SLKK

vernünftig versichert: die
ehemalige Schweizerische
Lehrerkrankenkasse

Bearbeitungsreglement zur Sicherstellung des Datenschutzes 2016

KRANKENKASSE SLKK

Dokumentenstatus

Dokumententyp:	Reglement
Klassifizierung:	Public
Editor:	Datenschutzbeauftragte
Editiert am:	06.10.2016
Prüfer:	Geschäftsleitung / EDÖB
Freigegeben am:	20.10.2016
Version:	1.1
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.

Inhaltsverzeichnis

1 Allgemeine Bestimmungen

1.1 Rechtliche Grundlage

Gestützt auf Art. 11 und Art. 21 der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) in Verbindung mit Artikel 84b des Bundesgesetzes über die Krankenversicherung (KVG) hat die KRANKENKASSE SLKK (SLKK) für die Datensammlung, welche besonders schützenswerte Daten oder Persönlichkeitsprofile beinhalten, das vorliegende Bearbeitungsreglement (Reglement) erstellt.

1.2 Ziel des Bearbeitungsreglements

Das Bearbeitungsreglement umschreibt insbesondere die Datenbearbeitungs- und Kontrollverfahren und den Betrieb der elektronischen Datenbearbeitung. 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 in Art. 84 KVG geregelt. Die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung des Gesetzes beauftragten Organe sind befugt, die Personendaten, einschliesslich besonders schützenswerter Daten und Persönlichkeitsprofile (Art. 3 lit. c, d DSG), zu bearbeiten, um die ihren nach dem Gesetz übertragenen Aufgaben zu erfüllen.

1.4 Verantwortliche Stelle

Die SLKK ist verantwortlich für die Abwicklung der obligatorischen Krankenpflegeversicherung nach KVG und somit Inhaberin der Datensammlungen. Mit den im Reglement vorgesehenen Massnahmen sorgt die SLKK für die Einhaltung der gesetzlichen Vorschriften.

1.5 Definition Datensammlung

Jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind, stellt eine Datensammlung nach Art. 3 lit. g DSG dar.

Die Erschliessbarkeit bildet jedoch nur eines von mehreren Kriterien, weitere ergeben sich aus dem Wortlaut, aber auch aus Sinn und Zweck der Bestimmungen betreffend Datensammlung. Weitere Voraussetzungen b bilden das Vorhandensein von Personendaten von mehr als einer Person, das Festhalten von Personendaten als solchen sowie von mehreren Datensätzen, welche zudem einen thematischen Zusammenhang sowie eine gewisse Beständigkeit aufweisen.

1.6 Richtliniendatenschutz- 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 und Art. 35 DSG

Sämtliche Mitarbeitende unterstehen während und über das Arbeitsverhältnis hinaus der Schweigepflicht nach Art. 33 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) und Art. 35 des Bundesgesetzes über den Datenschutz (DSG). Die Schweigepflicht bildet Bestandteil der unter Ziff. 1.6. erwähnten Richtlinien. Bei Verletzung der Schweigepflicht gelten die strafrechtlichen Bestimmungen von Art. 92 KVG.

2 EDV Struktur

2.1 Übersicht

SLKK arbeitet mit der ERP-Lösung BBT*individual* (BBTi), welche in Haus gewartet und betrieben wird. In diesem System werden folgende versicherungsrelevanten Daten bearbeitet:

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

2.2 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.

Medgate

Im Zusammenhang mit dem alternativen Versicherungsmodell SLKK-TelCare arbeiten wir mit Medgate zusammen. Medgate hat keinen Zugriff auf unsere Systeme, bekommt aber die versicherungstechnisch notwendigen Daten von der KRANKENKASSE SLKK über eine sichere Linie (SFTP) geliefert.

Vertrauensärztlicher Dienst
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. Auf alle anderen Versicherten hat er keinen Zugriff.
Der Vertrauenszahnarzt hat keinen Zugriff. Diese Anfragen werden schriftlich gestellt und mit der Post auf Papier versandt.
Der vertrauensärztliche Dienst arbeitet im Haus und ist räumlich von den anderen Organisationseinheiten abgegrenzt.

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

BBT Software:
Der Support von BBTi hat keinen Zugriff auf das ERP-System. Systemfehler werden auf einer Testdatenbank, in einer völlig unabhängigen Umgebung, eruiert. Updates und Fehlerbehebungen werden über Releases und Hotfixes gelöst, welche vom Systemadministrator der SLKK importiert werden.

Mit Authentifizierung, Verschlüsselungs- und modernen Übertragungstechnologien werden in Bezug auf diese und allfällige weitere Schnittstellen der Datenschutz und die Datensicherheit gewährleistet.

Die Mitarbeitenden der SLKK können via ihres Computers (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.

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

2.4. IT-Infrastruktur
Sowohl die Firewall als auch das Antivirus-Programm werden regelmässig automatisch aktualisiert.

3 Organisation

3.1 Geschäftsstellen, Filialen

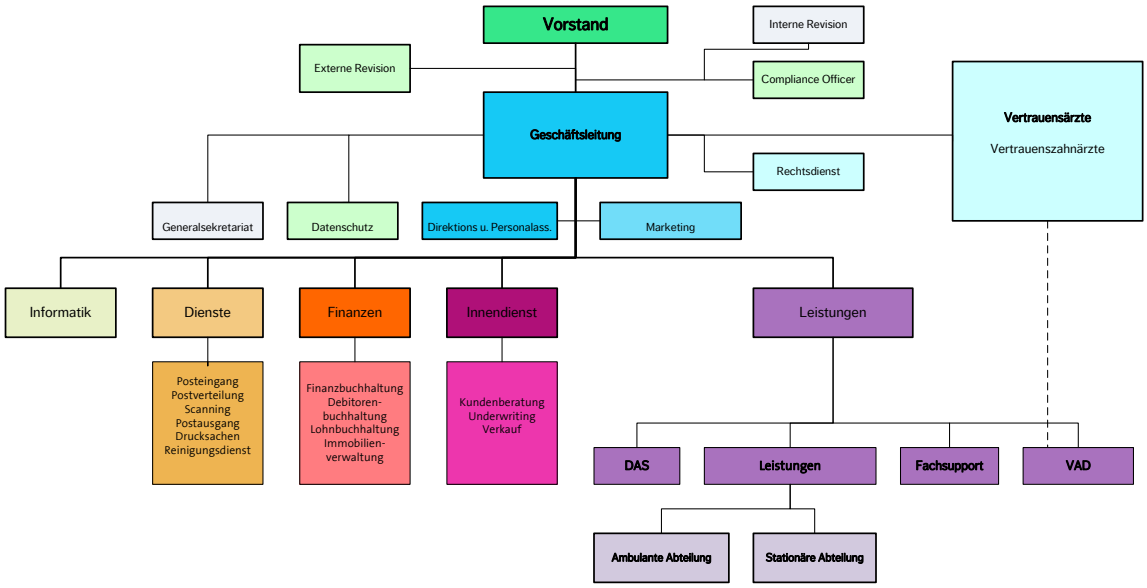
Die SLKK betreut Versicherte in der deutschsprachigen Schweiz in der obligatorischen Krankenpflegeversicherung. Wir haben weder Geschäftsstellen noch Filialen.

3.2 Organisationsstruktur

Die SLKK ist in folgende Bereiche aufgeteilt

- Leistungen mit dem vertrauensärztlichen Dienst
- Innendienst
- Finanzen
- Informatik
- Dienstleistungszentrum

Die Geschäftsleitung besteht aus drei Personen und ist für die operative Geschäftsführung zuständig. Die datenschutzverantwortliche Person im Unternehmen ist dem Direktor unterstellt.
Die SLKK beschäftigt 22 Mitarbeitende.
Die Genossenschaft KRANKENKASSE SLKK ist eine Genossenschaft mit Sitz in Zürich. Der Vorstand besteht aus vier Personen.



PUBLIC

3.3 Verantwortlichkeiten

Die Gesamtverantwortung für den Datenschutz tragen der Vorstand und die Geschäftsleitung. Diese Verantwortung ist nicht übertragbar.
Alle weiteren Aufgaben, Kompetenzen und Verantwortlichkeiten betreffend Datenschutz und Sicherheit sind in den entsprechenden Stellenbeschreibungen festgehalten.
Der betriebliche Datenschutzbeauftragte 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 Datensammlung (SLKK), bzw. bei den entsprechenden Abteilungen.

4 Benutzer und Datenzugriff

4.1 Benutzer

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 ist für die Definition der IT-Zugriffsrechte der einzelnen Mitarbeitergruppen 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 abgebildet und umschrieben und sind für alle Mitarbeitende abrufbar. 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 Datenkategorien

Es werden folgende wesentliche Datenkategorien im System geführt:

- Name, Vorname
- Geburtsdatum
- AHV-Nummer
- Sozialversicherungsnummer
- Versichertennummer
- Adresse
- Nationalität
- Zahladresse
- Vertragsdaten
- Leistungsdaten
- Prämiendaten
- Mahndaten

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, Be-

treibungsämter sowie mit schriftlicher Einwilligung der betroffenen Person an Dritte weitergegeben werden.

5.5 Anmeldung der Datensammlungen beim EDÖB

Da die SLKK über einen dem EDÖB gemeldeten, betrieblichen Datenschutzverantwortlichen nach Art. 12a und 12b VDSG verfügt, ist sie gemäss Art 11a Abs. 5 lit. e DSG vom Führen eines öffentlich zugänglichen Registers der Datensammlungen und von der Pflicht zur Anmeldung der Datensammlung befreit.

6 Archivierung und Vernichtung

6.1. 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).

6.2. 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.

6.3. 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.

7 Technische und organisatorische Massnahmen

7.1 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.

7.2 Authentifizierung der Benutzer

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.

7.3 Zusammenarbeit mit Partnern

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

8 Rechte der Versicherten

8.1 Informationspflicht beim Beschaffen von Personendaten

Art. 18a DSG verlangt die Information der betroffenen Person, wenn besonders schützenswerte Personendaten oder Persönlichkeitsprofile beschafft werden. Auf Grund des gesetzlichen Auftrages nach KVG zur Bearbeitung von Gesundheitsdaten gilt die Ausnahmeregelung nach Art. 18a Abs. 4 lit. a DSG, wonach die Informationspflicht des Inhabers der Datensammlung entfällt, wenn die Speicherung oder die Bekanntgabe ausdrücklich durch das Gesetz vorgesehen ist.

8.2 Auskunftsrecht nach Art. 8 DSG

Jede Person kann von der SLKK schriftlich Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Für das Auskunftsrecht richtet sich nach Art. 8 und 9 DSG sowie Art. 1 und 2 VDSG.

Die Auskunftsgesuche sind unter Beilage einer amtlichen Ausweiskopie an die KRANKENKASSE SLKK, zu Handen des Datenschutzbeauftragten, Hofwiesenstrasse 370, 8050 Zürich zu richten.

8.3 Berichtigungs- und Löschungsrechte

Die betroffenen Personen können gemäss Art. 5 Abs. 2 und Art. 25 DSG verlangen, dass ihre Daten berichtigt, vernichtet oder die Bekanntgabe an Dritte gesperrt werden. Die entsprechenden Gesuche sind an die KRANKENKASSE SLKK, zu Handen des Datenschutzbeauftragten, Hofwiesenstrasse 370, 8050 Zürich zu richten.

9 Abschliessende Bestimmungen

9.1. Änderung des Reglements

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

9.2. Inkrafttreten

Dieses Reglement wurde von der Geschäftsleitung genehmigt und ist per 1. November 2016 gültig. Es ersetzt das Bearbeitungsreglement Ausgabe 2013.

KRANKENKASSE SLKK

Peter M. Sieber
Direktor

Mariette Steiger
Datenschutzbeauftragte

Glossar

ATSG	Bundesgesetz über den Allgemeiner Teil des Sozialversicherungsrechts
BAG	Bundesamt für Sozialversicherungen
EDÖB	Eidgenössischer Datenschutz- und Oeffentlichkeitsbeauftragter
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-Stellen	Invaliden-Stellen
AHV-Stellen	Alters- und Hinterlassenenversicherung
Santésuisse	Branchenverband der Krankenversicherer
Sasis AG	Aktiengesellschaft für die Versichertenkarten (Veka)
Medgate	Schweizer Zentrum für Telemedizin
Medicall	Notruf- und Dienstleistungszentrale