Bearbeitungsreglement Datenschutz

Externes Dokument

Versionierung

Betreff	siehe Abstrakt
Autoren	mem
letzte Bearbeitung	mem
Versionsnr.	V9
Freigabe am	14.01.2021

Verteiler

GL rhenusana
CSO / CIO
Mitarbeiter rhenusana - zDAS

Ansprechperson

rhenusana
CSO / CIO
Widnauerstrasse 6
9435 Heerbrugg

Abstrakt

Regeln und Richtlinien zur Einhaltung des Datenschutzes für Mitarbeiterinnen und Mitarbeiter der rhenusana.

Inhaltsverzeichnis

1 Allgemeiner Teil

1.1 Beschreibung des Unternehmens

Die rhenusana – die rheintaler krankenkasse, nachfolgend rhenusana genannt, ist eine Krankenversicherung gemäss KVG, die sich seit 1944 kompetent und zuverlässig für ihre Mitglieder einsetzt. Sie bietet Familien wie auch Einzelpersonen einen umfassenden Schutz in der Krankenversicherung (KVG) sowie diverse Versicherungen im Zusatz-Bereich (VVG) an.

1.2 Interessierte Parteien

Die interessierten Parteien sind das EDÖB, BAG und die Versicherten.

1.3 Rechtliche Grundlagen

Als Grundlage der Bearbeitung von Personendaten gilt Art. 84 KVG und sieht ebenjene Bearbeitung durch Dritte ausdrücklich vor. Die Information der betroffenen Personen durch den Drittanbieter ist nicht erforderlich. Dies übernimmt die rhenusana in den Allgemeinen Versicherungsbedingungen. Für die automatisierte Datenbearbeitung im Rahmen der Swiss DRG wurden nachfolgende Gesetze und Verordnungen berücksichtigt:

- Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992
- Verordnung zum Bundesgesetz über Datenschutz (VDSG) vom 14. Juni 1993
- Verordnung über Datenschutzzertifizierung (VDSZ) vom 28. September 2007
- Verordnung über die Krankenversicherung (KVV) vom 27. Juni 1995 insbesondere Artikel 59a

1.4 Informationspflicht

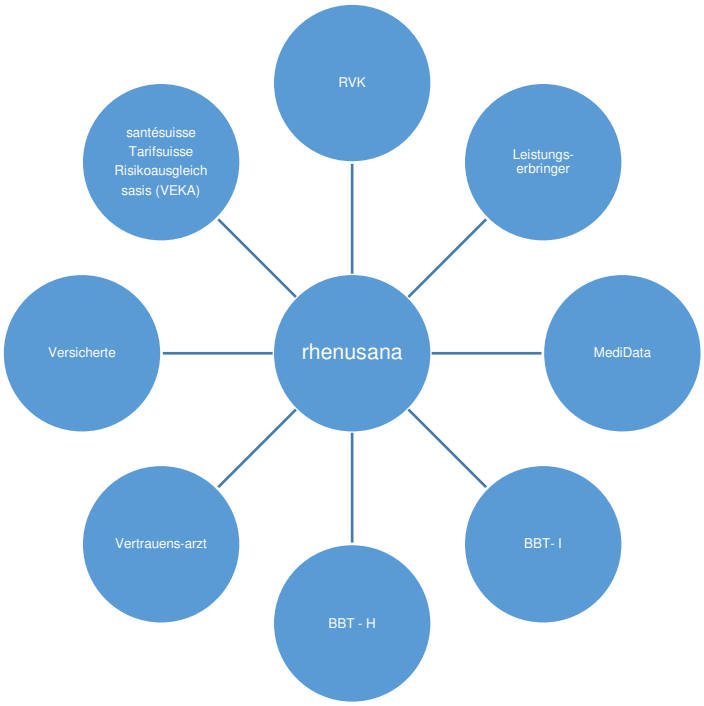
Als Datensammlung gelten nach Art. 3 lit. g DSG ein Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenenen Personen erschliessbar sind. Gemäss Art. 14 Abs. 5 i.V.m. Art. 9 Abs. 1 lit. a DSG besteht eine Ausnahme von der Informationspflicht für Krankenkassen, die eine Datenannahmestelle betreiben, gegenüber den betroffenen Personen.

Das externe Bearbeitungsreglement wird im Sinne von Art. 11 und Art. 21 VDSG i.V.m. Art. 84b KVG auf der Homepage der Krankenkasse (www.rhenusana.ch) veröffentlicht.

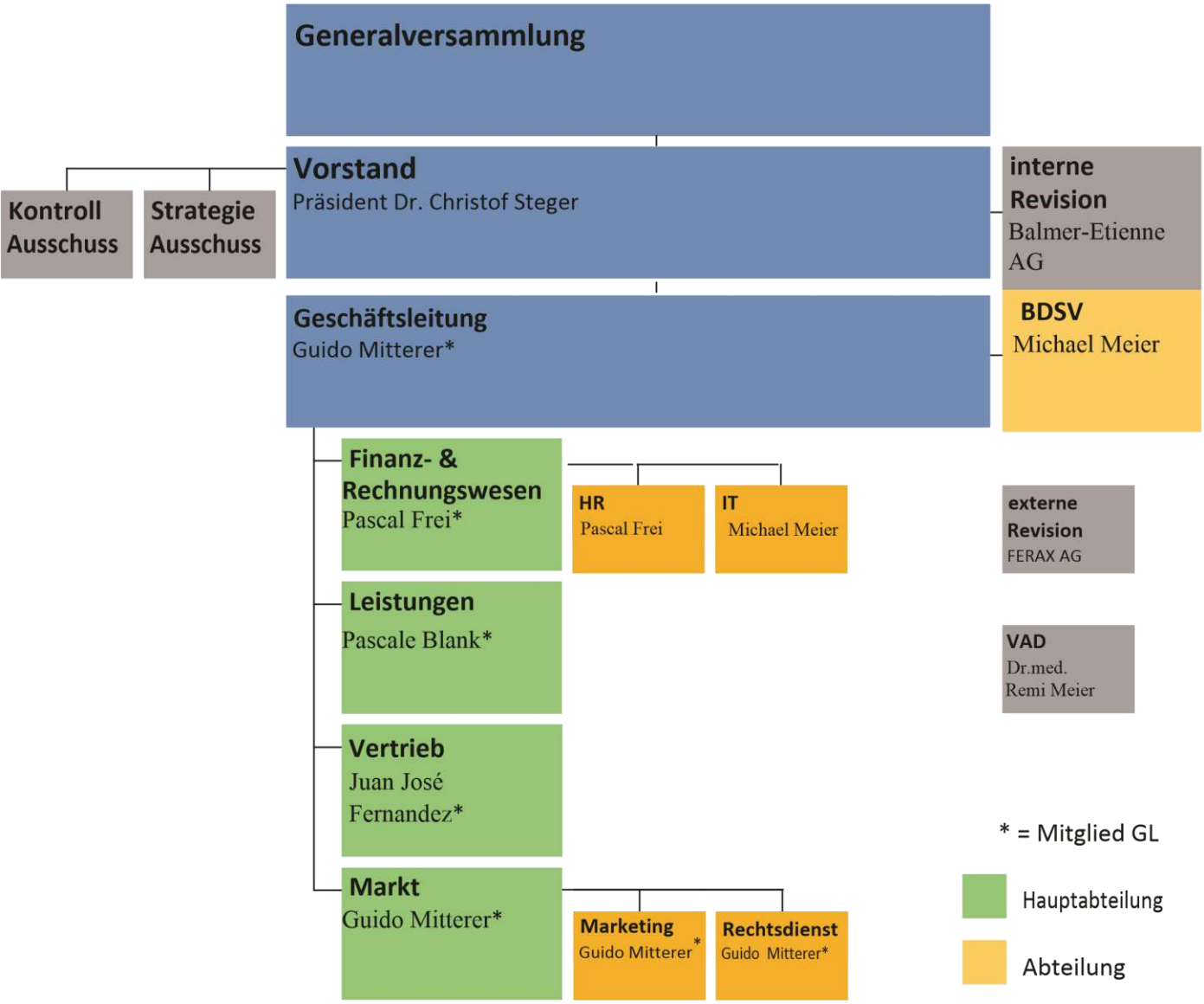
2 Organisation

2.1 Das System

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



2.2 Organigramm rhenusana — Organisation per 01.01.2021



2.3 Verantwortlichkeiten

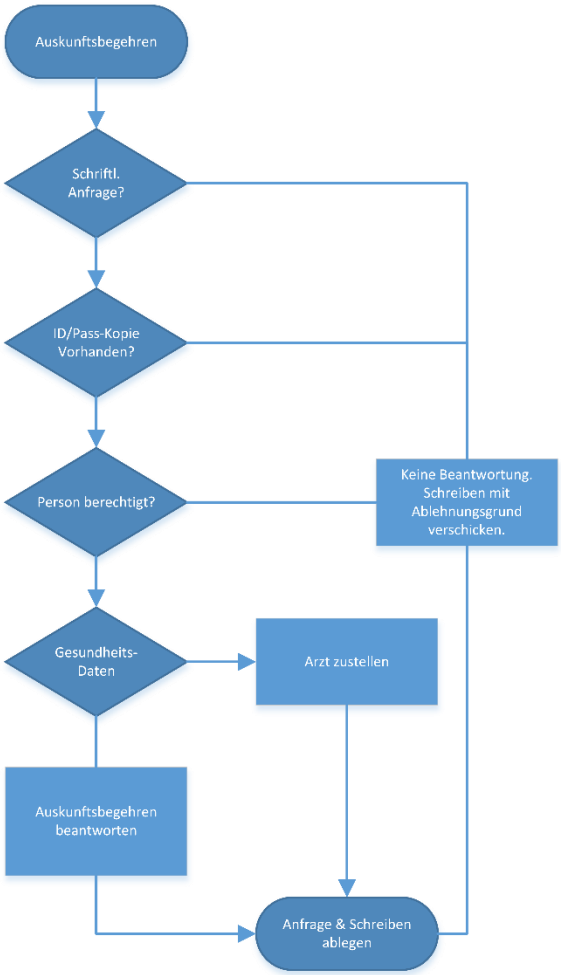
Die Gesamtverantwortung für den Datenschutz trägt die Geschäfts- und Bereichsleitung. Diese Verantwortung ist nicht übertragbar. Für die Umsetzung des Datenschutzes im Betrieb ist der CEO verantwortlich. Für IT-Themen wie das Betriebssystem, die Anwendungen, die Datenbank, das Netzwerk und die Datensicherheit ist CSO/CIO verantwortlich. Der betriebliche Datenschutzverantwortliche kontrolliert die Einhaltung des Datenschutzes, berät die Geschäftsleitung und die Mitarbeitenden und unterstützt die operative Umsetzung des Datenschutzes im Betrieb. Alle weiteren Aufgaben, Kompetenzen und Verantwortlichkeiten betreffend Datenschutz und Sicherheit sind in den entsprechenden Funktionsbeschreibungen festgehalten. Die Geschäftsleitung verfügt über aktuelle Versionen aller Funktionsbeschreibungen. Kontaktstelle bezüglich datenschutzrechtlichen Fragen

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

rhenusana
Betrieblicher Datenschutzverantwortlicher
Widnauerstrasse 6
9435 Heerbrugg

2.4 Prozessabläufe

Die internen Prozessabläufe sind in den Prozess-Dokumentationen geregelt.



2.5 Anmeldung der Datensammlungen beim EDÖB

Da die rhenusana 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.

2.6 Auskunftsbegehren

Nach Art. 8ff DSG und Art. 1 ff VDSG

2.6.1 Form, Inhalt und Anschrift

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

rhenusana
Betrieblicher Datenschutzverantwortlicher
Widnauerstrasse 6
9435 Heerbrugg

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

2.6.2 Auskunftsbegehren über die Gesundheit

Daten über die Gesundheit des Gesuchstellers werden an den Vertrauensarzt der rhenusana (Dr. med. R. Meier, Heerbrugg) übermittelt, nicht an den Gesuchsteller persönlich.

2.7 Kontrollverfahren

2.7.1 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 Funktionsbeschreibungen und Arbeitsverträgen.
- Die Zugänge zu den Büros sowie zum Archiv sind gesichert.
- jährliche Schulung aller Mitarbeitenden bezüglich Datenschutz und Datensicherheit.
- Weisungen betreffend Umgang mit E-Mail und Telefon. (Nutzungsbestimmungen für die IT-Infrastruktur)
- Das System zeichnet die Zugriffe auf Daten, den Zeitpunkt sowie den Umfang der Zugriffe auf.

2.7.2 Kontrollen durch die Geschäftsleitung

Die Bereichsleiter und die Geschäftsleitung nehmen ihre Führungs- und Überwachungsaufgaben durch folgende Kontrollen war:

- Periodische Prüfung der Bereiche der internen und externen Kontrollen und Ableiten von Massnahmen im Management Review.
- 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.

Des Weiteren lebt die Geschäftsleitung ihre 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.).
- Alle 2 Jahre Prüfung der Personendaten auf Ihre Richtigkeit.
- Jährliche Kontrolle der Zugriffsberechtigungen
- Jährliche Kontrolle des Security Konzeptes
- Jährliche Kontrolle des Aufbewahrungs- und Archivierungskonzepts

2.7.3 IT-Kontrollen

Die Bereichsleiter und die Geschäftsleitung nehmen ihre Führungs- und Überwachungsaufgaben durch folgende Kontrollen war:

- Protokollierung der Eingaben und Veränderungen
- Mindestens Halbjährliche Erneuerung der Passwörter (Mitarbeiter)
- Rechtmässigkeit der Berechtigungen

2.7.4 Interne Audits

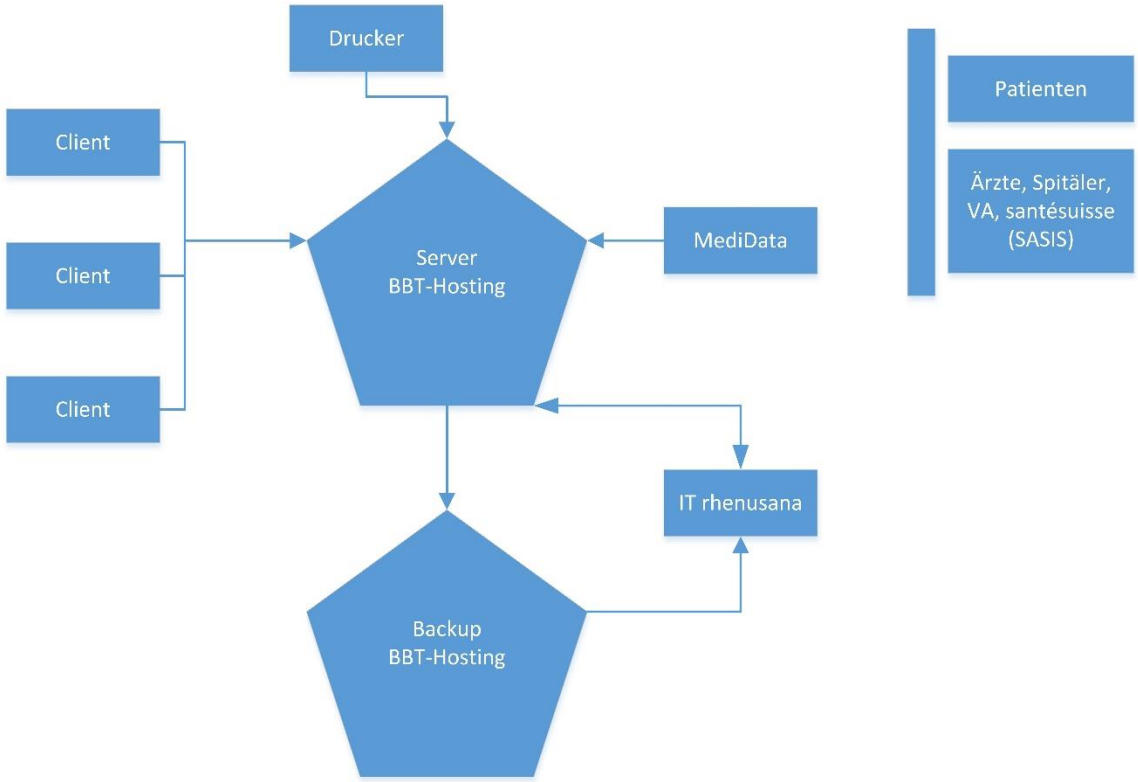
- Jährliche Kontrolle durch den betrieblichen Datenschutzbeauftragten
- Jährliche Kontrolle durch die interne Revision

Diese Kontrollen sind in das umfassende interne Kontrollsystem (IKS) des Unternehmens integriert.

3 IT-System

3.1 Informatikmittel

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



Die Mitarbeitenden können via ihrem Computer (Client) auf die Daten auf dem Server zugreifen, die sie für die Erfüllung ihrer Aufgaben brauchen. Alle Daten werden auf einem Backup-Server sicherheitsgespeichert (dupliziert). Lediglich der IT-Verantwortliche und der Outsourcing Partner BBT - H können auf die Backups zugreifen.

Nur die Hilfspersonen der rhenusana sind berechtigt, auf die Daten des VAD zuzugreifen.

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

3.2 Eingesetzte Informatikmittel

Jeder Mitarbeiter der rhenusana verfügt über eine Arbeitsstation mit Rechner und Bildschirm, sowie die nötigen Eingabegeräte. Die rhenusana bearbeitet Personendaten mit folgender Software (geordnet nach Abteilung):

- BBT individual (Bearbeitung der Versicherten)
- Consolidate (Archivsystem, E-Mail, etc.)
- Microsoft Office (Briefe, Listen, etc.)
- Browser

Zusätzlich Abteilung Finanz- und Rechnungswesen:

- Sage50 (SESAM)
- Banana Buchhaltung
- Swiss Interbanking (Übermittlung LSV)
- Postfinance (Übermittlung DD, EBPP)

Zusätzlich Abteilung Leistungen:

- Surplus Reader (Rechnungen der Leitungserbringer)
- Invoice Inspecter, MediData (Rechnungsprüfung)
- VEKA (Versichertenkarte)
- CaseNet (VAD, CM, DRG)

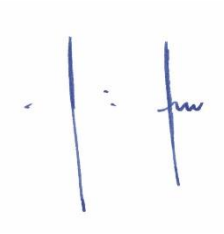
3.3 Schnittstellenbeschreibung

Siehe Anhang A Konformitätsnachweis.

3.4 Glossar

Abkürzung	Beschreibung
BBT - H	BBT - Hosting
BBT - I	Anwendungssystem der rhenusana
CM	Case-Management
DD	Debit Direct
EBPP	E-Rechnungen
EDÖB	Eidgenössischer Datenschutz und Öffentlichkeitsbeauftragter
IKS	Internes Kontrollsystem
IT	Informatik
KVG	Bundesgesetz vom 18. März 1994 über die Krankenversicherung
LSV	Lastschriftverfahren
RM	Risiko-Management
RVK	Verband der mittleren und kleinen
VAD	Vertrauensärztlicher Dienst
VVG	Bundesgesetz vom 2. April 1908 über den Versicherungsvertrag (Versicherungsvertragsgesetz)

Die vorliegende Regelung wird per 2021 in Kraft gesetzt und tritt an die Stelle des vorgängig gültigen Dokuments der rhenusana.



Geschäftsführer CSO / CIO

4 Anhang A Konformitätsnachweis

Konformitätsnachweis

Identifikation	*Inhaber*				*Informationsfluss*				*Zweckmässigkeit*		*Zweckgebundenheit*		*Verhältnismässigkeit*			*Integrität*	*Aufbewahrungsdauer*	
Bezeichnung	Inhaber der Daten-sammlung (Stelle / Organisations-einheit)	Kategorie[1]	Betroffene Person	Bearbeitungs-mittel	Herkunft	Datenempfänger	Zweck der Weitergabe	Medium der Weitergabe	Gesetzliche Grundlage	Einwilligung	Zweck	Warum entspricht dieser Zweck dem Gesetz / der Einwilligung?	Bearbeiter	Anzahl Zugriffs-berechtigte	Wie wird sichergestellt, dass nur so viele Daten wie für die Zweckerreichung wie unbedingt notwendig bearbeitet werden?	Wie wird die Richtigkeit der Daten überprüft?	Gesetzliche Grundlage	Dauer
Active Directory	CIO	A	Mitarbeiter	Server / Netzwerk	Mitarbeiter	CIO / BBT	Auftragserfüllung	JIRA	-	Arbeitsvertrag	Auftragserfüllung		IT / BBT	4	jährliche prüfung durch Dateninhaber	jährliche Prüfung	keine	bis Zweck erreicht
Hardware Inventar	CIO	A	Mitarbeiter	MS Excel	manuelle Erfassung	GL	Auftragserfüllung	-	-	-	Auftragserfüllung		IT / BBT	4	jährliche prüfung durch Dateninhaber	jährliche Prüfung	keine	bis Zweck erreicht
Netzwerk-Dokumentation	CIO	A	Mitarbeiter	MS Excel	manuelle Erfassung	GL	Auftragserfüllung	-	-	-	Auftragserfüllung		IT / BBT	4	jährliche prüfung durch Dateninhaber	jährliche Prüfung	keine	bis Zweck erreicht
Webseite - Rubrik Team	CIO	A	Mitarbeiter	Wordpress	Mitarbeiter	Öffentlich	Auftragserfüllung	Consolidate	-	schriftlich	Auftragserfüllung		IT	öffentlich		jährliche Prüfung	keine	bis Zweck erreicht
Lohndaten	CFO	C	Mitarbeiter	Sage50 Lohn	Mitarbeiter	GL	Auftragserfüllung	physisch	-	Arbeitsvertrag	Lohnerstellung		IT	2		jährliche Prüfung		10 Jahre
Personaldaten	GL	C	Mitarbeiter	MS Office	Mitarbeiter	GL	Auftragserfüllung	physisch		Arbeitsvertrag	diverse Verträge (Arbeitsvertrag, Stellenbeschrieb, usw.)		GL	2				
Mitarbeiter Versicherungsdaten	GL	C	Mitarbeiter	BBT-I	Leistungserbringer	GL	Auftragserfüllung	physisch / elektronisch			Auftragserfüllung		GL / BL	5	Security Konzept ERP System			5 Jahre
Vorstandsdaten	GL	B	Vorstand	MS Office	Vorstand	GL	Auftragserfüllung	physisch	-	Stellenbeschrieb	Auftragserfüllung		GL	2	automatisch durch System	jährliche Prüfung durch Dateninhaber		10 Jahre
Versichertendaten (Adressen, Deckung)	Vertrieb	B	Mitglieder	BBT-I	Vertragspartner	rhenusana	Auftragserfüllung	physisch / elektronisch	KVG / VVG	schriftlich	Auftragserfüllung		rhenusana	alle MA	Security Konzept ERP System			
Versichertendaten (Leistungen)	Leistungen	C	Mitglieder	BBT-I / Surplus Reader	Vertragspartner/Leistungserbringer/Medidata	rhenusana	Auftragserfüllung	physisch / elektronisch	KVG / VVG	KVG Art. 84	Auftragserfüllung	KVG Art. 84	Leistungen	5	Security Konzept ERP System		KVG Art. 84	5 Jahre
PKG Statistiken / Listen	Vertrieb	B	Mitglieder	MS Office	BBT-I / manuelle Erfassung	GL, Vertrieb	Auftragserfüllung	elektronisch	-		Auswertungen / Statistiken		Privatkunden				keine	5 Jahre
PKG Offerten	Vertrieb	B	Mitglieder	BBT-I	Mitglieder	Vertrieb	Vertragserfüllung	E-Mail / physisch					Privatkunden					unbegrenzt
PKG Anträge	Vertrieb	B	Mitglieder	Consolidate / BBT-I	PKG Offerten	Vertrieb	Vertragserfüllung	E-Mail / physisch		Einwilligung auf Eintrag	Vertragserfüllung		alle	alle MA				unbegrenzt
Gesundheitsdeklarationen	rhenusana	B		Consolidate / physisch	Mitglieder	GL / Vertrieb / Leistungen	Auftragserfüllung	physisch		Einwilligung auf Gesundheitsdeklaration	Vertragserfüllung		Privatkunden / Leistungen					unbegrenzt
Adressdaten Partner	rhenusana	A	Vertragspartner	Consolidate	BBT-I / manuelle Erfassung	rhenusana	Auftragserfüllung	elektronisch	-		Auftragserfüllung		alle	alle MA				unbegrenzt

Legende 1) bei Kategorie
A: Personendaten
B: besonders schützenswerte Personendaten
C: Persönlichkeitsprofile