Bearbeitungsreglement zum DSM der Krankenkasse Visperterminen

Datum	Version	Kommentar	Autor
30.11.2012	0.1	Erstellt	Bernardo Briggeler
09.12.2013	0.2	Passwortänderung pro Quartal	Bernardo Briggeler
30.04.2014	0.3	Anpassungen gemäss Empfehlung KPMG	Bernardo Briggeler
10.02.2016	0.4	Anpassungen gemäss zwischen Audit KPMG	Bernardo Briggeler
09.05.2017	0.5	Anpassungen gemäss Rezertifizierungsaudit KPMG	Bernardo Briggeler
04.09.2017	0.6	Anpassungen gemäss zwischen Audit KPMG	Bernardo Briggeler
06.05.2019	0.7	Anpassungen gemäss Audit KPMG	Bernardo Briggeler
11.7.2019	0.8	Ergänzung Sanktionswesen	Bernardo Briggeler

Inhaltsverzeichnis Bearbeitungsreglement

1. interne Organisation

Verantwortlichkeiten

Die Gesamtverantwortung für den Datenschutz trägt das Leitungsorgan. Diese Verantwortung ist nicht übertragbar.

Für die Umsetzung des Datenschutzes im Betrieb ist im DSM Good Priv@cy geregelt.

Für IT-Themen wie das Betriebssystem, Anwendungen, die Datenbank, das Netzwerk und die Datensicherheit ist im DSM Good Priv@cy geregelt.

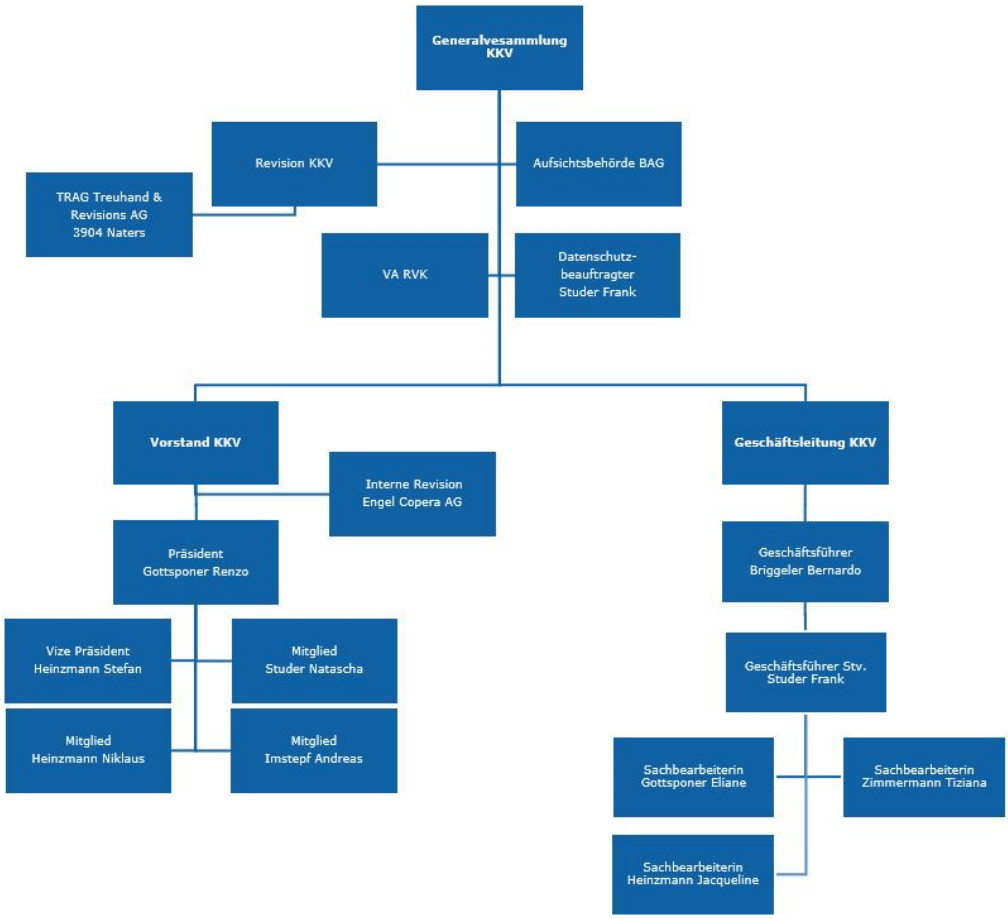
Der betriebliche Datenschutzverantwortliche kontrolliert die Einhaltung des Datenschutzes, berät die Geschäftsleitung und die Mitarbeitenden und unterstützt bei der operativen Umsetzung des Datenschutzes im Betrieb.

Kontaktstelle bezüglich datenschutzrechtlichen Fragen

Fragen in Zusammenhang mit dem Datenschutz sind an folgende Stelle zu richten:

Bernardo Briggeler
Geschäftsführer
3932 Visperterminen
027 948 00 50, kkv@visperterminen.ch

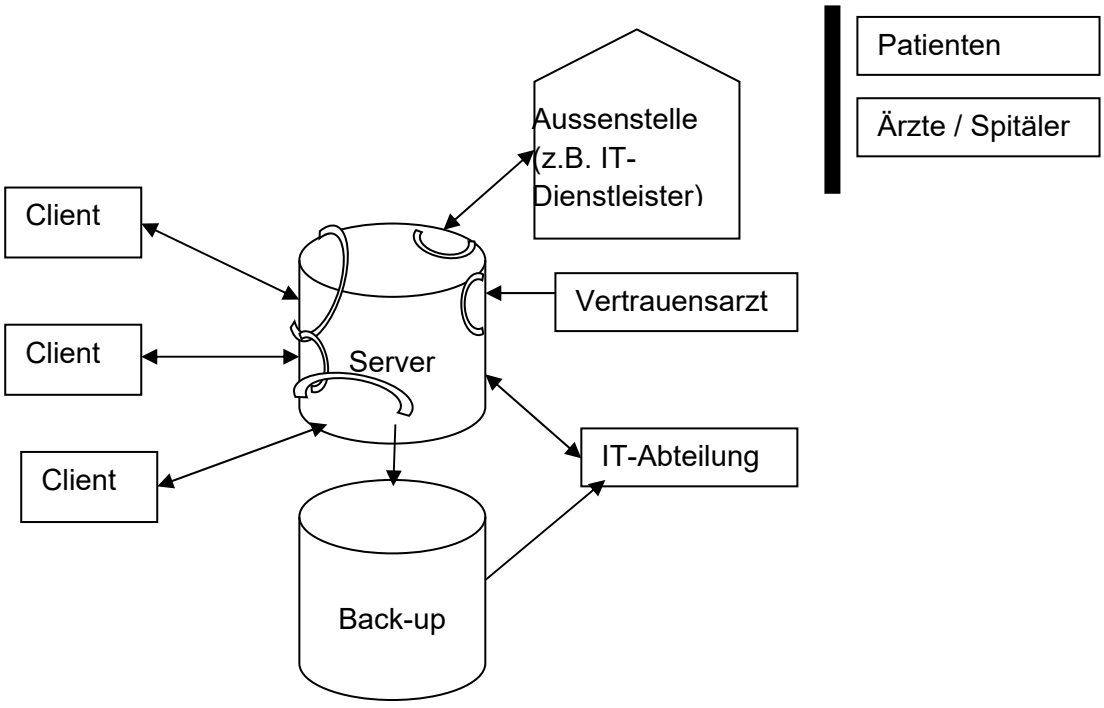
Organigramm



Die Krankenkasse Visperterminen beschäftigt 5 Mitarbeitende.

2. IT-Struktur

Die nachfolgende Grafik zeigt die IT Struktur auf, in welche das automatisierte Datenbearbeitungssystem eingegliedert ist.



Die Mitarbeitenden können via ihren Computer (Client) auf die Daten auf dem Server zugreifen, die sie für die Erfüllung ihrer Aufgaben brauchen. Alle Daten werden auf einem Back-up-Server sicherheitsgespeichert (dupliziert). Lediglich die Geschäftsleitung kann auf die Back-ups zugreifen. Die Back-ups sind mit einem Passwort geschützt. Der Vertrauensarzt kann auf die Daten zugreifen, die er für die Erfüllung seiner Aufgabe braucht. Die Mitarbeitenden der Krankenkasse können nicht auf die Daten des Vertrauensarztes zugreifen.

Weder die Patienten noch die Ärzte resp. Spitäler können auf die Daten zugreifen.

Eingesetzte Informatikmittel

Bei der Krankenkasse Visperterminen werden für die allgemeinen Textverarbeitungen das Microsoft Office Programm, für die Buchhaltung das Sesam Sage 50, für sämtliche Versicherungsdaten das BBT Programm BBTI verwendet, für Betreibungen das Collecta eSchKG und für das DSM und das QM wird der QM Pilot eingesetzt.

Integrierte Systeme

MediData: Elektronische Rechnungsübermittlung und –prüfung anhand von aktuellen Tarif- und Referenzdaten.

surplusREADER (IT-Surplus GmbH): Scanning-Software welche Dokumente beim Scannen automatisch klassifiziert und identifiziert.

CaseNet (MedCasePool RVK): Webapplikation zum sicheren Austausch von vertrauensärztlichen Daten an den unabhängigen Vertrauensarzt.

Zertifizierte Datenannahmestelle (BBT Software AG): Für die Entgegennahme, Prüfung und Weiterverarbeitung von DRG-Rechnungen gelten die Bestimmungen von Art. 59a KVV. Zur Erfüllung dieser gesetzlichen Vorgaben ist die Krankenkasse Visperterminen der zertifizierten Datenannahmestelle (zDAS) der BBT Software AG angeschlossen.

Schnittstellen

Schnittstellen bei der Datenbearbeitung sind im Konformitätsnachweis enthalten. Der aktuelle Konformitätsnachweis kann beim Geschäftsführer eingesehen werden.

3. Zugriffe

Zugriffsdifferenzierung

Es werden nur die notwendigsten Zugriffsrechte auf Netzwerke, Programme und Daten an Benutzer vergeben. Jeder Mitarbeitende erhält nur Zugriff auf genau diejenigen Daten, die er zur Erfüllung seiner Aufgabe unbedingt braucht.

Der Geschäftsführer entscheidet über die Vergabe und den Umfang der Zugriffsrechte. Sie entscheidet anhand der in der Weisung bezüglich Vergabe und Umfang der Zugriffsrechte definierten Regeln. Die Zugriffrechte sind auf die Funktion und Tätigkeitsfelder jeder Person zugeschnitten. Des Weiteren wird für jede Berechtigung entscheiden, ob eine Leseberechtigung genügt, oder Änderungsberechtigungen vergeben werden müssen.

Die Zugriffsrechte sind im Detail in der Zugriffsliste pro Mitarbeitenden festgehalten. Die Liste wird regelmässig durch das Management überprüft.

Authentisierung durch Passwörter

Der Mitarbeitende hat eine persönliche Identifikation (Benutzername) und ein Passwort. Die Weitergabe des persönlichen Passworts ist untersagt.

Die Weisung bezüglich der Zusammensetzung der Passwörter (Anzahl Stellen, Sonderzeichen etc.) liegt schriftlich vor und ist allen Mitarbeitenden bekannt.

4. Datensicherheit

Für die Gewährleistung der Datensicherheit d.h. dem Schutz von Daten während der Datenverarbeitung, -speicherung oder –transport vor Verlust, Zerstörung, Verfälschung, unbefugter Kenntnisnahme und unberechtigter Verarbeitung, werden folgende Massnahmen angewendet:

Organisatorische Massnahmen

- Es bestehen Informationsschutz- und Sicherheitsrichtlinien. Die Einhaltung wird durch die Geschäftsleitung jährlich geprüft.
- Erstellung von Sicherheitskopien auf einem separaten Speichermedium.
- Getrennte Aufbewahrung der Sicherheitskopien.
- Alle Computer sind passwortgeschützt.
- Mindestens 8-stellige Passwörter, die folgende Merkmale aufweisen müssen: [*mindestens ein Sonderzeichen, mindestens eine Zahl, Gross und Kleinschreibung*].
- Automatische Bildschirmsperrung nach 5 Minuten ohne Aktivität.
- Clean Desk Policy
- Alle Mitarbeitenden werden jährlich auf die Themen Datenschutz und Datensicherheit geschult.
- Die Mitarbeitenden der IT bilden sich regelmässig in Security Themen weiter.

Technische Massnahmen

- Es besteht ein Back-up-Konzept.
- Ein Firewall ist eingerichtet und wird mindestens monatlich aktualisiert.
- Virenprüfung: die IT-Abteilung ist verantwortlich, dass alle Computer immer über den aktuellsten Virenschutz verfügen.
- Plattenspiegelung: Der Datenbestand einer Festplatte wird nach jeder Veränderung auf eine zweite Festplatte kopiert.
- Vertrauliche Daten werden nur per Post oder verschlüsselter E-Mail übermittelt.
- Zutrittskontrollen zum Rechenzentrum und Dokumentation der Zutritte.
- Das Rechenzentrum befindet sich in einem Sicherungsraum.

5. Interne und externe Kontrollen

In Ergänzung zu Kapitel 4 „Datensicherheit“ sind folgende Massnahmen Kontrollen im Unternehmen implementiert:

Die Einhaltung der datenschutzrechtlichen Bestimmungen wird **intern** folgendermassen sichergestellt und kontrolliert:

Massnahmen auf Unternehmungsebene

- schriftlich festgehaltene Datenschutzpolitik, die allen Mitarbeitenden bekannt ist.
- Datenschutz- und Datensicherheitsrichtlinien resp. –konzept
- Regelungen von Aufgaben, Verantwortlichkeiten und Kompetenzen bezüglich Datenschutz und Datensicherheit in den Pflichtenheften der Mitarbeitenden.
- Thematisierung des Datenschutzes und der Datensicherheit in allen Stellenbeschreibungen und Arbeitsverträgen.
- Die Zugänge zu den Büros sowie zum Archiv sind gesichert.
- *jährlich* Schulung aller Mitarbeitenden bezüglich Datenschutz und Datensicherheit.
- Weisungen betreffend Umgang mit E-Mail und Telefon.
- Das System zeichnet die Zugriffe auf Daten, den Zeitpunkt sowie den Umfang der Zugriffe (lesen, verändern etc.) auf.

Kontrollen durch das Management

Das Leitungsorgan und die Geschäftsleitung nehmen ihre Führungs- und Überwachungsaufgaben durch folgende Kontrollen war:

- Prüfen der Bereiche der Internen Kontrolle und Ableiten von Massnahmen.
- Prüfung der Umsetzung der Datenschutzpolitik.
- Sorgfältige Auswahl und Instruktion aller externer Dienstleister, die auf Daten zugreifen können oder an denen Daten weitergegeben werden.
- Verfassen von Datenschutz- und Datensicherheits-Vertragsklauseln mit allen Dienstleistern, die auf Daten zugreifen können oder an denen Daten weitergegeben werden sowie Kontrolle, ob die Dienstleister die Vorschriften bezüglich Datenschutz und Datensicherheit einhalten.
- Periodisch Prüfung der Zugriffsrechte sowie des Umfangs der Zugriffsrechte jedes Mitarbeitenden anhand der Zugriffsliste.
- Auswertung der Systemaufzeichnungen bezüglich Zugriffe auf Daten, Zeitpunkt sowie Umfang der Zugriffe und Abgleich mit der Zugriffsliste.

Des Weiteren lebt das Management seine Vorbildfunktion aktiv und täglich und stellt die notwendigen Mittel für die kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit bereit.

Kontrollen auf Prozessebene

- Prüfung der Konformität vor Einrichtung einer Datensammlung und Dokumentation im Konformitätsnachweis.
- jährliche Kontrolle des Konformitätsnachweises (Vollständigkeit, Korrektheit, ist die Datenbearbeitung immer noch zweckmässig? Ist der Empfänger der Daten noch korrekt etc.).
- laufende Prüfung der Personendaten auf Ihre Richtigkeit.

IT-Kontrollen

Der Grossteil der IT-Kontrollen wurde bereits unter „Datensicherheit“ erläutert. Hier sind nur noch die ergänzenden aufgelistet.

- Protokollierung der Eingaben und Veränderungen

Interne Audits

- jährliche Kontrolle durch den betrieblichen Datenschutzbeauftragten.
- jährliche Kontrolle durch die Interne Revision

Diese Kontrollen sind in das umfassende Interne Kontrollsystem des Unternehmens integriert.
Diese Kontrollen werden durch folgende externe Kontrollen ergänzt.

- Audits im Rahmen der zertifizierten Datenannahmestelle, Durchführung: KPMG
- Kontrollen des internen Kontrollsystems (IKS), Durchführung: Engel Copera AG

6. Auskunftsbegehren

Geregelt in: Art. 8ff DSG und Art. 1 ff VDSG

Form, Inhalt und Anschrift

Auskunftsbegehren sind schriftlich zusammen mit einer Kopie der ID oder des Passes an folgende Adresse und Kontaktperson zu senden:

Krankenkasse Visperterminen
Bernardo Briggeler
Dienstleistungszentrum
3932 Visperterminen

Diese Person resp. sein Stellvertreter trägt die Verantwortung für eine termingetreue Bearbeitung des Antrags.

Auskunftsbegehren über die Gesundheit

Daten über die Gesundheit des Gesuchstellers werden an einen vom Gesuchsteller bestimmten Arzt übermittelt, nicht an den Gesuchsteller persönlich.

Prozessablauf

Der interne Prozessablauf ist in der Prozess-Dokumentation gemäss Anhang 8 geregelt.

7. Archivierung und Vernichtung

Archivierungspflichtige Dokumente werden während der gesetzlich verlangten Dauer archiviert und vor Veränderungen oder unbefugten Zugriffen geschützt.

Die Zutritte zum Archiv werden sehr restriktiv vergeben und protokolliert. Die Protokolle werden aufbewahrt.

Nach Ablauf der gesetzlichen Archivierungsfrist werden die Dokumente vernichtet, da die rechtliche Grundlage (Zweckmässigkeit) wegfällt.

Der Ablauf der Aufbewahrung, Archivierung und Vernichtung ist in einem Datenaufbewahrungs- und Archivierungskonzept festgehalten.

Die Aufbewahrungsdauer für jede Datensammlung ist aus dem Konformitätsnachweis im Anhang dieses Bearbeitungsreglements ersichtlich.

8. Verfahren, wenn eine betroffene Person die Bekanntgabe oder Bearbeitung ihrer Daten verbietet

Eine betroffene Person kann die Bekanntgabe oder die Bearbeitung ihrer Daten verbieten.

Beide Begehren sind an folgende Kontaktperson zu richten:

Bernardo Briggeler
Geschäftsführer
Dienstleistungszentrum
3932 Visperterminen

Diese Person resp. sein Stellvertreter trägt die Verantwortung für eine termingetreue Bearbeitung des Antrags.

Das Bearbeitungsreglement ist auf unserer Homepage www.kkv.ch aufgeschaltet und wurde an das EDÖB im Sinne von KVG Art. 84b vorgelegt.

9. Sanktionen

Bei Verstössen gegen die internen Prinzipien, Verhaltensweisen und Richtlinien können Sanktionen ausgesprochen werden. Je nach Schweregrat wird die Geschäftsleitung und/oder der Vorstand informiert.

Verdachtsfälle resp. Verstösse müssen immer gemeldet werden. Dies kann auch in anonymer Form geschehen, wie zum Beispiel mit einem Brief ohne Absender.

Bei Verdachtsfällen auf Verstösse können sich die Mitarbeitenden an die vorgesetzte Person oder an die Mitglieder der Geschäftsleitung wenden. Ist die Klärung der vorgesetzten Stelle oder der Geschäftsleitung nicht möglich oder bleiben weiterhin Bedenken, können sich die Mitarbeitenden den Vorstandspräsidenten oder an ein Mitglied des Vorstands wenden.

Diejenigen Personen, die Verdachtsfälle melden, werden geschützt und auf Wunsch geheim gehalten. Strikte Vertraulichkeit sowie der Verzicht auf Repressalien werden in jedem Fall zugesichert.

Konsequenzen bei Verstössen

Für Mitarbeitende der Krankenkasse Visperterminen können je nach Schweregrat des Verstosses folgende Konsequenzen ausgesprochen werden:

- mündliche Abmahnung
- schriftliche Abmahnung
- ordentliche Kündigung
- fristlose Kündigung
- Geldstrafe bis maximal Fr. 5'000.00

Die Sanktionen werden jeweils laut Mehrheitsbeschluss vom Vorstand der Krankenkasse Visperterminen festgelegt und sind durch die Geschäftsleitung umzusetzen.

Dieses Bearbeitungsreglement tritt per 01.01.2019 in Kraft.

Briggeler Bernardo

Geschäftsführer

Anhang 1: Datenschutzpolitik resp. Datenschutzleitbild

1. Gesetzliche Grundlagen

Zur Aufgabenerfüllung ist es unumgänglich, dass Personendaten von Mitgliedern, Versicherten und Mitarbeitenden speichert, bearbeitet und in bestimmten Fällen weitergeben werden. Die gesetzlichen Bestimmungen werden strikte eingehalten. In verschiedenen Bereichen werden besonders schützenswerte Gesundheitsdaten bearbeitet. Angesichts der Sensibilität dieser Daten und der daraus gewonnen Informationen werden die gesetzlichen Bestimmungen (DSG, KVG und ATSG) für Krankenversicherer eingehalten.

2. Personendaten und Datensammlungen

Personendaten sind Angaben über eine bestimmte oder bestimmbare natürliche oder juristische Person. Datensammlungen sind Bestände von Personendaten, die so aufgebaut sind, dass die Daten nach den betroffenen Personen erschliessbar sind.

3. Daten von Mitgliedern

Die Krankenkasse Vispererminen als Krankenversicherer im Besitz von betriebswirtschaftlichen Daten seiner Mitglieder, die Auskunft über die Risikofähigkeit des einzelnen Mitgliedes geben. Deshalb sind diese Daten schützenswert.

4. Verhältnismässigkeit

Grundlage für die Verarbeitung von Daten ist die Verhältnismässigkeit, was bedeutet, dass nur Daten gespeichert und bearbeitet werden, bei denen eine Rechtsgrundlage vorhanden ist.

5. Bearbeitungsreglement

Die Krankenkasse Visperterminen verfügt über ein Bearbeitungsreglement, welches auf unserer Homepage www.kkv.ch aufgeschaltet ist.

6. MCD Minimal Clinical Datasets

Leistungsbelege inkl. MCD sind besonders schützenswerte Daten und Sie wurden im Rahmen der Kontrollen für die Datenschutz-Governance gemäss der Verordnung über die Datenschutzzertifizierungen (VDSZ, SR 235.13) zertifiziert. Die MCD-Datensätze werden gemäss Klassifizierung 3 vertraulich behandelt.

Aus dieser Datenschutzpolitik ergeben sich die Leitsätze zum Datenschutz.

Anhang 2: Leitsätze zum Datenschutz

Die Erreichbarkeit der Ziele der Krankenkasse Visperterminen hängt unmittelbar von richtigen Daten und den daraus entwickelten Informationen sowie einer zuverlässigen IT-Infrastruktur, welche die Verfügbarkeit garantiert, ab.

- Beim der Krankenkasse Visperterminen werden nur Daten verarbeitet, die richtig und erforderlich sind.

- Vertrauliche und besonders schützenswerte Daten sind vor dem Zugriff Unbefugter geschützt

- Mitarbeitende und Vorstand kennen den Wert und die Bedeutung der Daten und Informationen.

- Mitarbeitende und Vorstand kennen die gesetzlichen Bestimmungen und die internen Richtlinien. Sie handeln danach.

- Berechtigte Mitarbeitende können jederzeit auf die benötigten Daten zugreifen.

- Mitarbeitende und Vorstand gehen verantwortungsvoll mit Daten, Informationen und der IT-Infrastruktur um.

- Mitarbeitende und Vorstand sind in ihrer Funktion für die Schaffung der notwendigen und angemessenen Rahmenbedingungen für den Datenschutz und die Datensicherheit verantwortlich.

- Alle Daten werden ordnungsgemäss gesichert und nach Ablauf der gesetzlichen Aufbewahrungsfrist, oder wenn sie nicht mehr benötigt werden, vorschriftsmässig vernichtet.

Anhang 3: Datenschutzrichtlinien

Betreffend Umgang mit Personendaten im KVG- und VVG-Bereich

Präambel

Die Krankenkasse Visperterminen bearbeitet Informationen über die versicherten Personen in komplexen organisatorischen Abläufen und mit anspruchsvollen technischen Einrichtungen. Mit der Einhaltung der vorliegenden Datenschutzrichtlinien stellt die Krankenkasse Visperterminen sicher, dass die Persönlichkeit der versicherten Personen und deren Grundrechte entsprechend den gesetzlichen Bestimmungen geschützt werden. Gleichzeitig zeigt die Krankenkasse Visperterminen mit den Datenschutzrichtlinien auf, mit welchen Mitteln sie sicherstellt, dass sie ihre Aufgaben datenschutzkonform erledigt.

1 Gesetzliche Grundlage / Geltungsbereich

1.1 Das vorliegende Reglement stützt sich auf
- das Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG),
- die Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSG),
- das Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts vom 6. Oktober 2000 (ATSG),
- die Verordnung über den Allgemeinen Teil des Sozialversicherungsrechts vom 11. September 2002 (ATSV),
- das Bundesgesetz über die Krankenversicherung vom 18. März 1994 (KVG).
- Die Verordnung über die Krankenversicherung vom 27. Juni 1995 (KVV).

1.2 Im Bereich der obligatorischen Krankenpflegeversicherung gehen die Bestimmungen des ATSG und des KVG den Bestimmungen des DSG vor. Die Bestimmungen des DSG gelten subsidiär.

2 Begriffe

2.1 Personendaten (DSG 3a)
Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.

2.2 Betroffene Personen (DSG 3b)
Betroffene Personen sind natürliche oder juristische Personen, über die Daten bearbeitet werden.

2.3 Besonders schützenswerte Personendaten (DSG 3c)
Besonders schützenswerte Personendaten sind Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen.

Insbesondere folgende Daten können Informationen über die Gesundheit einer Person enthalten:

- Aufzeichnungen über den Verlauf einer Behandlung
- Symptombeschreibungen
- Diagnosen
- ärztliche Verordnungen
- ärztliche Berichte / Spitalberichte
- Therapien
- Medikamente
- Überweisungen
- Laborresultate
- Tarifpositionen

- Aufzeichnungen von bildgebenden Verfahren etc.

2.4 Persönlichkeitsprofil (DSG 3d)
Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

2.5 Bearbeiten (DSG 3e)
Bearbeiten ist jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.

2.6 Bekanntgeben (DSG 3f)
Bekanntgeben ist das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen.

2.7 Datensammlung (DSG 3g)
Datensammlung ist der Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind.

3 Sachlicher Geltungsbereich

Dieses Reglement gilt für jede automatisierte und manuelle Bearbeitung von Daten von natürlichen oder juristischen Personen.

4 Personeller Geltungsbereich

Das Reglement gilt für alle Mitarbeiterinnen und Mitarbeiter der Krankenkasse Visperterminen sowie für beigezogene Dritte gemäss Art. 14 DSG, die Zugang zu Gebäude oder Einblick in Personendaten haben.

5 Verantwortung für Umsetzung und Einhaltung des Reglementes

5.1 Datenschutz ist in erster Linie Sache aller Mitarbeitenden der Krankenkassse Visperterminen. Jede Mitarbeiterin und jeder Mitarbeiter ist in ihrem / seinem Zuständigkeitsbereich verantwortlich, dass sie / er das Reglement einhält. Die Krankenkasse Visperterminen kann bei Nichtbeachten des Reglementes Sanktionen arbeitsrechtlicher Natur aussprechen. Im Weiteren können Verletzungen von Auskunfts- und Schweigepflicht zu strafrechtlichen Sanktionen führen.

5.2 Der Geschäftsführer ist verantwortlich, dass er und seine Mitarbeiter das Reglement umsetzen und einhalten. Er ist insbesondere verantwortlich, dass die EDV-Zugriffsrechte der Mitarbeiterinnen und Mitarbeiter richtig definiert werden. Der Geschäftsführer hat die Mitarbeiterinnen und Mitarbeiter auf die Bedeutung des Reglementes und die Folgen von dessen Nichteinhaltung aufmerksam zu machen.

5.3 Für die einzelnen Datensammlungen ist der Geschäftsführer verantwortlich.

5.4 Der Geschäftsleiter überprüft periodisch, ob dieses Reglement den gesetzlichen Anforderungen und den faktischen Gegebenheiten genügend Rechnung trägt und passt es nötigenfalls an.

6 Information und Schulung der Mitarbeiterinnen und Mitarbeiter

6.1 Jede neue Mitarbeiterin und jeder neue Mitarbeiter wird bei Stellenantritt auf die Grundsätze des Datenschutzes, der gesetzlichen Schweigepflicht und der Datensicherheit aufmerksam gemacht.

6.2 Jede Mitarbeiterin und jeder Mitarbeiter hat bei Stellenantritt eine Datenschutzverpflichtung zu unterzeichnen und bestätigt somit die Einsicht in dieses Reglement.

6.3 Die Mitarbeiterinnen und Mitarbeiter werden regelmässig über Neuerungen und Änderungen betr. Datenschutz informiert. Der Geschäftsführer stellt sicher, dass die Mitarbeiterinnen und Mitarbeiter die Bedeutung des Reglementes verstehen und fördern ihr Bewusstsein in Sachen Datenschutz.

7 Bearbeitungsgrundsätze

7.1 Personendaten dürfen nur bearbeitet werden, wenn dies eine gesetzliche Bestimmung vorsieht oder die betroffene Person eingewilligt hat.

7.2 Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

7.3 Bei der Bearbeitung von Personendaten ist das Verhältnismässigkeitsprinzip einzuhalten. Das Verhältnismässigkeitsprinzip verlangt insbesondere, dass nur diejenigen Personendaten beschafft werden, welche sowohl nötig wie auch geeignet sind, um einen bestimmten Zweck zu erreichen.

8 Zugriffsberechtigung

Jede Mitarbeiterin und jeder Mitarbeiter hat nur Zugriff auf die Personendaten, welche sie / er für ihre / seinen Aufgabenerfüllung benötigt.

9 Externe Weitergabe von Personendaten

9.1 Eine externe Weitergabe von Personendaten erfolgt nur an Berechtigte.

9.2 Die Berechtigung wird im Einzelfall von der zuständigen Führungskraft überprüft.

9.3 Zu beachten insbesondere

Art. 84a KVG: Bekanntgabe von Daten

Art. 32 Abs. 2 ATSG und Art. 82 KVG: Verwaltungshilfe

Art. 120 KVV: Informationspflicht der Versicherer

Art. 47 ATSG: Akteneinsicht

10 Akteneinsichtsrecht und Auskunftsrecht der betroffenen Person

10.1 Den versicherten Personen wird im Rahmen von Art. 47 ATSG Akteneinsicht in die sie betreffenden Daten gewährt.

10.2 Die Krankenkasse Visperterminen darf den im Gesetz genannten Personen und Stellen Personendaten auf schriftliches und begründetes Gesuch bekannt geben (Art. 84a KVG).

10.3 Sofern überwiegende Privatinteressen gewahrt bleiben, steht die Akteneinsicht zu:
a) der versicherten Person für die sie betreffenden Daten:
b) den Parteien für Daten, die sie benötigen, um einen Anspruch oder eine Verpflichtung nach dem Sozialversicherungsgesetz zu wahren oder zu erfüllen oder um Rechtsmittel gegen eine auf Grund desselben Gesetzes erlassene Verfügung geltend zu machen:
c) Behörden, die zuständig sind für Beschwerden gegen aufgrund eines Sozialversicherungsgesetzes erlassene Verfügung, für die Erfüllung dieser Aufgabe erforderlichen Daten:
d) der haftpflichtigen Personen und ihrem Versicherer für die Daten, die sie benötigen, um eine Rückgriffsforderung der Sozialversicherung zu beurteilen.

Handelt es sich um Gesundheitsdaten, deren Bekanntgabe sich für die zur Einsicht berechtigte Person gesundheitlich nachteilig auswirken könnte, so kann von ihr verlangt werden, dass sie einen Arzt bezeichnet, der ihr diese Daten bekannt gibt.

Die Krankenkasse Visperterminen gibt den im Gesetz genannten Personen und Stellen (Art. 84 lit. a KVG) Daten und im speziellen Personendaten nur auf schriftliches und begründetes Gesuch hin bekannt.

11 Bearbeitung von Personendaten durch Dritte

Falls die Bearbeitung von Personendaten auf Dritte übertragen wird, bleibt die Krankenkasse Visperterminen für den Datenschutz verantwortlich. Sie sorgt dafür, dass die Personendaten auftragsgemäss bearbeitet werden (Art. 22 VDSG). Diese Stellen sind ebenfalls, gemäss Artikel 4, diesem Reglement unterstellt.

12 Informatiksysteme – IT-Infrastruktur

12.1 **Hardware**
Die bei der KKV installierte oder den Mitarbeitenden zur Verfügung gestellte IT-Infrastruktur darf nur für firmeneigene Zwecke eingesetzt werden. Ihre Konfiguration darf nur nach Rücksprache mit dem Geschäftsführer geändert werden.

12.2 **Software**
Alle auf den IT-Systemen der KKV eingesetzten Programme gehören der KKV. Sie dürfen nicht für firmenfremde Zwecke verwendet werden.

12.3 **Passwörter**
Die Zugriffsmöglichkeit auf Daten und Programme wird mit Passwörtern gesteuert. Die Passwörter werden nach Aufgaben, Verantwortung und Datenklassifizierung individuell verteilt. Jeder Mitarbeitende ist persönlich für das Passwort (Missbrauch usw.) verantwortlich. Eine Weitergabe an Dritte ist nicht gestattet.

Passwörter werden im täglichen Gebrauch für verschiedene Zugriffsberechtigungen benötigt:

- Netzwerk / Server
- Persönlicher Rechner
- E-Mail
- FTP-Server
- Software wie z.B. E-Banking
- Remote-Verbindungen

Die folgenden Regelungen gelten für alle Anwendungen.

12.3.1 **Gestaltung Passwörter**

a) Vorgaben
Das Passwort darf nicht aus einem Wort bestehen, das in irgendeinem Wörterbuch beliebiger Sprache gefunden werden kann. Personennamen sind nicht zulässig.

Das Passwort darf mit dem Benutzernamen oder dem richtigen Namen nichts zu tun haben. Auch vertauschte Buchstaben oder eine andere Reihenfolge sind nicht zulässig.

Angehängte Zahlen bringen keine zusätzliche Sicherheit.

Das Passwort muss Grossbuchstaben an unüblichen Stellen enthalten. Es muss mindestens ein Sonderzeichen wie Zahlen, Satzzeichen oder Zeichen (z.B $_& usw.) verwendet werden.

Das Passwort muss aus mindestens acht Zeichen bestehen.

b) Passwortcheck
Das Passwort kann mit dem KeePass Programm überprüft werden.

Es dürfen nur Passwörter verwendet werden, die mit diesem Check mehr als 60 Bits aufweisen.

12.3.2 **Haftung**

Das persönliche Passwort darf nicht an andere Personen oder Institutionen weitergegeben werden. Wurde das Passwort durch den Benutzer weitergegeben, haftet dieser für den Missbrauch des Passwortes durch Dritte. Das Passwort ist unverzüglich zu wechseln, wenn es unautorisierten Personen bekannt geworden ist.

12.3.3 **Passwortwechsel**

Die Passwörter müssen mindestens viermal jährlich – im Januar, April, Juli und Oktober – geändert werden.

12.4 **Datenspeicherung Server**

Alle Daten auf den Servern werden mittels Veem Backup & Replication Console in einer Cloud gesichert.

Alle Daten und Programme auf dem Server werden täglich auf ein Speichermedium übertragen und stehen in verschiedenen Versionen als Sicherheitskopie zur Verfügung (Generationenprinzip). Aus Sicherheitsgründen werden die Daten zusätzlich extern (d.h. ausserhalb der der Geschäftstelle DLZ) periodisch gespeichert.

12.5 Datenspeicherung Clients

Die Daten und Programme auf den Clients werden nicht automatisch gesichert. Für die Speicherung der Daten und Programme auf dem Client ist jeder Mitarbeitende selbst verantwortlich. Zu diesem Zweck ist auf dem Server ein persönliches Laufwerk eingerichtet, auf das die Daten übertragen werden können, um im automatischen Sicherungslauf berücksichtigt zu werden. Der Zugriff auf das persönliche Laufwerk erfolgt durch das persönliche Login auf dem Server.

12.6 Protokollierung Internet und E-Mail

Der Verkehr über Internet und E-Mail wird protokolliert. Diese Protokolldaten sind nur für den Administrator zur Einsicht freigegeben und werden nicht ausgewertet. Die Daten werden bei jedem Neustart des Servers gelöscht.

12.7 Wartung

Eine regelmässige Wartung der Hard- und Software gewährleistet ein reibungsloses Funktionieren der IT-Infrastruktur.

Für die Problemlösung erhalten die IT-Partner einen Zugang über das Internet (Fernwartung). Die IT-Partner haben Zugang zu allen Teilen der IT-Einrichtungen (Administrator-Passwort). Die vorliegenden Richtlinien gelten deshalb auch für die IT-Partner.

12.8 Virenschutz

Ein Virenscanner mit den aktuellsten Virusdefinitionen gewährt einen ausreichenden Schutz vor allen Virenarten.

12.9 Unberechtigter Zugriff von Dritten

Ein Firewall gewährleistet einen möglichst grossen Schutz vor An- und Zugriffen von unberechtigten Dritten.

13 Internet, E-Mail und Telefon

13.1 Internet

13.1.1 Internetzugang

Auf allen Clients ist ein Internet-Zugang für geschäftliche Zwecke konfiguriert.

13.1.2 Private Nutzung

Die private Nutzung 10 Minuten pro Tag ist gestattet.

Private Online-Chat und Online-Spiele sind ausnahmslos untersagt. Der Down- und Upload von Files und Programmen für private Zwecke ist nicht gestattet (Virengefahr usw.).

13.1.3 Massnahmen

Die KKV behält sich vor, unzulässige Internet-Nutzung durch geeignete Massnahmen zu unterbinden. Eine mögliche Massnahme ist das Sperren von Internet-Seiten, welche keinen geschäftlichen Bezug haben.

13.2 E-Mail

13.2.1 E-Mail-Konto

Jedem Mitarbeitenden wird ein individuelles E-Mail-Konto eingerichtet.

Die private Nutzung 10 Minuten pro Tag ist erlaubt. Private E-Mail-Abonnemente sind nicht zugelassen.

13.2.2 Bewirtschaftung E-Mail-Konto

Die Mailbox muss mindestens dreimal täglich auf neue E-Mails abgefragt werden. Bei Abwesenheit ist der Mitarbeitende für einen Stellvertretung verantwortlich.

13.2.3 Sicherheit

Der E-Mail-Verkehr ist nicht sicher. Dies gilt auch für die Attachments. Für den Versand von empfindlichen Daten müssen zusätzliche Massnahmen zum Schutz der Informationen vorgenommen werden (Verschlüsselung, Passwort-Schutz usw.). Das Passwort darf nicht mit dem gleichen Medium übermittelt werden (Übermittelung z.B. per Telefon, SMS oder anderen Empfänger direkt erreichenden Medien).

Beim Öffnen von Attachments mit den Erweiterung wie *.vbs, *.exe usw. ist Vorsicht geboten. Files von unbekannten Absendern sind, ohne sie zu öffnen, sofort zu löschen.

13.3 Telefon

Jedem Mitarbeitenden wird eine Direktwahl-Nummer eingerichtet. Die private Nutzung ist in einem vertretbaren Rahmen erlaubt. Nicht erlaubt sind private Auslandgespräche und kostenpflichtige Nummern.

14 Verstösse gegen die Richtlinien

14.1 Vorgehen

Ein Verdacht auf Verletzung oder Missbrauch ist dem Geschäftsführer oder Präsidenten zu melden. Nach Rücksprache mit dem Präsidenten werden die notwendigen Massnahmen eingeleitet.

14.2 Auswertung von Protokolldateien

Protokolldateien werden nicht zur Leistungskontrolle oder Überwachung der Mitarbeitenden eingesetzt. Bei Verdacht auf Verletzung oder Missbrauch können jedoch folgenden Protokolldateien ausgewertet werden.

- Protokoll des Verkehrs über Internet und E-Mail
- Protokoll der Telefongespräche

15 Bearbeitung von DRG Rechnungen und MDC

Im Zusammenhang der Bearbeitung der DRG-Rechnungen und MCD gilt das Bearbeitungsreglement der BBT. S. BBT_Bearbeitungsreglement_zDas

16 Vertrauensarzt

Die Übermittlung von Personendaten vom Leistungserbringer an den Vertrauensarzt, die Bearbeitung der Personendaten durch den Vertrauensarzt sowie die Weitergabe von Personendaten vom Vertrauensarzt an die Versicherung ist im Vertrauensarztvertrag sowie Art. 57 KVG geregelt.

Dies bedeutet insbesondere:

- Die Vertrauensärztin und der Vertrauensarzt sind befugt, bei der Arbeit Hilfspersonen beizuziehen.
- Die Hilfspersonen unterstehen dem ärztlichen Berufsgeheimnis.
- Die Vertrauensärztin und der Vertrauensarzt tragen die Verantwortung für die Auswahl, die Instruktion und Überwachung der Hilfspersonen.
- Die Vertrauensärztin und der Vertrauensarzt gewährleisten den vertraulichen Umgang mit den an sie gerichteten oder für sie bestimmten Informationen.
- Für den PartnerPool Vertrauensarzt des RVK gelten die gegenseitig unterzeichneten Verträge.

17 Aufbewahrung und Entsorgung von Personendaten

- Alle Räumlichkeiten, in denen Personendaten aufbewahrt werden, werden gegen unbefugten Zutritt gesichert. Soweit möglich, werden Personendaten unter Verschluss aufbewahrt
- Personendaten werden gemäss den gesetzlichen Aufbewahrungsvorschriften aufbewahrt. Nach Ablauf der Aufbewahrungsvorschriften werden die Personendaten geschreddert oder bei der Kehrichtverbrennungsanlage in Gamsen als Geheimakten vernichten
- Besonders schützenswerte Personendaten in Papierform werden weder dem gewöhnlichen Kehricht noch der Papiersammlung zugeführt. Diese Papiere werden geschreddert.
- Bevor elektronische Datenträger entsorgt werden, müssen sämtliche Informationen nicht wieder lesbar gelöscht werden (mechanische Zerstörung mit Zertifikat).

18 Sicherheit der Räumlichkeiten gegenüber unbefugten Dritten

18.1 Der Zugang der Mitarbeiterinnen und Mitarbeiter zu Räumlichkeiten, in denen ein Zugriff auf Personendaten möglich ist, wird in einem Sicherheitskonzept geregelt.

18.2 Besucher dürfen sich nicht (ev. nur in Anwesenheit einer Mitarbeiterin oder eines Mitarbeiters) in Räumlichkeiten aufhalten, in denen ein Zugriff auf Personendaten möglich ist.

18.3 Räumlichkeiten, in denen ein Zugriff auf Personendaten möglich ist, sind angemessen gegen Einbruch zu sichern.

19 Datenschutzbeauftragte Person

Auskunftsbegehren gemäss Art. 8 DSG wird durch den Geschäftsführer und seine Stellvertretung erledigt. Er leitet eine Kopie des Auskunftsbegehrens an den Vertrauensarzt weiter. Der Vertrauensarzt ist verantwortlich, dass die vertrauensärztlichen Dokumente direkt an die betroffene Person mitgeteilt werden.

Die Krankenkasse Visperterminen bestimmt dafür den Geschäftsführer und seine Stellvertretung welche folgende Aufgaben übernimmt:

- Sie / er prüft alle Verträge und Projekte, die eine Bearbeitung von besonders schützenswerten Personendaten beinhalten.
- Sie / er stellt sicher, dass die Datensammlungen inventarisiert werden, unabhängig davon, ob es sich um eine Datensammlung im Sinne Art. 11 DSG handelt oder nicht.
- Sie / er stellt sicher, dass allfällige Auskunftsbegehren i.S.v. Art. 8 DSG inhaltlich korrekt und termingerecht bearbeitet werden.
- Sie / er ist Ansprechperson gegenüber dem Eidg. Datenschutzbeauftragten.
- Sie / er unterstützt die operativen Einheiten bei der Implementierung der Datenschutz- und Datensicherheitsmassnahmen.

20 Inkrafttreten

Dieses Reglement ersetzt das bestehende Datenschutzgesetz der Krankenkasse Visperterminen vom 1. Juli 2018 und tritt ab dem 1. Januar 2019 in Kraft.

Anhang 4: Checkliste Datenschutz

Präambel

Diese Checkliste gibt eine Übersicht bezüglich des Datenschutzes. Sie basiert auf den Datenschutzrichtlinien der Krankenkasse Visperterminen.

1 Zweck des Datenschutzes

- Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden (= betroffene Personen);
- Schutz der Privatsphäre;
- Schutz vor Missbrauch von persönlichen Daten;
- keine Behinderung der Antrags- und Schadenbearbeitung.

2 Geltungsbereich des Datenschutzgesetzes

- Das Datenschutzgesetz ist grundsätzlich bei jeder Bearbeitung von Daten natürlicher und juristischer Personen anwendbar.
- Unter Datenbearbeitung versteht man das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren und Vernichten von Personendaten.
- Personendaten sind alle Angaben, die sich auf eine bestimmte Person beziehen.
- Ausgenommen sind Daten, die zum ausschliesslichen persönlichen Gebrauch bearbeitet und nicht weiteren Mitarbeitern zugänglich gemacht werden (z.B. persönliche Agenda, privates Notizbuch).
- Das Datenschutzgesetz ist ebenfalls nicht anwendbar auf hängige Zivilprozesse, Strafverfahren und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren (Verfügungen und Einspracheentscheide).

3 Grundsätze der Datenbearbeitung

Rechtmässigkeit	Personendaten dürfen nur rechtmässig beschafft werden (kein Verstoss gegen Normen des Straf- und Zivilrechts). Unzulässig ist etwa die Datenbeschaffung mittels Gewalt, Arglist oder Drohung).
Transparenzgebot	Grundsätzlich sollen Daten nicht heimlich beschafft werden. Für die betroffene Person muss erkennbar sein, wer welche Daten wie bearbeitet.
Verhältnismässigkeit	Es sollen nicht mehr Daten bearbeitet werden, als für die Antrags- und Schadenbearbeitung nötig sind.
Zweckbindungsgebot	Daten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgeschrieben ist. Daten sollen nicht auf Vorrat erhoben werden.
Richtigkeit	Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern.

4 Allgemeine Voraussetzung für Datenbearbeitung

Obschon mit der Datenverarbeitung in die Persönlichkeit der betroffenen Personen eingegriffen werden kann, ist sie rechtmässig (alternative Voraussetzungen):

- bei Einwilligungen der betroffenen Person,
- bei überwiegenden privaten oder öffentlichen Interessen (Rechtfertigungsgrund)
- wenn eine gesetzliche Grundlage besteht.

5 Rechte der betroffenen Personen

Recht auf Berichtigung	Jede betroffene Person kann verlangen, dass unrichtige Daten berichtigt werden. Unrichtig können nur objektive Tatsachen (Geburtsdatum, Krankheit), nicht aber Werturteile sein.
Bestreitungsvermerk	Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so kann die betroffene Person verlangen, dass bei den Daten ein entsprechender Vermerk angebracht wird (insbesondere bei subjektiven Werturteilen wie „Die Person ist depressiv veranlagt.“)
Auskunftsrecht	Jede Person kann vom Inhaber einer Datensammlung (ein Versicherten Dossier gilt als Datensammlung aus der Warte der versicherten Person) Auskunft darüber verlangen, ob und welche Daten über sie bearbeitet werden. Die Auskunft ist schriftlich, in Form eines Ausdrucks oder einer Kopie sowie in der Regel kostenlos zu erteilen. Aufwändige Abklärungen sind entschädigungspflichtig.
Vernichtung oder Anonymisierung von Daten	Betroffene können die Vernichtung oder Anonymisierung von widerrechtlich bearbeiteten oder nicht mehr benötigten Daten verlangen.

6 Datenbearbeitung durch Dritte

Die Krankenkasse Visperterminen kann ohne Einwilligung der betroffenen Person Dritte, z.B. externe Spezialisten, Datenverarbeiter beauftragen. Der Dritte darf die Daten nur so bearbeiten, wie es der Auftraggeber selber darf (keine Änderung des Bearbeitungszwecks).

7 Bekanntgabe von Personendaten an Dritte

Die Datenweitergabe an Dritte ist ohne Einwilligung der betroffenen Person, überwiegende Interessen oder eine gesetzliche Grundlage nicht statthaft.

Die unbefugte Bekanntgabe von besonders schützenswerten Personendaten (z.B. Gesundheitsdaten) kann strafbar sein.

8 Datentransfer ins Ausland

Daten dürfen ohne Einwilligung der betroffenen Person nicht ins Ausland bekanntgegeben werden, wenn ein Datenschutz fehlt, der dem schweizerischen gleichwertig ist.

Anmeldung der Datensammlungen beim EDÖB

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

Die Konformität jeder einzelnen Datensammlung die Personendaten erhält, wird vor Implementierung sowie kontinuierlich für alle bestehenden Datensammlungen geprüft und im Konformitätsnachweis dokumentiert. Der Konformitätsnachweis befindet sich im Anhang dieses Bearbeitungsreglements.

Dokumentierte Prozessabläufe

Alle Prozessabläufe inkl. Angaben zu Verantwortlichkeiten sind in einem internen QMS definiert und dokumentiert. Einsichtnahmen in Prozesse können bei folgender Person vereinbart werden:

Bernardo Briggeler
Geschäftsführer
Wierastrasse
3932 Visperterminen
027 948 00 50
kkv@visperterminen.ch

Datenfluss

Der Datenfluss wird im Konformitätsnachweis über die Felder „Herkunft“ und „Empfänger“ dokumentiert. Der Konformitätsnachweis befindet sich im Anhang dieses Bearbeitungsreglements.

Anhang 5: Konformitätsnachweis Datensammlung

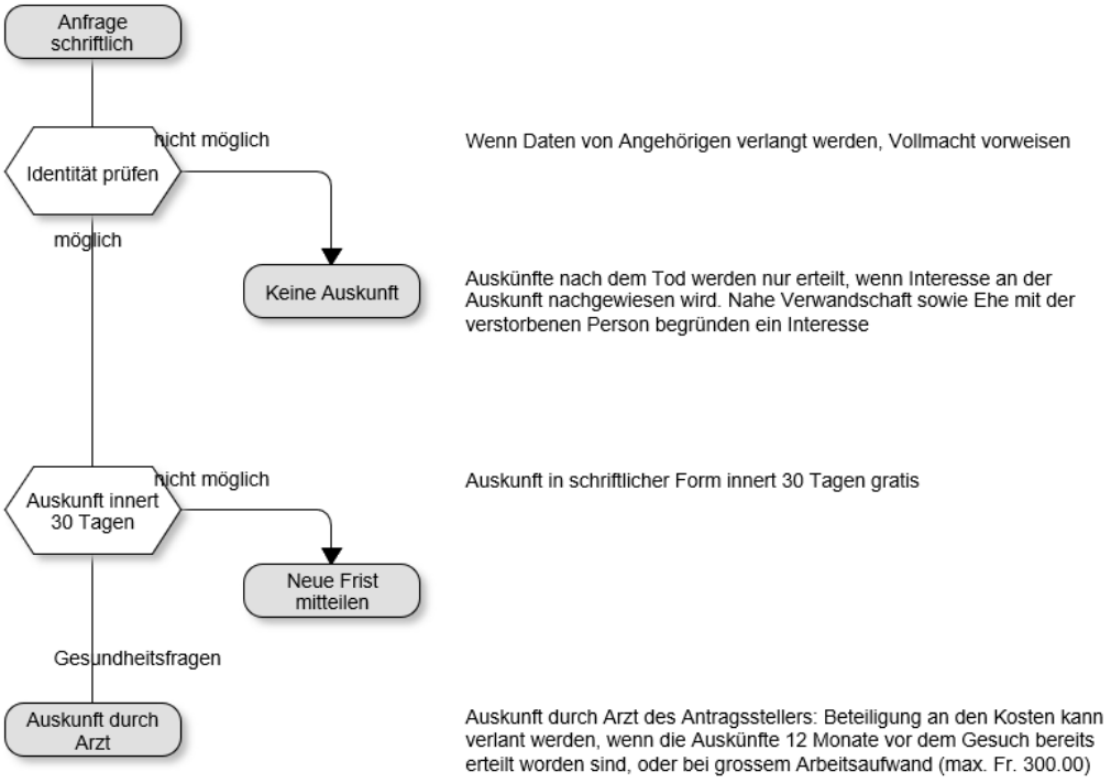
Verhältnismässigkeit			Datenrichtigkeit	Datentransfer Ausland	Outsourcing	Weitergabe an Dritte
Zugriffsberechtigte	**Aufbewahrungsdauer**	**Datenmenge**				
Kapitel 1 – Führung						
elektronisch Passwort- und usergesteuerter Zugriff **Papier** Abgesicherte Räumlichkeiten und abgeschlossene Schränke	10 Jahre	Die Menge der Daten ist aufgrund der Sitzungen beschränkt.	Für die Datenrichtigkeit ist der Protokollführer und der Präsident der KKV verantwortlich. Die Protokolle werden jeweils unterschrieben.	Es werden keine Daten ins Ausland weitergegeben.	Keine Weitergabe der Daten zur Weiterverarbeitung an Dritte	Revisionsstelle Handelsregister
Kapitel 2 - Politik und Strategie						
Keine Daten mit Klassifizierung 3						
Kapitel 3 - Mitarbeiter						
elektronisch Passwort- und usergesteuerter Zugriff **Papier** Abgesicherte Räumlichkeiten und abgeschlossene Schränke	**Lohndaten/Unterlagen Arbeitsverhältnis** 10 Jahre **Akten, die den Mitarbeitenden gehören** Rückgabe oder Vernichtung nach Beendigung des Arbeitsverhältnisses. Nicht benötigte Bewerbungsunterlagen werden mit	Die Anzahl der Personaldossiers entspricht der Anzahl der Mitarbeitenden.	Die Daten basieren auf den Angaben der Mitarbeitenden. Die Mitarbeitenden haben die Möglichkeit, ihre Personal- und Lohndaten jährlich anhand der Lohnabrechnungen zu überprüfen.	Es werden keine Daten ins Ausland weitergegeben.	Keine Weitergabe der Daten zur Weiterverarbeitung an Dritte	**Lohnausfall / UVG** Allianz hat Anspruch auf Personaldaten wie sie im Reglement definiert sind. **Personalvorsorge** AXA Winterthur hat im Rahmen des Vertrages Anspruch

	Absageschreiben zurückgesandt. **Akten, die der KKV gehören** Vernichtung nach 5 Jahren, spätestens nach Beendigung des Arbeitsverhältnisses.		Mit der Unterschrift unter das Mitarbeiterförderungsgespräch und den Arbeitsvertrag von Arbeitgeber und Arbeitnehmer wird die Richtigkeit des Inhaltes bestätigt. Die Mitarbeitenden haben jederzeit die Möglichkeit, in ihr persönliches Personaldossier Einsicht zu nehmen.			auf Personendaten. **AHV/IV/AIV/EO/FAK** Bekanntgabe von der versicherten Lohnsummen **Lohnausweis/ Lohnauskunft** Der Lohnausweis wird nur den Mitarbeitenden abgegeben. Auskünfte werden nur gegenüber der Steuerbehörde und der ALV gegeben.
Kapitel 4 - Partnerschaften und Ressourcen						
Keine Daten mit Klassifizierung 3						
Kapitel 5 - Prozesse						
elektronisch Passwort- und usergesteuerter Zugriff **Papier** Abgesicherte Räumlichkeiten und abgeschlossene Schränke	Die Aufbewahrungsdauer ist in der Datensammlung definiert und beträgt je nach Dokument 2 – 10 Jahre. Bei Dokumenten, bei denen Gesundheitsdaten für weitere Behandlungen notwendig sind, werden diese bis zum Abschluss des Falles, also auch länger als 10 Jahre, aufbewahrt.	Die Datenmenge entspricht den Anzahl Versicherten der KKV. Eine jährliche Durchsicht und Bereinigung der Datensammlung garantiert die Aufbewahrungsdauer und dementsprechend eine vertretbare Datenmenge.	Die Daten basieren bei Personalangaben auf den Angaben der Versicherten. Bei den übrigen Dokumenten basiert die Richtigkeit auf den jeweiligen Verfasser des zugestellten Dokumentes oder Rechnung.	Es werden keine Daten ins Ausland weitergegeben.	Sämtliche Kostengutsprachen, die durch den VA gesetzlich bewilligt werden müssen, werden dem PartnerPool der RVK weitergeleitet und somit von diesem bearbeitet.	Daten, die zur Weiterverarbeitung eines Falles von einer Sozialversicherung oder dem VA benötigt werden. Daten, bei denen eine Vollmacht des Versicherten vorliegt.

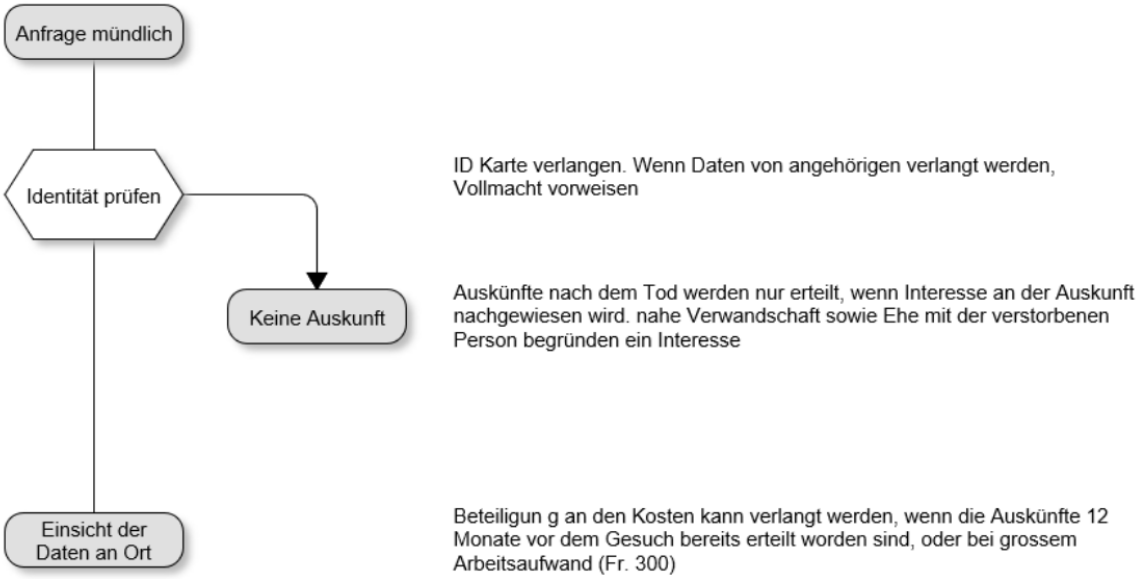
	Bei Todesfällen oder Austritten des Versicherten aus der KKV werden die Daten nach 10 Jahren gelöscht. Verlang der Versicherte nach dem Austritt seine Daten, so werden diese ausgehändigt und anschliessend unwiderruflich gelöscht. Elektronische Daten, bzw. BBTI-Daten, werden nach 10 Jahren automatisch im System gelöscht MCD Minimal Clinical Datasets – Keine Aufbewahrung		Für interne Dokumente ist jeweils der Verfasser der KKV verantwortlich.			Prämienangabe zur Berechnung der Subventionen an die kantonale Steuerverwaltung.

Anhang 6: Prozessablauf Auskunftsbegehren

Prozessablauf Auskunftsbegehren schriftlich



Prozessablauf Auskunftsbegehren mündlich



10. Anhang 7: Checkliste Dokumente

Im Rahmen dieses Bearbeitungsreglements wird auf diverse Dokumente verwiesen. Diese Checkliste gibt einen Überblick über alle erwähnten Dokumente die vorhanden sein müssen.

Dokument	Vorhanden?
Organigramm	
Datenschutzpolitik	
Datenschutz- und Datensicherheitsrichtline / -konzept	
Konformitätsnachweis	
Weisung bezüglich Vergabe und Umfang von Zugriffsrechten	
Weisung bezüglich Zusammensetzung der Passwörter	
Weisung bezüglich Umgang mit E-Mail und Telefon	
Dokumentation der Prozessabläufe (QMS)	
Dokumentation der IT-Struktur	
Informationsschutz- und Sicherheitsrichtlinie	
Back-up-Konzept	
Pflichtenhefte der Mitarbeitenden inkl. Angaben über Aufgaben, Verantwortlichkeiten und Kompetenzen bezüglich Datenschutz und Datensicherheit.	
Schriftliche Arbeitsverträge inkl. Regelungen bezüglich Datenschutz und Datensicherheit.	
Dokumentiertes Internes Kontrollsystem	
Datenaufbewahrungs- und Archivierungskonzept	
Übersichtsliste Zugriffsrechte / Mitarbeitender	
Kopien der Anmeldungen von Datensammlungen an den EDÖB	
Weisungen im Umgang mit Informatikmittel	
Information an Mitarbeitenden bezüglich Kontrollmassnahmen und Monitoring.	