

Bearbeitungsreglement Sicherheitskonzept

Inhaltsverzeichnis

1. Versionskontrolle	3
1.1. Änderungskontrolle	3
1.2. Freigabe	3
1.3. Offene Punkte	3
2. Grundlagen und Aufbau	4
2.1. Zielrichtung	4
2.2. Rechtliche Grundlage	4
3. Zuständig- und Verantwortlichkeiten	4
3.1. Organisationseinheiten und Prozessbeschriebe	4
4. Übersicht der Partner	5
5. Allgemeine Datenverarbeitung	5
5.1. Datenverarbeitung durch die Datenannahmestelle	5
5.2. Datenweitergabe nach KVG Art. 84 und Art 84a	5
5.3. Schulung der Mitarbeiter/-innen	5
5.4. Tür- und Fenstersicherung	5
5.5. Aktenführung und Aktenaufbewahrung	5
5.6. Archiv und Aufbewahrungsfristen	6
5.7. Reinigungspersonal	6
5.8. Kundenverkehr	6
5.9. Auskünfte, Datenübermittlung	6
6. Automatisierte Datenverarbeitung	7
6.1. PC-Benutzer/-innen	7
6.2. Kennwörter	7
6.3. Externe Dienstleister/-innen	7
6.4. Arbeitsplatz-PC	7
6.5. Zentrale Rechner (Server)	8

Dateiname: Bearbeitungsreglement.docx
Erstellungsdatum: 24.06.2020
Letzte Änderung: 07.09.2020
Datum: 07.09.2020


6.6. Zentrale Drucker	8
6.7. Faxgerät	8
6.8. Datenverwaltung	8
6.9. Datensicherung	8
6.10. Datenträger	8
6.11. Benutzer/-innen und Rechteverwaltung	8
6.12. Applikationen	8
7. Internet- E-Maldienste	9
8. Abschliessende Bestimmungen	9
8.1. Änderungen des Reglements	9

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

1.2. Freigabe

Datum	Version	Name	Beschreibung
07.09.2020	1.1	Deplazes I.	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 (VD SG) 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 Geheimhaltungs- und Schweigepflicht.

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 Personalchef verfügt über aktuelle Versionen aller Stellenbeschreibungen.

Die Geschäftsführung ist für die ordentliche Anmeldung der Datensammlungen beim EDÖB zuständig.

3.1. Organisationseinheiten und Prozessbeschriebe

Die Organisationseinheiten, die zugehörigen Aufgaben und Prozessbeschriebe sind in einer internen Anwendung definiert und im 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 Rückgriffsrechts 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 Mitarbeiter/-innen

- Die Mitarbeiterinnen und Mitarbeiter 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. Sie sind grundsätzlich in verschlossenen Schränken aufzubewahren.

- 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 sind Schredder vorzusehen.

5.6. Archiv und Aufbewahrungsfristen

- Die Aufbewahrung von Akten im Archiv ist bereichsbezogen durchzuführen.
- 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 sind grundsätzlich zu löschen, wenn sie für die Aufgabenerledigung nicht mehr erforderlich sind und Aufbewahrungsfristen nicht entgegenstehen.
- Die Akten sind einer physikalischen Vernichtung zuzuführen, 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 Verpflchtungsgesetz 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.

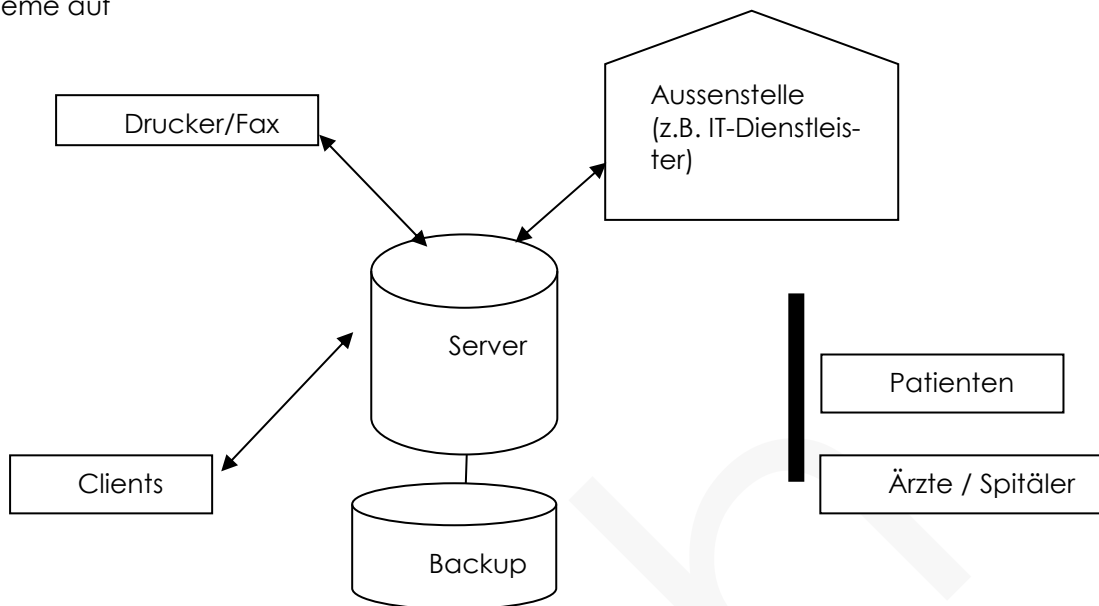
5.9. Auskünfte, Datenübermittlung

Jede Person kann von vita surselva Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Das Auskunftsrecht richtet sich nach Art. 8 und 9 DSGVO sowie Art. 1 und 2 BDSG.

- 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 Um Systeme auf



6.1. PC-Benutzer/-innen

- Die PC-Benutzerinnen und PC-Benutzer sind vor Aufnahme der Arbeit an PCs umfassend zu schulen. Ihnen sind entsprechende Handbucher zur Verfugung zu stellen.
- Die PC-Benutzerinnen und PC-Benutzer sind selbst fur die ordnungsgemasse Nutzung der ihnen zur Verfugung gestellten Hard- und Software zustandig.
- Sie sind uber die grundsatzlichen Datensicherungsmaassnahmen aufzuklaren.

6.2. Kennworter

- Fur alle PC-Benutzerinnen und PC-Benutzer sind Zugangskennungen fur das Netzwerk und fur die Verfahren zu vergeben.
- Dabei sind neben Benutzernamen auch Kennworte zu verwenden.
- Nicht erfolgreiche Anmeldeversuche sind aufzuzeichnen

6.3. Externe Dienstleister/-innen

- Der Leistungsumfang externer Dienstleisterinnen und Dienstleister ist durch schriftlichen Vertrag zu regeln.
- Die Dienstleisterinnen und Dienstleister sind zu verpflichten, Daten, die ihnen durch ihre Tatigkeit fur die vita surselva bekannt werden, vertraulich zu behandeln.
- Fernadministration hat auf gesicherten Leitungen zu erfolgen.
- Die Leitungen sind nach Ende der Tatigkeit wieder zu sperren.

6.4. Arbeitsplatz-PC

- Beim Auf- oder Umstellen der Gerate ist auf geeignete Standorte (Lichtverhaltnisse, 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 fur die dienstliche Aufgabe notwendigen Funktionen und Anwendungen zu installieren. Die Entscheidung hieruber 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 einer Serverakte zu dokumentieren.

6.6. Zentrale Drucker

- Beim zentralen Drucker ist darauf zu achten, dass Ausdrücke 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 in der Systemakte zu dokumentieren.

6.10. Datenträger

- Externe Datenträger (Disketten, USB-Sticks, externe Festplatten) sind vor ihrem Einsatz durch bevollmächtigte Mitarbeiter/innen 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. Benutzer/-innen und Rechteverwaltung

- Es ist eine Auflistung über PC-Benutzerinnen und PC-Benutzer und den ihnen zugewiesenen Rechten zu erstellen.
- Benutzerinnen und Benutzer sind ausschliesslich auf den Zentralrechnern einzurichten.
- Zur Vereinfachung der Rechtezuweisung sind Benutzergruppen zu bilden.
- Den Benutzerinnen und Benutzern 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 Lieferantinnen abgelegt. Die Unterlagen bezüglich des Betriebes sind bei der vita surselva in der Applikation selber integriert.

Die Schnittstellenbeschreibungen sind im Konformitätsnachweis in folgenden Spalten ersichtlich:

- Herkunft der Daten: Spalte „f“
- Empfänger der Daten: Spalte „g“

- Periodizität der Datenweitergabe: Spalte „h“
- Zweck der Datenweitergabe: Spalte „i“
- Medium der Datenweitergabe: Spalte „j“
- Zweck der Datenbearbeitung: Spalte „k/l“

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 Attachments (Dateien) sind einer Virenüberprüfung zu unterziehen. Die dazu eingesetzte Virenschutzsoftware ist täglich zu aktualisieren
- Attachments 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