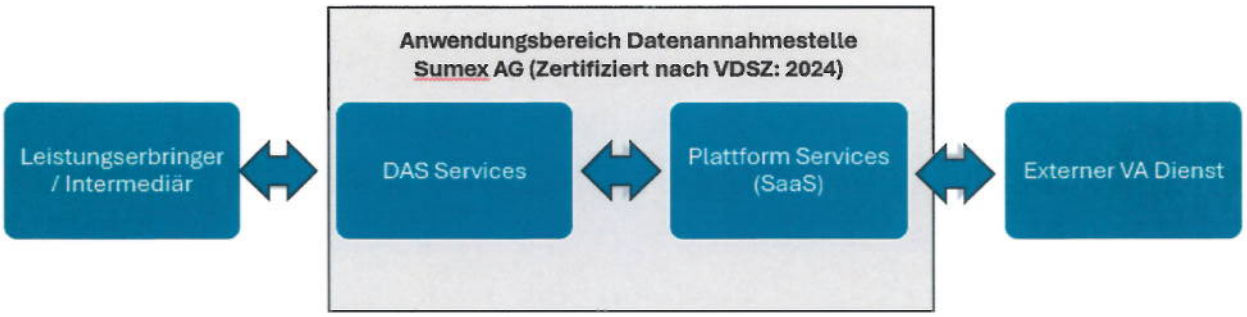
Die versicherungstechnischen Prüfungen erfolgen im System Siddhartha der SLKK. Das Regelwerk für diese Prüfungen wird nach einem festgelegten Prozess definiert, implementiert, überprüft und regelmässig angepasst. Vor jeder Regeländerung erfolgt eine Prüfung durch die Datenschutz-beratenden der Sumex AG auf Konformität und Machbarkeit. DRG-Rechnungen, bei denen sowohl die MCD-Prüfung als auch die Prüfung anhand des SLKK-Regelwerks in Siddhartha keine Auffälligkeiten ergeben, werden automatisch zur Zahlung freigegeben. Nicht ausgelenkte MCD-Daten sind für die Mitarbeitenden der SLKK nicht zugänglich.

6.2 Prozessbeschreibung «Datenannahmestelle (DAS) Services»

«DAS Services» umfasst den Dokumentenempfang und -versand gegenüber Leistungserbringern in einem geführten Prozess. Die «Plattform Services (SaaS)» der SUMEX AG bieten als Software-as-a-Service (SaaS) die ERP-Lösung «Siddhartha» und die automatisierte Rechnungsprüfung «Sumex Suite».

Gemeinsam decken «DAS Services» und «Plattform Services (SaaS)» die Datenannahmestelle für die elektronische Rechnungsstellung von Spitalrechnungen gemäss Art. 59a KVV ab. Die Datenannahmestelle der SUMEX AG ist VDSZ:2023 zertifiziert.

Systemübersicht «DAS Services» der SUMEX AG



Leistungen von DAS Services

- Entgegennahme elektronischer Rechnungen, Container und MCD (Minimal Clinical Dataset) von Leistungserbringern oder Intermediären
- Vergabe einer Tracking-ID zur Nachverfolgung der Dokumente
- Weiterleitung der Dokumente an die SL:
    - Einlesen der Dokumente in Sumex SaaS und Durchführung der Dunkelprüfung via DRG-Box
    - Auslenkung auffälliger MCD im Sumex Client SaaS mit Berechtigungssteuerung

- Möglichkeit zur Weiterleitung auffälliger MCD an externe VA-Dienste
- Archivierung der Originaldokumente (XML) mit Zugriff via Sumex Client (SaaS)

Verantwortungsbereich der SLKK

- Inhaber der Datensammlung
- Import und Verarbeitung der elektronischen Rechnungen sowie Export der Rückmeldung
- Datenbereitstellung/Abholung seitens Dunkelprüfung-Service durch Sumex
- Dunkelprüfung
- Plausibilität der Dunkelprüfung
- Datenverbindung/Internet
- Wartung und Betrieb der IT-Infrastruktur
- Vergabe der Zugriffsrechte in Bezug auf die MCDs
- Arbeitsprozess, im Speziellen von VA/VAD, inklusive Verwendung DRG-Expert
- Gesetzliche Rahmenbedingungen
- Rechtliche Grundlage Art. 59a KVV

6.1 Bearbeitungsprozess der DAS

Die DRG, Tarpsy- und STReha-Daten (Rechnung + MCD) werden von den Leistungserbringern elektronisch an die DAS der SMEX AG übermittelt. Die elektronische Datenübermittlung zwischen den Leistungserbringern und der DAS erfolgt mittels Intermediär, namentlich über H-Net und MediDataNetz. Die Datenübermittlung erfolgt verschlüsselt mittels PGP-Verschlüsselung.

Durch den Eingang im DAS der SUMEX AG als XML-File gelangen die DRG, Tarpsy- und Reha-Rechnungen sowie das MCD in den Scope der durch die SUMEX AG betriebenen DAS. Die MCD-Prüfung erfolgt durch die Sumex AG, wobei die anonymisierten MCD-Daten über die SUMEX-Dienstleistung verarbeitet werden. Diese Daten werden verschlüsselt bei der Sumex AG gespeichert. Zugriff auf diese Daten hat ausschliesslich der VA/VAD der SLKK, sofern dies gemäss Art. 59a KVV erforderlich ist.

Die Rechnungen werden, wenn seitens des Leistungserbringers möglich, nur noch elektronisch empfangen. Falles der Leistungserbringer die SwissDRG- oder die Tarpsy Rechnung als Papierdokument an die SLKK versendet, wird das Couvert 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.

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

Die Sumex AG ist Dienstleistungspartner nach Art. 10a DSG für die Datenannahmestelle nach Art. 59a KVV für die SLKK. Die Datenannahmestelle der Sumex AG beinhaltet im Wesentlichen:

- Empfang elektronischer Rechnungen mit MCD
- Technischer Transport zur Dunkelprüfung mittels Sumex Box
- Handhabung und Bereitstellung der Information, ob eine Auslenkung von auffälligen MCD auf dem Kundenserver stattfinden muss. Falls es zu einer Auslenkung kommt, kann die Rechnung durch befugte Personen (z.B. VAD) beurteilt werden.

- Sicherstellung, dass nur die vom Versicherer bezeichneten Personen Zugriff auf die MCD's haben

Zugriffskontrollen

Die SLKK-Mitarbeitenden greifen über ihren persönlichen Sumex Client-Zugang auf die Cloud-Daten zu. Dies umfasst:

1. **Dokumentenaustausch:** Empfang und Versand von Rechnungen und MCD-Dokumenten
2. **Weiterleitung:** Übermittlung der Dokumente an die Plattform Services (SaaS)
3. **Prüfung & Zugriff:** Rechnungs- und MCD-Prüfung mit Zugriffskontrolle
4. **Externe Schnittstellen:** Anbindung an externe VA-Dienste

Daten werden gesichert gespeichert. Der Vertrauensarzt hat Zugriff auf für seine Aufgaben erforderliche Daten, während SLKK-Mitarbeitende keinen Zugriff auf die Vertrauensarzt-Daten haben. Kunden und Leistungserbringer haben keinen direkten Zugriff auf gespeicherte Daten.

USER	Vertrauensarzt	Vertrauensärztlicher Dienst VAD	Fachperson mit besonderen Kenntnissen (ohne MA SLKK)	Fachperson mit besonderen Kenntnissen (mit MA SLKK)
DAS SUMEX AG				
Auffällige MCD mit VAD-Flag	Zugriff	kein Zugriff	kein Zugriff	Kein Zugriff
MCD ohne VAD-Flag	Zugriff	Zugriff	kein Zugriff	kein Zugriff
Ausgelenkte DRG Rech'g	Zugriff	Zugriff	kein Zugriff	Zugriff
Abgeschlossene Rechnungen	Zugriff	Zugriff	kein Zugriff	Zugriff

7 Archivierung und Vernichtung

7.1 Aufbewahrungspflicht

Archivierungspflichtige Dokumente werden für die gesetzlich vorgeschriebene Dauer sicher aufbewahrt und gegen unbefugten Zugriff sowie Veränderungen geschützt. Für Daten der sozialen Krankenversicherung nach KVG gilt eine gesetzliche Aufbewahrungspflicht von zehn Jahren (Art. 958f OR). Der gesamte Prozess der Aufbewahrung, Archivierung und anschliessenden Vernichtung ist in der Richtlinie zum Umgang mit Assets und Dokumentationsschutz geregelt.

7.2 Vernichtung physischer Daten

Die Vernichtung vertraulicher oder besonders schützenswerter physischer Dokumente erfolgt bei der SLKK in Übereinstimmung mit den datenschutzrechtlichen Vorgaben. Nach Ablauf der gesetzlichen Archivierungsfrist werden diese Dokumente fachgerecht und sicher vernichtet, da die rechtliche Grundlage für deren Aufbewahrung entfällt. Die Entsorgung erfolgt nicht über öffentlich zugängliche Behälter, sondern ausschliesslich durch eine zertifizierte Entsorgungsfirma.

7.3 Vernichtung elektronischer Daten

Elektronische Datenträger werden vor der Entsorgung entweder unlesbar gemacht oder von einem zertifizierten Unternehmen datenschutzkonform vernichtet. Nach Ablauf der gesetzlichen Aufbewahrungsfrist erfolgt eine endgültige, unwiederbringliche Löschung elektronischer Daten, um sicherzustellen, dass keine Wiederherstellung möglich ist.

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 andere Systeme der SLKK ist durch eine USER-ID geschützt. Das Login auf den Rechner erfolgt ausschliesslich über Fingerprint-Authentifizierung. Für den Zugriff auf Umsysteme ist zusätzlich eine Passwort-Eingabe erforderlich.

Zur Verhinderung unbefugter Zugriffe auf automatisierte Datenbearbeitungssysteme über externe Datenübertragung wurden folgende Sicherheitsmassnahmen implementiert:

- Protokollierung aller Zugriffe und Aktivitäten
- Einsatz von Anti-Viren-Software zur Prävention von Schadsoftware und unautorisierten Zugriffen
- Einsatz von 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.

8.7 Kontrollen

Die Einhaltung der datenschutzrechtlichen Bestimmung wird intern folgendermassen sichergestellt und kontrolliert. Folgende Massnahmen sind definiert:

- Schriftlich festgehaltene Datenschutzpolitik, die allen Mitarbeitenden bekannt, und in Intranet der SLKK publiziert ist.
- Datenschutz- und Datensicherheitsrichtlinie/-weisung.
- Regelungen von Aufgaben, Verantwortlichkeiten und Kompetenzen bezüglich Datenschutzes und Datensicherheit in verträglichen Unterlagen.
- Die Zugänge zu den Büros sowie zum Archiv sind sowohl technisch als auch mechanisch gesichert.
- Jährliche Schulung aller Mitarbeitenden bezüglich Datenschutzes und Datensicherheit.
- Der Datenschutzberatende führt jährliche Audits durch gemäss dem Plan.
- GL und Vorstand werden regelmässig über Einhaltung der Vorschriften und über die Massnahmen via Berichte informiert. Jährliche Risikoanalyse im Rahmen eines Management Reviews.
- 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.
- Regelmässige Überprüfung der Outsourcing-Partner, durch Kontrolle der aktuellen Reglemente, der Erfüllung von Projektplänen und der aktuellen Auditberichte.
- IKS-Kontrollen inkl. der jährliche Kontrolle des Verzeichnisses der Bearbeitungstätigkeiten auf dessen Vollständigkeit, Korrektheit und die Zweckmässigkeit der Datenbearbeitung sowie eine Überprüfung der gesamten Dokumentation.
- Es erfolgt eine jährliche IT-Kontrolle durch eine externe Revision.

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 Händen des Datenschutzberatenden, Hofwiesenstrasse 370, 8050 Zürich zu richten.

9.3 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.

9.4 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.

9.5 Anhänge

Die im vorliegenden Bearbeitungsreglement erwähnten Anhänge sind integrierende Bestandteile dieses Bearbeitungsreglements. Die Anhänge können auf der Geschäftsstelle eingesehen werden:

- Vertrag mit SUMEX inkl. DAS Services
- Verträge betreffend Hilfspersonen VA
- Stellenbeschreibung der Datenschutzbeauftragten

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 27. März 2025 gültig. Es ersetzt das Bearbeitungsreglement Ausgabe 1. September 2023.

KRANKENKASSE SLKK

Zürich, 27. März 2025

Felix L'Orange	Roland Kleiner	Yanina Zawisla
Präsident	Direktor	Datenschutzberaterin

11 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