Bearbeitungsreglement Datenschutz

rhenusana
Heinrich-Wild-Strasse 210
9435 Heerbrugg
Tel. 071 727 88 00
Fax 071 727 88 99
E-Mail: info@rhenusana.ch

Ausgabe Mai 2017

Ausgangslage
Dieses Dokument umschreibt Regeln und Richtlinien für die Einhaltung des Datenschutzes der Mitarbeiterinnen und Mitarbeiter der rhenusana.

Inhaltsregister:

1. Beschreibung des Unternehmens

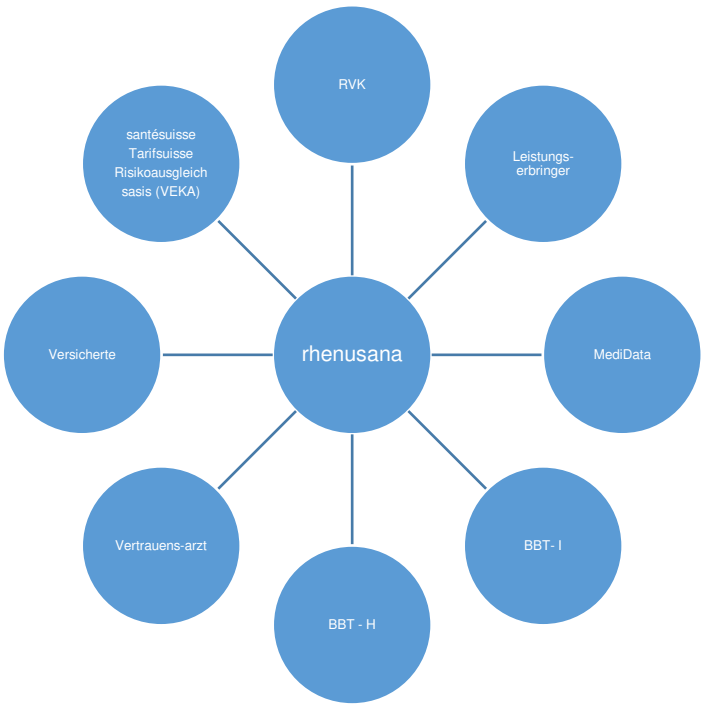
Die rhenusana ist eine Krankenversicherung gemäss KVG, die sich seit über 70 Jahren kompetent und zuverlässig für Einzelpersonen und Firmen einsetzt. Sie bietet Ihren Versicherten einen umfassenden Schutz gegen Krankheit, Mutterschaft und Unfall an.

rhenusana bietet Firmen Kollektiv-Verträge bei den Heilungskosten und der Lohnfortzahlung zu attraktiven Konditionen an. Auch bietet die rhenusana Familien wie auch Einzelpersonen einen umfassenden Schutz in der Krankenversicherung (KVG) und diverse Versicherungen im Zusatz-Bereich (VVG) an.

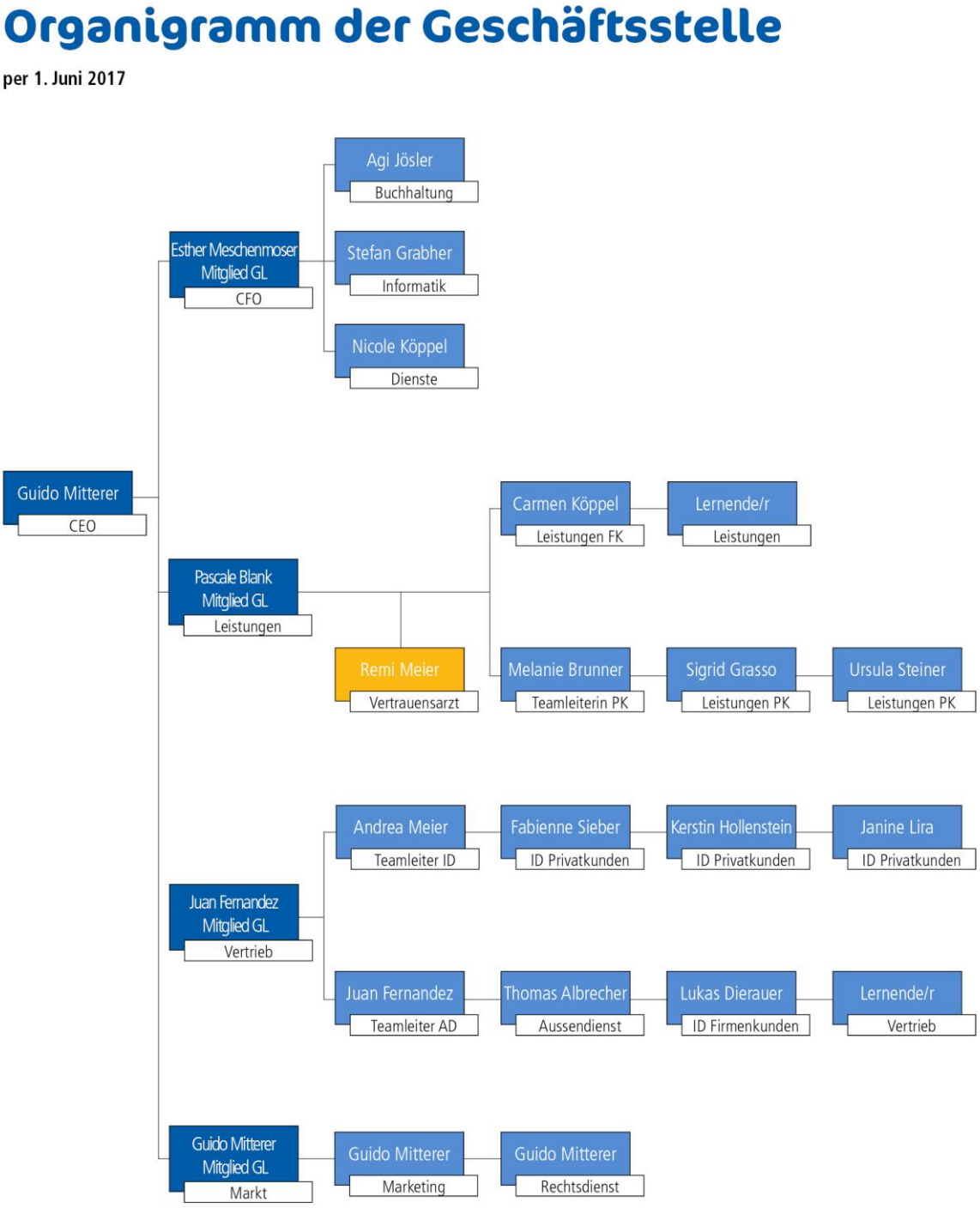
2. Organisation

2.1 Das System

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



2.2 Organigramm



Die rhenusana beschäftigt 21 Mitarbeitende.

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 Guido Mitterer verantwortlich. Für IT-Themen wie das Betriebssystem, die Anwendungen, die Datenbank, das Netzwerk und die Datensicherheit ist CSO/CIO Stefan Grabher 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.

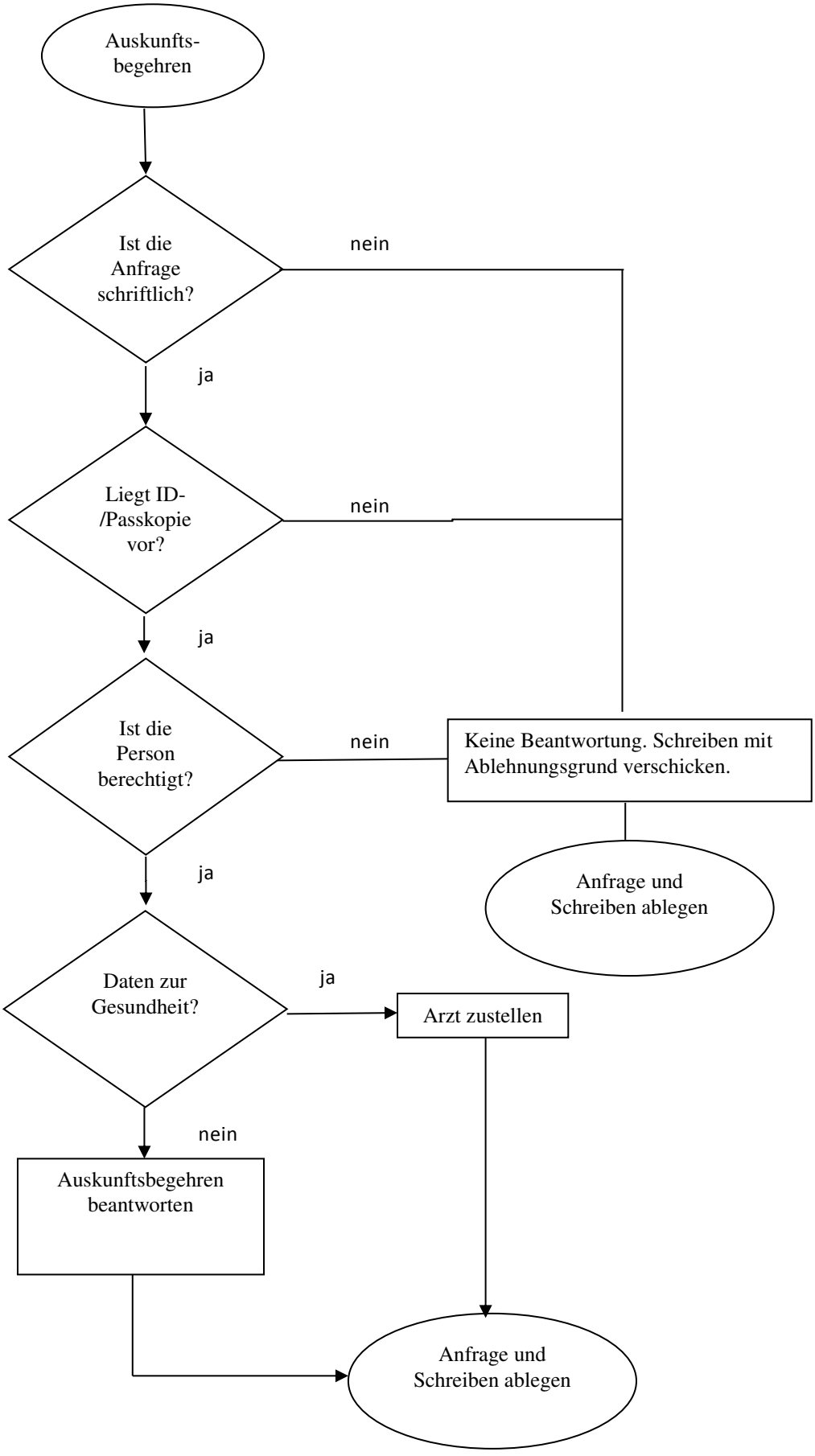
Kontaktstelle bezüglich datenschutzrechtlichen Fragen

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

rhenusana
Stefan Grabher
Betrieblicher Datenschutzverantwortlicher
Heinrich-Wild-Str. 210
9435 Heerbrugg
071 727 88 17
Stefan.grabher@rhenusana.ch

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

Geregelt in: 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
Stefan Grabher
Betrieblicher Datenschutzverantwortlicher
Heinrich-Wild-Str. 210
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:

- 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.

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.

2.7.3 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

2.7.4 IT-Kontrollen

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

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

2.7.5 Interne Audits

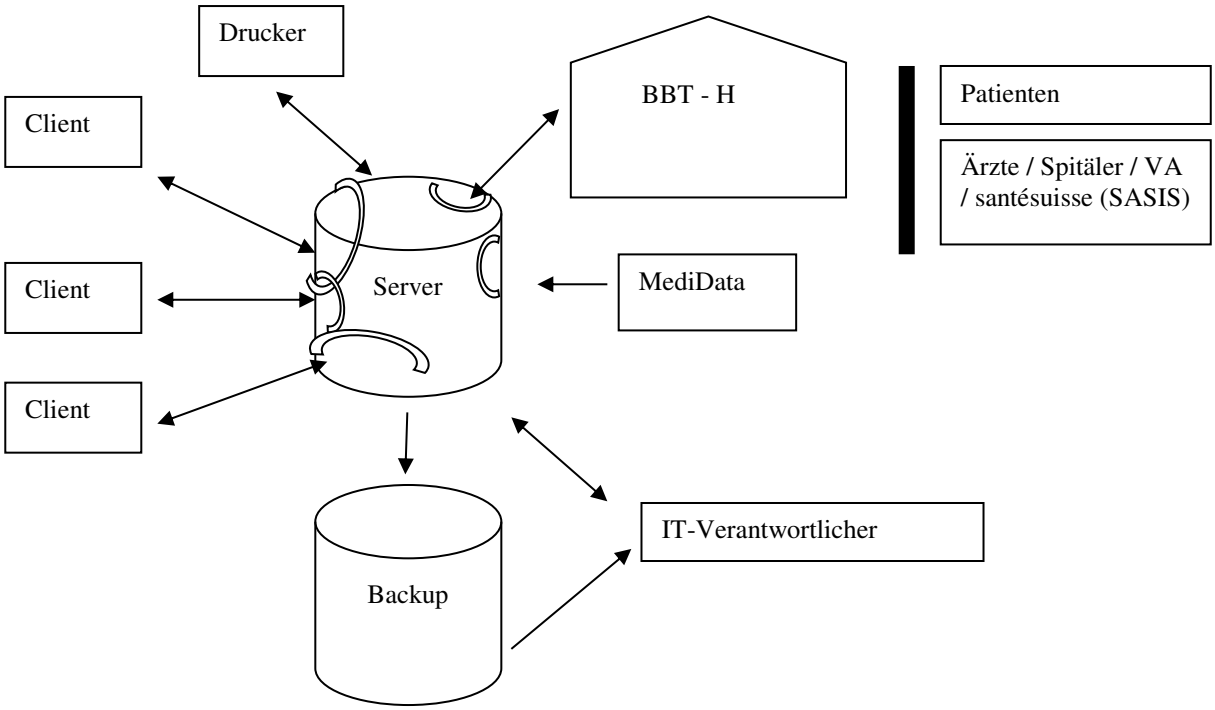
- Jährliche Kontrolle durch den betrieblichen Datenschutzbeauftragten.
- Jährliche Kontrolle durch die interne Revision

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

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 2013 Professional Plus (Briefe, Listen, etc.)
- Browser

Zusätzlich Abteilung Finanz- und Rechnungswesen:

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

Zusätzlich Abteilung Leistungen:

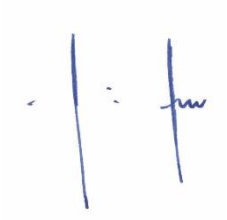
- IT Surplus (Scannen von Rechnungen der Leitungserbringer)
- Invoice Inspecter, MediData (Rechnungsprüfung)
- VEKA (Versichertenkarte)
- CaseNet (VAD, CM, DRG)

3.3 Schnittstellenbeschreibung

Die Schnittstellenbeschreibungen sind im Konformitätsnachweis ersichtlich:
Die Geschäftsleitung ist in Besitz des aktuellen Konformitätsnachweises.

3.4 Abkürzungen

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 Krankenkassen
VAD	Vertrauensärztlicher Dienst
VVG	Bundesgesetz vom 2. April 1908 über den Versicherungsvertrag (Versicherungsvertragsgesetz)



Guido Mitterer
Geschäftsführer

Stefan Grabher
CSO