vita surselva
ihr krankenversicherer - nossa cassa

Bearbeitungsreglement Sicherheitskonzept

Inhaltsverzeichnis

Dateiname:	Bearbeitungsreglement.docx
Erstellungsdatum:	24.06.2020
Letzte Änderung:	31.08.2022
Datum:	31.08.2022

Postfach 44 · 7130 Ilanz/Glion · Tel. 081 925 61 60 · Fax 081 925 61 73 · info@vitasurselva.ch · www.vitasurselva.ch

1. Versionskontrolle

1.1. Änderungskontrolle

Datum	Version	Name	Beschreibung
17.02.2020	1.0	Deplazes I.	Dokument mit Versionskontrolle ergänzt
17.02.2020	1.0	Deplazes I.	Punkt 3.1. Organisationseinheiten und Prozessbeschriebe eingefügt
24.06.2020	1.1	Deplazes I.	Punkt 4 Übersicht der Partner erstellt
07.09.2020	1.1	Deplazes I.	Dokument geprüft und freigegeben
31.08.2021	1.2	Deplazes I.	Dokument mit Verlinkungen ergänzt und Bezeichnungen angepasst.
21.06.2022	1.3	Deplazes I.	Dokument geprüft.
19.08.2022	1.4	I. Deplazes	Interne Verlinkungen geprüft und angepasst.

1.2. Freigabe

Datum	Version	Name	Beschreibung
31.08.2022	1.4	I. Deplazes	Geschäftsführer Stv. Unterschrift

1.3. Offene Punkte

Datum	Name	Thema

2. Grundlagen und Aufbau

2.1. Zielrichtung

Die vita surselva ist eine nach dem Krankenversicherungsgesetz sowie nach dem Versicherungsvertragsgesetz tätige Krankenversicherung. Das Tätigkeitsgebiet erstreckt sich auf die gesamte Schweiz. Das Hauptgeschäftsfeld konzentriert sich hingegen vorwiegend auf die Bündner Surselva wie auch auf das übrige Kantonsgebiet. Der Sitz der Unternehmung befindet sich in Ilanz. Seit dem Jahr 2008 wird die vita surselva in der Rechtsform einer Stiftung geführt.

Die vita surselva verfährt für die Datenverarbeitung nach folgendem Datenschutzkonzept:
Die Verarbeitung personenbezogener Daten soll unter Berücksichtigung

- der Integrität (z. B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen oder der Manipulation von Daten),
- der Vertraulichkeit (z. B. Schutz vor unbefugter Kenntnisnahme von Daten) und
- der Verfügbarkeit (z. B. Schutz vor Diebstahl oder Zerstörung)

gewährleistet werden.

Die Sicherheitsmassnahmen werden in dem Datenschutzkonzept in die Bereiche

- Allgemeine Datenverarbeitung
- Automatisierte Datenverarbeitung
- Nutzung der Internetdienste

unterteilt

2.2. Rechtliche Grundlage

Gestützt auf Art. 21 der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) in Verbindung mit Art. 84 des Bundesgesetzes über die Krankenversicherung (KVG) hat die vita surselva für die Datensammlung, die besonders schützenswerte Daten oder Persönlichkeitsprofile beinhaltet, das vorliegende Bearbeitungsreglement erstellt.

Sämtliche Mitarbeitenden unterstehen der Schweigepflicht nach Art. 33 ATSG. Bei Verletzungen der Schweigepflicht unterstehen sie spezialgesetzlich den Strafbestimmungen des Art. 92 KVG. Die Mitarbeitenden sind über die Sanktionen informiert. Zusammen mit dem Arbeitsvertrag unterzeichnen Mitarbeitende die Schweigepflichtserklärung.

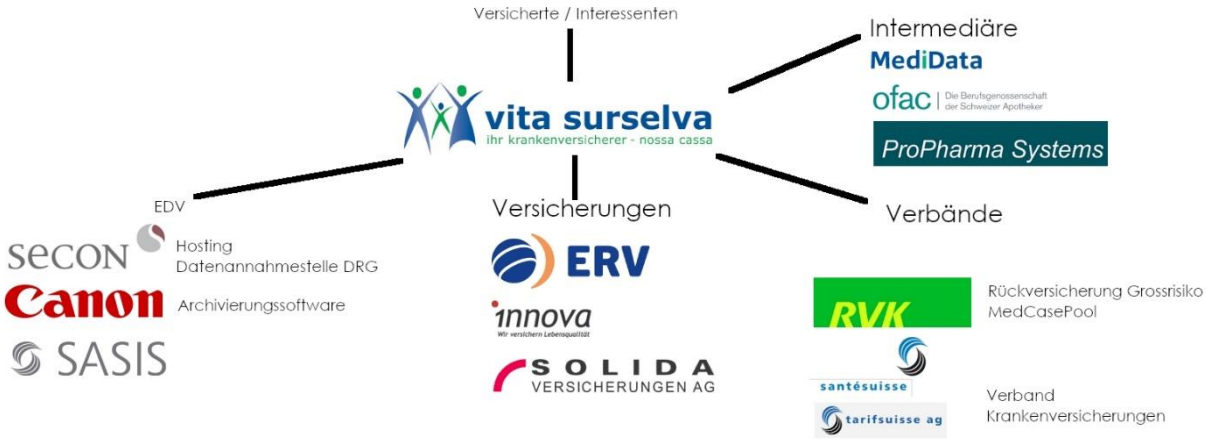
3. Zuständig- und Verantwortlichkeiten

Die Gesamtverantwortung für den Datenschutz trägt die Geschäftsführung. Diese Verantwortung ist nicht übertragbar. Alle weiteren Aufgaben, Kompetenzen und Verantwortlichkeiten betreffend Datenschutz und Sicherheit sind in den entsprechenden Stellenbeschreibungen festgehalten. Die Leiterin / der Leiter der Organisationseinheit Personal verfügt über aktuelle Versionen aller Stellenbeschreibungen.

3.1. Organisationseinheiten und Prozessbeschriebe

Die Organisationseinheiten, die zugehörigen Aufgaben und Prozessbeschriebe sind in einer internen Anwendung definiert und im internen Dokument Zuständigkeiten festgehalten.

4. Übersicht der Partner



5. Allgemeine Datenverarbeitung

5.1. Datenverarbeitung durch die Datenannahmestelle

Die Bearbeitung von Daten durch die Datenannahmestelle regelt ein spezifisches, detailliertes Bearbeitungsreglement, das den Anforderungen der Zertifizierung der Datenannahmestelle entspricht. Damit sind in diesem Rahmen alle datenschutzrechtlich relevanten Bestimmungen eingehalten.

5.2. Datenweitergabe nach KVG Art. 84 und Art. 84a

Daten werden bekannt gegeben für die

- Einhaltung der Versicherungspflicht (Art. 7 Abs. 5 KVG: Angaben zum Vorversicherer bzw. Nachversicherer)
- Beurteilung von Leistungsansprüchen (Bsp. Limitierungen nach KLV)
- Koordination mit anderen Sozialversicherungen (Bsp. Art. 27 KVG Koordination mit der IV bezüglich Geburtsgebrechen)
- Geltendmachung eines Rückgriffrechts gegenüber haftpflichtigen Dritten
- Führung von Statistiken
- Zuweisung oder Verifikation der Versicherten-Nummer an die AHV
- Bestätigung von Versicherungszeiten an ausländische Krankenversicherungen für die Befreiung der dortigen Versicherungspflicht (Formular E104)

5.3. Schulung der Mitarbeitenden

- Die Mitarbeitenden sind über die bei ihrer Tätigkeit anzuwendenden datenschutzrechtlichen Vorschriften zu unterrichten und zu schulen.
- Während der Einarbeitungszeit hat eine umfassende Unterrichtung über die einschlägigen Datenschutzbestimmungen zu erfolgen.
- Datenschutzrechtliche Vorschriften müssen fester Bestandteil der Fortbildungsplanung sein. Dies schliesst auch die Fortbildung im Umgang mit technikunterstützter Informationsverarbeitung und den daraus resultierenden Datensicherheitsmassnahmen ein.

5.4. Tür- und Fenstersicherung

- Nicht besetzte Büro- und Arbeitsräume sowie die Archive sind abzuschliessen.
- Die Schlüssel sind abzuziehen und sicher zu verwahren.
- Bei längerer Abwesenheit und Dienstende sind die Fenster zu schliessen

5.5. Aktenführung und Aktenaufbewahrung

- Akten, in denen personenbezogene Daten verarbeitet werden, sind so aufzubewahren, dass eine Einsichtnahme durch unbefugte Dritte nicht möglich ist.
- Dies gilt auch für Vorgänge, die in der laufenden Bearbeitung sind (Clear-Desk-Anweisung).

- Bei Akten, die einem besonders schutzwürdigen Interesse unterliegen, entscheidet die jeweilige Organisationseinheit über die darüber hinaus erforderliche Form der Aufbewahrung.
- Für die Vernichtung von Papierabfällen werden Schredder eingesetzt.

5.6. Archiv und Aufbewahrungsfristen

- Die Aufbewahrung von Akten im Archiv werden bereichsbezogen durchgeführt.
- Akten, die einem besonders schutzwürdigen Interesse unterliegen (z.B. Personalakten) sind vor der Einsichtnahme durch unbefugte Dritte besonders zu sichern.
- Akten und die damit verarbeiteten personenbezogenen Daten werden grundsätzlich gelöscht, wenn sie für die Aufgabenerledigung nicht mehr erforderlich sind und Aufbewahrungsfristen nicht entgegenstehen.
- Die Akten werden einer physikalischen Vernichtung zugeführt, bei der gewährleistet ist, dass unbefugte Dritte keine Einsicht nehmen können.
- Den Ablauf der Frist überwacht die für die Aktenführung zuständige Organisationseinheit.

5.7. Reinigungspersonal

- Das Reinigungspersonal ist von der Vergabestelle rechtswirksam nach dem Verpflichtungsgesetz zu verpflichten, keinen Einblick in Akten oder Kenntnis von automatisiert verarbeiteten Daten zu nehmen.
- Das Reinigungspersonal darf nur den Büro- und Arbeitsraum geöffnet haben, in dem gerade die Reinigung erfolgt.
- Die Kontrolle der Einhaltung dieser Vorschriften ist sicherzustellen.

5.8. Kundenverkehr

- Es ist sicherzustellen, dass Bürgerinnen und Bürger bei ihrer Vorsprache in der jeweiligen Organisationseinheit andere, als die ihre Angelegenheit betreffende personenbezogene Daten, nicht zur Kenntnis nehmen können. Dies gilt sowohl für Daten in Akten, als auch für automatisiert verarbeitete Daten.
- Bildschirme sind so aufzustellen, dass sie für Dritte nicht einsehbar sind.

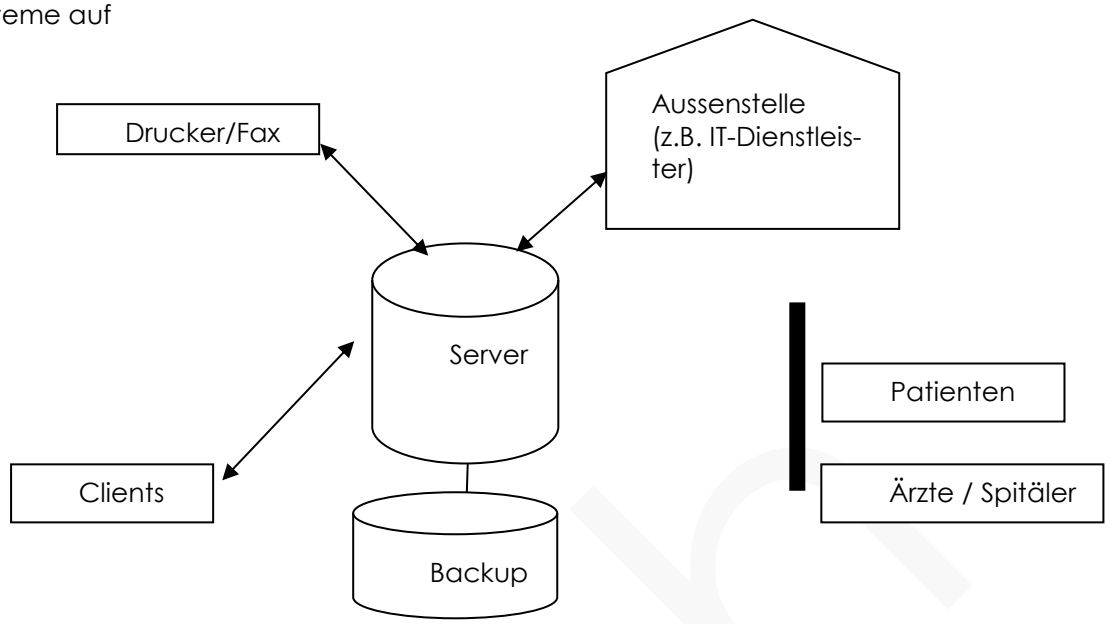
5.9. Auskünfte, Datenübermittlung

Jede Person kann von vita surselva Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Das Auskunftsrecht richtet sich nach Art. 8 und Art. 9 DSG.

- Bei einer Auskunftserteilung bzw. Datenübermittlung ist die Identität der bzw. des Ersuchenden zu prüfen und zu dokumentieren.
- Die Auskunftserteilung bzw. Übermittlung von personenbezogenen Daten hat grundsätzlich nur aufgrund einer schriftlichen Anfrage auf schriftlichem Wege zu erfolgen.
- Die jeweiligen Organisationseinheiten entscheiden selbständig über die Erforderlichkeit und die Festlegung von einheitlichen Verfahrensregelungen für die Auskunftserteilung bzw. Übermittlung von personenbezogenen Daten an Dritte.

6. Automatisierte Datenverarbeitung

Die nachfolgende, grafische Übersicht zeigt die von der Datenbearbeitung betroffenen Umsysteme auf



6.1. PC-Benutzenden

- Die PC-Benutzenden sind vor Aufnahme der Arbeit an PCs umfassend zu schulen. Ihnen sind entsprechende Handbücher zur Verfügung zu stellen.
- Die PC-Benutzenden sind selbst für die ordnungsgemässe Nutzung der ihnen zur Verfügung gestellten Hard- und Software zuständig.
- Sie sind über die grundsätzlichen Datensicherungsmassnahmen aufzuklären.

6.2. Kennwörter

- Für alle PC-Benutzenden sind Zugangskennungen für das Netzwerk und für die Verfahren zu vergeben.
- Dabei sind neben Benutzernamen auch Kennworte zu verwenden.
- Nicht erfolgreiche Anmeldeversuche sind aufzuzeichnen.

6.3. Externe Dienstleistende

- Der Leistungsumfang externer Dienstleistenden ist durch schriftlichen Vertrag zu regeln.
- Die Dienstleistenden sind zu verpflichten, Daten, die ihnen durch ihre Tätigkeit für die vita surselva bekannt werden, vertraulich zu behandeln.
- Fernadministration hat auf gesicherten Leitungen zu erfolgen.
- Die Leitungen sind nach Ende der Tätigkeit wieder zu sperren.

6.4. Arbeitsplatz-PC

- Beim Auf- oder Umstellen der Geräte ist auf geeignete Standorte (Lichtverhältnisse, Ergonomie, Ausschluss der Bildschirmeinsicht durch Fremde) zu achten.
- Die vita surselva stellt die Installation, Konfiguration und den Netzzugang der PCs sicher.
- Es sind ausschliesslich die für die dienstliche Aufgabe notwendigen Funktionen und Anwendungen zu installieren. Die Entscheidung hierüber trifft die Verantwortliche Organisationseinheit.

6.5. Zentrale Rechner (Server)

- Der Server ist mit einer unterbrechungsfreien Stromversorgung (USV) auszustatten.

- Sämtliche an Servern vorgenommene Arbeiten (Einstellungen oder Reparaturen) sind in einem Protokoll zu dokumentieren.

6.6. Zentrale Drucker

- Beim zentralen Drucker ist darauf zu achten, dass Ausdrucke mit personenbezogenen Daten nicht unbeaufsichtigt erfolgen.

6.7. Faxgerät

- Das Faxgerät ist so aufzustellen, dass Unbefugte keine Kenntnis von Inhalten eingehender und übertragener Telefaxe erhalten können.

6.8. Datenverwaltung

- Alle Datenbestände sind zentral auf dem Server zu speichern.
- Die Daten sind durch Zugriffsrechte auf dem Server voneinander abzugrenzen.
- Für die persönliche Datenablage auf dem Server (z. B. Entwurfsschreiben) sind besondere Verzeichnisse zu erstellen.
- Die dauerhafte Speicherung von Dateien als Muster oder Textbausteine ist nur zulässig, wenn sie anonymisiert werden.

6.9. Datensicherung

- Die Daten der Server sind täglich zu sichern.
- Die durchgeführten Sicherungen sind zu protokollieren.

6.10. Datenträger

- Externe Datenträger (Disketten, USB-Sticks, externe Festplatten) sind vor ihrem Einsatz durch bevollmächtige Mitarbeitende auf vorhandenen schädigenden Code (z. B. Viren) zu prüfen.
- Das gleiche gilt, wenn dienstliche Daten auf externen Datenträgern gespeichert und weitergegeben werden sollen.

6.11. PC-Benutzende und Rechteverwaltung

- Es ist eine Auflistung über PC-Benutzende und den ihnen zugewiesenen Rechten zu erstellen.
- PC-Benutzende sind ausschliesslich auf den Domänen-Server einzurichten.
- Zur Vereinfachung der Rechtezuweisung sind Benutzergruppen zu bilden.
- Den PC-Benutzenden sind mit Zustimmung der Verfahrensverantwortlichen entsprechende Zugriffsrechte zu erteilen.
- Die Berechtigungen sind soweit einzuschränken, dass ausschliesslich verfahrensbezogene Verzeichnisse genutzt werden können.

6.12. Applikationen

- Für die Verarbeitung des Krankenversicherungsgeschäfts wird die Kernapplikation Jetavana der Secon AG, Fehraltorf eingesetzt. Diese umfasst die Erfassung/Verarbeitung von Leistungen, Versichertenadministration, Rechnungsstellung und Mahnwesen.
- Für das Scannen von Dokumenten wird die Applikation Therefore von der Canon AG eingesetzt

Unterlagen bezüglich Planung und Realisierung der Applikationen sind bei den Lieferanten abgelegt. Die Unterlagen bezüglich des Betriebes sind bei der vita surselva in der Applikation selber integriert.

Die Schnittstellenbeschreibungen sind im Konformitätsnachweis wie folgt beschrieben:

- Herkunft der Daten
- Empfänger der Daten
- Periodizität der Datenweitergabe
- Zweck der Datenweitergabe
- Medium der Datenweitergabe
- Zweckmässigkeit der Datenbearbeitung

Die verantwortliche Stelle Geschäftsführung ist im Besitz des aktuellen Konformitätsnachweises.

7. Internet- E-Maildienste

- Die Übergänge vom internen Netz zum externen Netz sind durch Firewall-Systeme (z. B. Router, Gateways etc.) zu schützen.
- Die Verbindung für den Internetdienst www ist über eine Standleitung zur Firewall der Datenzentrale einzurichten. Das Sicherheitskonzept der Datenzentrale ist zu beachten.
- Eine Fernadministration der Firewall-Komponenten ist nicht gestattet.
- Die Einstellungen der einzelnen Komponenten des Firewall-Systems sind zu dokumentieren
- E-Mails und die an ihnen angehängten Dateien sind einer Virenüberprüfung zu unterziehen. Die dazu eingesetzte Virenschutzsoftware ist stündlich zu aktualisieren.
- Dateianhänge mit ausführbaren Programmen und Dateien (Dateiendungen: z. B. exe, com, bat und vbs) dürfen nicht geöffnet werden. Sofern diese E-Mails nicht explizit angefordert wurden, werden sie ohne weitere Überprüfung gelöscht.
- Das Herunterladen ausführbarer Programme und Dateien (Dateiendung: z. B. exe, com, bat und vbs) ist auf den Arbeitsplätzen nicht zugelassen.

8. Abschliessende Bestimmungen

8.1. Änderungen des Reglements

Das Bearbeitungsreglement/Sicherheitskonzept wird gemäss Art. 11 VDSG regelmässig von der Inhaberin der Datensammlung aktualisiert.