GEWERBLICHE KRANKENKASSE BERN

Neuengasse 20, Postfach, 3001 Bern
Tel. 031 310 11 11 Fax 031 310 11 22
gkk@smgv-regionbern.ch
www.gkk-bern.ch

Geschäftsmodell, Zuständigkeitenordnung, Arbeitsabläufe und Datenschutz der Gewerblichen Krankenkasse Bern

Erstellt: 15.11.2012, erstes Dokument
Autor: Leonhard Sitter
Fachgebiet: Organisation, Prozesse und Datensicherheit
Ausgabe: 6 vom 25.08.2023
Klassifikation: öffentlich
Verteiler: Deniz Anselmo, Fabio Büschlen, Leonhard Sitter, Mitglieder, Öffentlichkeit

Änderungskontrolle

Datum	Beschreibung	Freigabe durch	Datum
30.10.2012	Erstellung neues Dokument, Version 01.00	Bernhard Boegli	20.11.2012
12.12.2014	Anpassungen aufgrund Wechsel Sachbearbeiter/in, IT-Lieferant (unter Berücksichtigung 03.12.2012 EDÖB)	Leonhard Sitter	12.12.2014
31.10.2015	Aktualisierung des Dokuments zwecks Prüfung im Rahmen der Zwischenrevision	Leonhard Sitter	31.10.2015
07.05.2019	Aktualisierung des Dokuments aufgrund Erstellung Geschäftsplan, Anpassungen von Statuten und Versicherungsreglement	Leonhard Sitter	07.05.2019
10.06.2021	Aktualisierung des Dokuments aufgrund Überprüfung bez. Geschäftsplan, Anpassungen von Statuten	Leonhard Sitter	10.06.2021
25.08.2023	Aktualisierung des Dokuments aufgrund neuen Datenschutzgesetzes per 01.09.23	Leonhard Sitter	25.08.2023

Inhalt

Abbildungsverzeichnis

1 Abkürzungsverzeichnis

ATSG	Allgemeiner Teil des Sozialversicherungsrechts des Bundes
DSG	Bundesgesetz über den Datenschutz, gültig ab 01.09.2023
DSV	Verordnung zum Bundesgesetz über den Datenschutz, gültig ab 01.09.2023
GKK	Gewerbliche Krankenkasse Bern
KVAG	Bundesgesetz betreffend die Aufsicht über die soziale Krankenversicherung (Krankenversicherungsaufsichtsgesetz) vom 26. September 2014
KVAV	Verordnung betreffend die Aufsicht über die soziale Krankenversicherung vom (Krankenversicherungsaufsichtsverordnung) 18. November 2015
KVG	Bundesgesetz über die Krankenversicherung vom 18. März 1994
KVV	Verordnung über die Krankenversicherung vom 27. Juni 1995
VVG	Bundesgesetz über den Versicherungsvertrag (Versicherungsvertragsgesetz, VVG) vom 2. April 1908

2 Gegenstand und Zweck dieses Dokuments

2.1 Zweck des Dokuments

Mit diesem Dokument soll das Unternehmen der Gewerblichen Krankenkasse Bern und deren Geschäftstätigkeit beschrieben sowie die notwendigen Dokumentierungen und Regulierungen dargelegt werden. Dazu werden die strategische Ausrichtung, die Arbeitsabläufe (Prozesse) und die Risikosituation mit Sicherheitsanforderungen und Massnahmen zur Gewährleistung eines geregelten Geschäftsverlaufs und des Datenschutzes aufgezeigt.

Das Dokument soll dem Leser ein umfassendes Bild des Unternehmens vermitteln.

Ferner soll das Dokument die Funktion einer Arbeitsanweisung erfüllen und als Bearbeitungsreglement im Sinne des eidgenössischen Datenschutzgesetzes (DSG) und der darauf basierenden Verordnung (DSV) dienen.

2.2 Art des Dokuments

Das Dokument vereint mehrere Funktionen zugleich. Es ist Konzept, Umsetzungs- und Datenschutzdokumentation in einem:

- Geschäftsmodell und strategische Ausrichtung
- Dokumentation des Managementsystems
- Richtlinien und Anweisungen in Bezug auf das Tagesgeschäft (insbesondere werden praktizierte Abläufe, Arbeitsmittel sowie der Umgang und die dafür vorgesehenen Sicherheitsmassnahmen im Zusammenhang mit erhobenen und bearbeiteten Daten dokumentiert.)
- Daten-Bearbeitungsreglement (im Sinne des revidierten DSG, per 01.09.2023)
- Geschäfts- und Zuständigkeitenordnung der GKK

3 Ausgangslage und Rechtsform der GKK

Die GKK wurde durch die Verbände „Maler- und Gipserunternehmerverband Region Bern“ und „Maler- und Gipserunternehmerverband Region Bern-Land“ ins Leben gerufen. Gemäss den Zweckbestimmungen beider Verbände, sollten damit die Interessen des Berufsstandes und der Arbeitnehmer und Arbeitgeber in der Branche unterstützt werden, ohne ein Gewinnziel zu verfolgen. Die GKK ist eine kleine Krankentaggeldversicherung, primär für die Branche der Maler- und Gipserunternehmen in der Region Bern, seit der Statutenänderung vom Mai 2021 auch für weitere Branchen des Bau- und Baunebengewerbes im Kanton Bern.

Auszug aus den Statuten der GKK vom 11. Mai 2021:

1. Name, Sitz und Zweck

Art. 1
Name, Rechtsnatur, Sitz

Der „Verein Krankentaggeldversicherung für Berner KMU Bern – Gewerbliche Krankenkasse“ ist ein Verein gemäss Art. 60 ff. ZGB mit Sitz in Bern. Er ist im Handelsregister von Bern eingetragen.

Art. 2
Zweck und Tätigkeitsgebiet

Der Verein will mithelfen, seine Mitglieder vor den wirtschaftlichen Folgen von Krankheit und Unfall und Mutterschaft zu bewahren. Zu diesem Zweck betreibt er eine Krankentaggeldversicherung für KMU, vorwiegend in der Region Bern.

Art. 3
Unterstellung unter das KVG

Der Verein untersteht dem ZGB. Soweit er die Krankenversicherung betreibt, untersteht er dem Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) vom 6. Oktober 2000 (SR 830.1) und dem Bundesgesetz über die Krankenversicherung (KVG) vom 18. März 1994 (SR 832.10) mit den jeweiligen Ausführungsbestimmungen.

Damit ist festgelegt, dass die Tätigkeiten des Vereins ausschliesslich aus der Geschäftstätigkeit der Krankentaggeldversicherung finanziert werden.

Art. 4
Bekanntmachungen

Bekanntmachungen erfolgen in rechtsverbindlicher Weise durch Zirkular an die Mitglieder. Bei Kollektivversicherungen werden die Mitteilungen dem versicherten Betrieb zugestellt.

2. Mitgliedschaft

Art. 5
Art der Mitgliedschaft

1) Dem Verein können einzelversicherte und kollektivversicherte Personen angehören.
2) Näheres über Erwerb, Verlust, Rechte und Pflichten der Mitgliedschaft sind in den Allgemeinen Versicherungsbestimmungen beziehungsweise im Reglement enthalten.

Die GKK operiert explizit als nicht auf Gewinnerzielung ausgerichtetes Unternehmen (non profit organisation). Das Geschäft verläuft seit Jahren stabil, Gewinne werden zur Äuffnung gesetzlicher Reserven und zur freiwilligen Risikosicherung thesauriert.

Es ist erklärte Absicht, das Geschäft sowie die GKK als Unternehmen zum Vorteil Ihrer Mitglieder (Ihrer Kunden) auf unbestimmte Zeit weiterzuführen und die statutarisch vorgesehenen Leistungen erbringen und laufend verbessern zu können. Dies impliziert auch eine kontinuierliche Verbesserung der unternehmerischen Tätigkeit. Dazu ist der Betrieb laufend den ändernden Gegebenheiten, Kundenanforderungen und gesetzlichen Anforderungen anzupassen.

4 System und Organisation der GKK

4.1 Geschäftsmodell

Die GKK ist eine nicht auf Erzielung von Gewinn ausgerichtete Unternehmung. Sie erwirtschaftet über eingenommene Versicherungsprämien Erträge und richtet Leistungen im Falle von Krankheits- und Unfallschäden bei Arbeitnehmern:innen seiner Mitglieder an diese aus. Die damit verbundenen Risiken sichert die GKK mit finanziellen Reserven in Form von Kapitalanlagen ab.

4.2 Managementsystem und Prozesse

Wie jedes Managementsystem, umfasst dasjenige der GKK langfristige Ziele (Vision, Mission), mittel- und kurzfristige Ziele (Strategie, Prozessziele) und Aktivitäten des Tagesgeschäftes. Besonderes Augenmerk wird auf die korrekte, gesetzmässige Verrichtung der Arbeiten und die Sicherheit in Bezug auf den Schutz der erhobenen und bearbeiteten Daten der versicherten Personen gelegt.

Vision: Die GKK ist das bevorzugte Versicherungsinstitut seiner Mitglieder für deren Absicherung vor den wirtschaftlichen Folgen von Krankheit und Unfall.

Mission: Die GKK erbringt überdurchschnittliche Leistungen (Versicherungsdeckung, Kulanz, Kundennähe) zu den tiefst möglichen Versicherungsprämien (im Verhältnis zu andern, insbesondere grossen Versicherungsanbietern).

Leitbild: Kundinnen und Kunden: Wir überraschen sie mit Qualitätsarbeit, über-durchschnittlicher Kulanz und Dienstleistungen bei günstigen Prämien. Unsere Kunden spüren die Kompetenz und Zuvorkommenheit unserer Mitarbeiter:innen.

Mitarbeiterinnen und Mitarbeiter: Zu unserem grössten Gut tragen wir tagtäglich Sorge. Wir motivieren unser Personal zu aussergewöhnlichen Leistungen. Wir fördern die freie, eigenverantwortliche Entfaltung der Mitarbeiter.

Lieferanten: Wir pflegen faire, marktwirtschaftliche und langjährige Beziehungen.

Umwelt: Nachhaltiges Handeln in allen Unternehmensbereichen ist für uns selbstverständlich. Wir sind uns der Notwendigkeit nachhaltigen Handelns in Bezug auf die soziale, die ökonomische und die ökologische Umwelt bewusst und verhalten uns danach.

Strategie: Die GKK sichert ihr Kundenportfolio durch personelle und funktionelle Nähe zu den Versicherten und den Verbandsmitgliedern der Bau- und Baunebenbranchen im Kanton Bern, insbesondere der Gipser- und Malerbranche.

Die GKK sichert optimale Leistungen durch persönliche Kontakte zu den Kunden, und den Versicherten und verhält sich in Zweifelsfällen überdurchschnittlich kulant (im Verhältnis zu andern, insbesondere grossen Versicherungsanbietern).

Die GKK sichert unterdurchschnittlich hohe Prämien durch schlanke Unternehmensstrukturen.

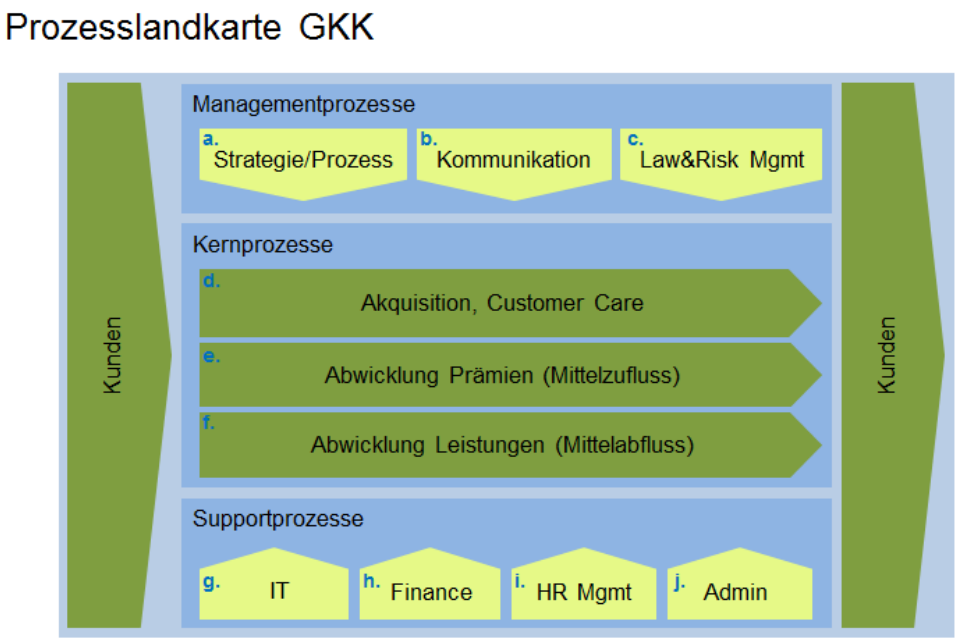

Abbildung 1: Prozesslandkarte GKK

In den Kernprozessen entsteht die Wertschöpfung der GKK und werden geschäftliche Daten bearbeitet, insbesondere beschafft, gespeichert, aufbewahrt, verwendet, verändert, bekanntgegeben, archiviert (abgelegt), gelöscht oder vernichtet. Die Führungsprozesse (Managementprozesse) und die Unterstützungsprozesse (Supportprozesse) sind lediglich zur Organisation und Funktionalität der Kernprozesse und der darin bearbeiteten Daten zuständig.

Die drei Kernprozesse lassen sich in Hauptprozesse konkretisieren:

Abbildung 2: Kern- und Hauptprozesse GKK

4.3 Organe und Dateneinsicht

Die gesetzlichen und statutarischen Organe der GKK sind (gemäss Statuten vom 11.05.2021):

3. Organe

Art. 6
Organe

Die Organe sind:

a) die Mitgliederversammlung
b) der Vorstand
c) die Geschäftsstelle
d) die Kontrollstelle

A. Mitgliederversammlung

Art. 7
Zusammensetzung

1) Die Mitgliederversammlung ist das oberste Organ. Sie besteht aus dem Vorstand und allen Versicherten gemäss Art. 2.

4.3.1 Organe, organisatorische Schnittstellen und Dateneinsicht

Die Organisationseinheiten, welche Daten von Kunden und Versicherten erheben und bearbeiten, sind ausschliesslich im Organ der Geschäftsstelle angegliedert.

Die Organe des Vorstands und der Mitgliederversammlung des Vereins GKK sehen lediglich Finanzzahlen und keine personenbezogenen Daten Versicherten.

Das Organ der Kontrollstelle kann grundsätzlich alle geschäftlichen Daten einsehen, untersteht jedoch einer gesetzlichen Schweigepflicht.

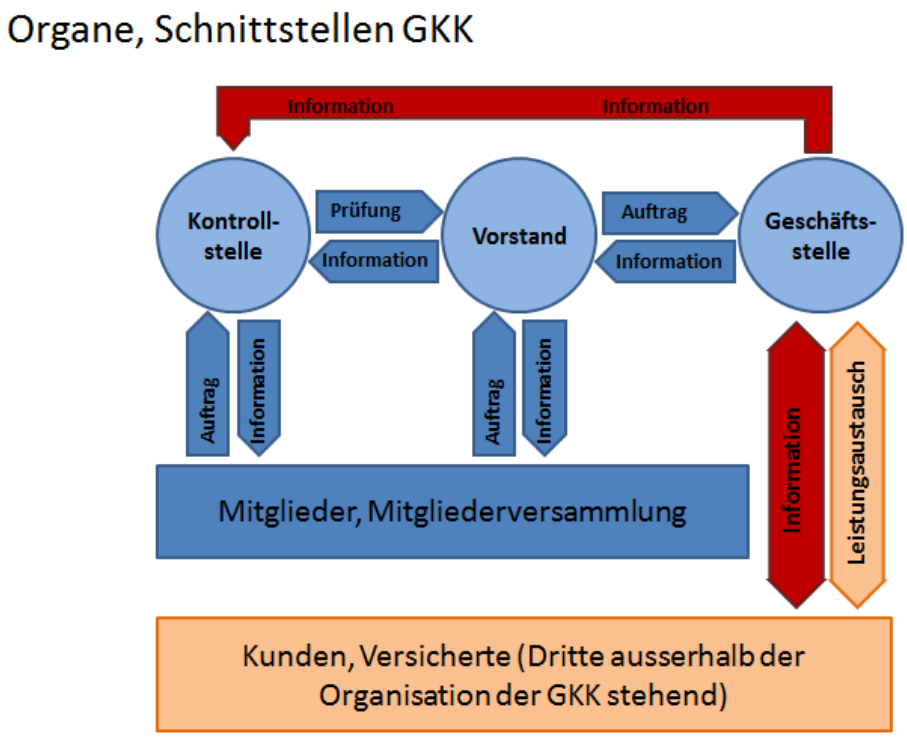

Abbildung 3: Organe, Schnittstellen GKK

In Abbildung 3 sind die oben beschriebenen Organe und zusätzlich die Kunden und die Versicherten als ausserhalb der operativen Organisation stehende Personengruppe dargestellt.

Die innerorganisatorischen Schnittstellen zwischen den Organen, welche Informationen oder Aufträge mit innerbetrieblichem Gehalt betreffen, sind mit Pfeilen in blauer Farbe dargestellt.

Mit Pfeilen in roter Farbe sind Schnittstellenverhältnisse ausgewiesen, die ausserbetriebliche Informationen betreffen, die unter anderen, gemäss Art 5, Litt c DSG sog. «besonders schützenswerten Daten» sind (Informationen über die Gesundheit einer Person).

Die Schnittstelle zwischen den versicherten Unternehmungen (Kunden) sowie den versicherten Personen und der Geschäftsstelle (rosa Pfeil) betrifft regelmässig Daten mit mittlerem Schutzbedarf, sog. «schützenswerte Daten» wie Versicherungsleistungen zum Ausgleich von finanziellen Einbussen durch Erwerbsausfälle aufgrund von Krankheit und Unfall, soweit aus diesen nicht auf die gesundheitlichen Umstände der betroffenen Personen geschlossen werden kann.

4.3.2 Schnittstellen der GKK zu Stellen ausserhalb der Unternehmung

Ansprechgruppen ausserhalb der GKK, mit denen die Unternehmung Schnittstellen aufweist und Daten austauscht sind:

- Kunden (Unternehmungen, die bei der GKK eine kollektive Krankentaggeldversicherung abgeschlossen haben)
- Versicherte (natürliche Personen, die aufgrund eines Schadenfalles einen direkten Leistungsanspruch an die GKK haben, der nicht direkt an das arbeitgebende Unternehmen (Kunde) zu richten ist) und Einzelversicherte
- Ärzte und heilbehandelnde Institutionen, die Arbeitsunfähigkeitsausweise ausstellen
- Unfallversicherer
- Krankenpflegeversicherungen
- Regionale Arbeitslosenkassen, Invalidenversicherungen und weitere Sozialversicherer

4.3.3 Aufgaben, Kompetenzen und Verantwortlichkeiten

Oberstes Organ ist die Mitgliederversammlung. Sie beschliesst über die ihr statutarisch und von Gesetzes wegen übertragenen Angelegenheiten (bezüglich der Aufgaben der Mitgliederversammlung wird auf die Statuten verwiesen). Damit verantwortet sie gegenüber sämtlichen Ansprechgruppen ausserhalb der Unternehmung die unternehmerische Tätigkeit der GKK.

Der Vorstand ist das ausführende strategische Organ. Ihm obliegt die Beschlussfassung über alle geschäftlichen Belange, über welche nicht die Mitgliederversammlung zu beschliessen hat. Somit trägt er gegenüber der Mitgliederversammlung die vollumfängliche Verantwortung für die Geschäftsführung und für den Datenschutz.

Die Kontrollstelle überprüft zuhanden der Mitgliederversammlung die Geschäftstätigkeit des Vorstandes. Zu ihrer Information greift sie auf die operative Geschäftsführung durch die Geschäftsstelle zurück. Mittels Revisionsbericht (ordentliche Revision), der den gesetzlichen Anforderungen zu entsprechen hat, informiert sie die Mitgliederversammlung. Die Kontrollstelle verantwortet einerseits gegenüber Ansprechgruppen ausserhalb der Unternehmung die richtige, gesetzeskonforme Rechnungslegung und korrekt ausgeführte Administration im Sinne des KVG, KVV, KVAG und des KVAV, andererseits gegenüber der Mitgliederversammlung.

Für die Klärung der Aufgaben, Kompetenzen und Verantwortlichkeiten und die Regelungen zwischen den versicherten Mitgliedern (Kunden), den leistungsberechtigten Kunden und versicherten Personen, existiert neben den Statuten das Versicherungsreglement der GKK.

Die operative Geschäftsführung wird durch die Geschäftsstelle vorgenommen. Sie verantwortet die gesamte geschäftliche Tätigkeit gegenüber dem Vorstand, insbesondere auch den Schutz der durch die GKK bearbeiteten Daten.

4.4 Geschäftsstelle, Geschäftsführer, Verantwortlicher Datenschutz

Die Geschäftsstelle als Organ der GKK, welches die operativen Tätigkeiten des Unternehmens ausführt, ist die einzige Stelle innerhalb der GKK, welche schützenswerte (und besonders schützenswerte Daten) im Sinne des DSG bearbeitet. Daher sind die Organisation und die Tätigkeiten der Geschäftsstelle hier besonders offenzulegen. Er Geschäftsführer ist der Verantwortliche für Datenschutzangelegenheiten

4.4.1 Organisationseinheiten, organisatorische Schnittstellen und Dateneinsicht

Die Organisationseinheiten innerhalb der Geschäftsstelle sind die folgenden, auf Abbildung 4 dargestellten.

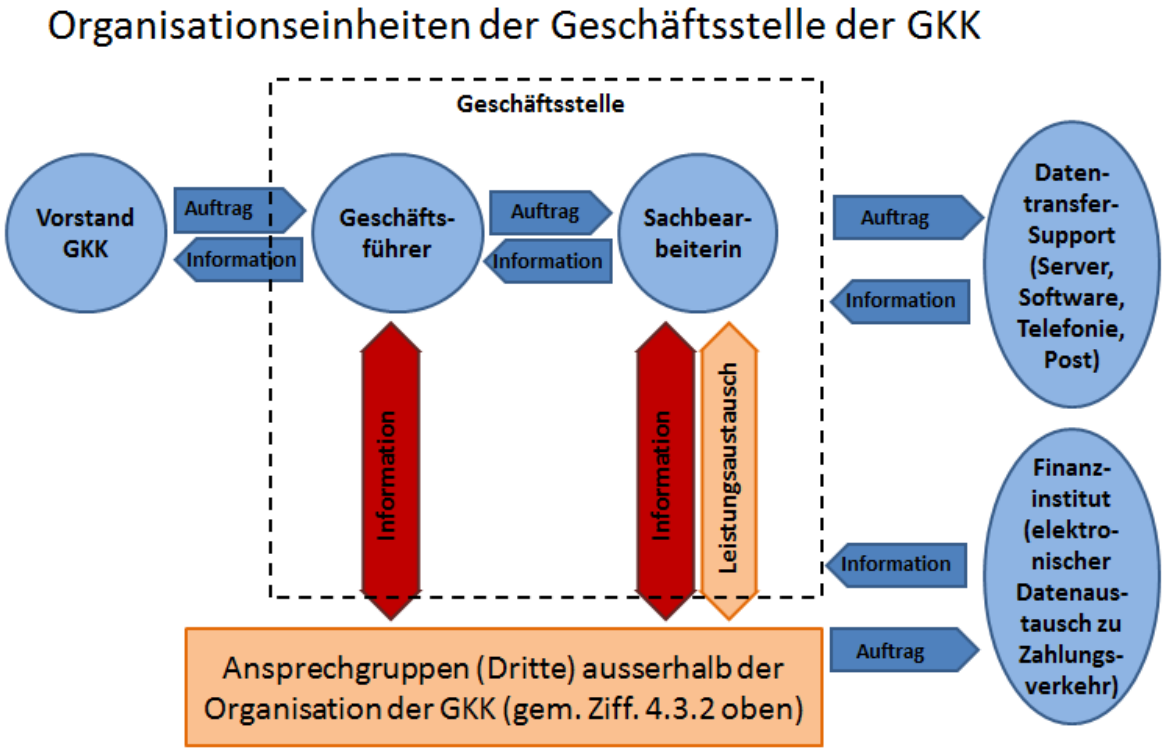

Abbildung 4: Organisationseinheiten, Schnittstellen der Geschäftsstelle GKK

Wie auf Abbildung 4 zu sehen ist, bearbeiten innerhalb der Unternehmung GKK nur der Geschäftsführer (Verantwortliche Datenschutz) und die Sachbearbeiter:innen die Daten der Kunden und von betroffenen Personen, sowie von deren Ärzten und deren Arbeitslosen-, Unfall- und Krankenpflege- und weiteren Sozialversicherern oder auch von Strafverfolgungsbehörden. Daten mit besonderem Schutzbedarf werden auch nur zwischen diesen Organisationseinheiten der GKK mit den betreffenden Stellen ausserhalb der Unternehmung ausgetauscht. Folgende Dienstleister sind Dritte, welche unter gewissen Umständen Personendaten im Auftrag der GKK wahrnehmen können: IT-System-Supporter:in, Applikationslieferant:in, Supporter:in für Rechnungslegungsaufgaben, Revisionsstelle. Dies geschieht ausschliesslich zur Sicherstellung GKK-interner Prozesse. Das Einsehen von Personendaten durch diese Dienstleister erfolgt ausschliesslich in den Geschäftsräumlichkeiten oder im operativen IT-System der GKK. Besagte Dienstleister nehmen keine andere Bearbeitung personenbezogener Daten wahr. Ferner werden diese vertraglich zur Einhaltung der aktuell geltenden Datenschutzgesetzgebung sowie zur Geheimhaltung und Vertraulichkeit verpflichtet.

4.4.2 Aufgaben, Kompetenzen und Verantwortlichkeiten

Der Geschäftsführer und Verantwortlicher Datenschutz verantwortet gegenüber dem Vorstand der GKK die gesamte operative Geschäftstätigkeit. In seiner Verantwortung steht auch die

Tätigkeit der Sachbearbeiter:innen. Dazu gehört insbesondere die Wahrung der Sicherheitsanforderungen und -bestimmungen im Sinne des DSG. Neben Daten mit geringem oder mittlerem Schutzbedarf werden auch Daten mit besonderem Schutzbedarf zwischen den Organisationseinheiten der Geschäftsstelle der GKK mit ausserhalb der Unternehmung stehenden Instanzen ausgetauscht.

Die GKK ist als Branchenlösung in der Krankentaggeldversicherung für Unternehmen der Bau- und Baunebenbranchen, insbesondere er Maler- und Gipserunternehmen in der Region Bern eine Kleinstversicherung. Für die Ausführung der Hauptprozesse und des operativen Tagesgeschäfts (gemäss Ziffer 4.2, Abbildung 2 oben), sind auf der Geschäftsstelle die Sachbearbeiter:innen alleine zuständig. Bei ausserordentlichen Fragestellungen ziehen diese den Geschäftsführer (Verantwortlicher Datenschutz) bei.

Die regelmässig auszuführenden und unter der direkten Verantwortung des Geschäftsführers stehenden Aufgaben sind:

- Handhabung von Reklamationen durch die Kunden
- Mahnung von Ärzten, Heilinstituten und andern Versicherungsunternehmungen bei wiederholtem Ausbleiben einer Antwort nach Aufforderungen zur Lieferung benötigter Angaben, Informationen und Belegen
- Juristische Beurteilung besonderer Fälle und Beilegung von Uneinigkeiten zwischen der GKK und Kunden, Versicherten, Ärzten, Heilinstituten und andern Versicherungsunternehmungen
- Erstellung aller Berichte, Konzepte und Projektunterlagen der GKK, inkl. Dokumentation des Geschäftsplanes, der Geschäftsberichte, des IKS, der Dokumentation rund um den Datenschutz und des vorliegenden Dokuments
- Anlaufstelle für alle Fragen rund um den Datenschutz
- Disposition der Kapitalanlagen in Zusammenarbeit mit der Vermögensverwaltung der Valiant Bank AG und Sicherstellung der Einhaltung des Anlagenreglements
- Organisation und Administration der Vereins- und Vorstandssitzungen
- Beisitz und Protokollierung anlässlich von Vereins- und Vorstandssitzungen
- Unterstützung und Beratung des Präsidenten und der Vorstandsmitglieder der GKK
- Kontrolle und allfällig notwendige Bereinigungen der Rechnungslegung
- Erstellung von Kalkulationen und Risikoeinschätzungen
- Kontakt zu der Kontrollstelle und Organisation der jährlichen Revision
- Wahrnehmung der Schnittstellen der GKK zu Behörden, der Öffentlichkeit, Gönnern und interessierten Dritten
- Erfüllung der Anforderungen der öffentlichen Hand und deren Ämtern, Direktionen und Kontrollorganen
- Handhabung aller ausserordentlichen Geschäfte der GKK

5 Datenbearbeitungsgrundsätze, Rechte betroffener Personen

5.1 Grundregeln der Datenbearbeitung

5.1.1 Rechtmässigkeit

Personendaten müssen rechtmässig bearbeitet werden. Die Bearbeitung gilt nur als rechtmässig, wenn sie durch (a) Einwilligung der betroffenen Person, durch (b) ein überwiegendes privates oder öffentliches Interesse oder durch (c) Gesetz gerechtfertigt ist.

5.1.2 Transparenz

Die Bearbeitung der Daten muss grundsätzlich so erfolgen, dass sie der betroffenen Person bekannt ist.

5.1.3 Verhältnismässigkeit

Bei der Bearbeitung von Personendaten ist der Grundsatz der Verhältnismässigkeit zu beachten. Gemäss diesem Grundsatz dürfen nur solche Daten erhoben werden, die für den entsprechenden Zweck notwendig und geeignet sind.

Weiter dürfen Personendaten nur so lange gespeichert werden, wie dies für den Zweck notwendig ist (vgl. hiernach).

5.1.4 Zweckbindung

Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist, was bei der GKK nicht schwerfällt, da deren Tätigkeiten u.A. durch die Gesamtarbeitsverträge der angeschlossenen Betriebe und Branchen bekannt und gefordert sind.

Werden die Personendaten zum Zweck der Bearbeitung nicht mehr benötigt, müssen diese vernichtet oder anonymisiert werden.

5.1.5 Richtigkeit, Vernichten von nicht benötigten Daten

Alle Mitarbeiter:innen der GKK haben darauf zu achten, dass Personendaten richtig sind und auf dem neuesten Stand gehalten werden.

Es müssen alle angemessenen Massnahmen getroffen werden, um unzutreffende oder unvollständige Daten zu berichtigen oder zu vernichten.

Personendaten, welche die GKK nicht mehr zur Durchführung ihrer geschäftlichen vertraglichen oder gesetzlichen Tätigkeiten benötigt, werden nach Ablauf der gesetzliche oder vertraglichen Archivierungsvorschriften vernichtet. Für Daten, welche für die Kernprozesse der GKK oder zur möglichen Verfolgung rechtlicher Ansprüche aus dem Krankenversicherungsgeschäft unabdingbar sind, gilt eine Verjährungsfrist von mindestens fünf Jahren, für Daten, welche die Rechnungslegung der GKK betreffen eine solche von zehn Jahren.

5.1.6 Datensicherheit

Für die GKK ist von grosser Bedeutung, dass die Sicherheit der Daten jederzeit gewährleistet ist. Vor diesem Hintergrund sind die Personendaten durch technische und organisatorische Massnahmen u.a. gegen Verlust, gegen unbefugten Zugriff und vor anderen Gefahren geschützt und zu schützen.

Für die einzelnen Vorgänge der Datenbearbeitung sind die konkreten Schutzmassnahmen im Dokument «Arbeitsabläufe und Datensicherheit GKK Bern» definiert und werden laufend auf ihre Angemessenheit überprüft.

Die IT-Lieferanten:innen und Supporter:innen der GKK empfehlen gegebenenfalls weiterführende IT-spezifische Verbesserungen und Vorgaben im Interesse der Datensicherheit, insbesondere in Bezug auf die Nutzung der IT-Systeme, welchen die GKK in aller Regel folgt.

5.1.7 Einwilligung und Widerspruch

Eine ausdrückliche Einwilligung der betroffenen Person zur Datenbearbeitung durch die GKK

ist grundsätzlich nicht erforderlich und wird nur bei der Bearbeitung von besonders schützenswerten Personendaten von Dritten gefordert. An sich sind auch diese für die Krankentaggeldversicherung GKK ohne ausdrückliche Einwilligung der betroffenen Personen beschaffbar, was sich aus den einschlägigen Gesetzen und den allgemeinverbindlich erklärten Gesamtarbeitsverträgen der angeschlossenen Betriebe und Branchen ergibt.

Widerspricht die betroffene Person hingegen einer Datenbearbeitung ausdrücklich, ist diese nur gerechtfertigt, wenn überwiegende Interessen der GKK, bzw. des Verantwortlichen oder eine gesetzliche Grundlage vorliegen.

5.1.8 Informationspflicht

Betroffene Personen werden vorgängig darüber informiert, zu welchem Zweck Personendaten über sie erhoben und bearbeitet werden. Dies wird mit dem öffentlich zugänglichen Dokument «Datenschutzerklärung GKK Bern» (zu finden unter https://www.smgv-region-bern.ch/de/GKK-Bern/dokumente) gewährleistet, auf welches betroffene Personen durch die GKK (Einzelversicherte, angeschlossene Unternehmungen) oder durch deren Arbeitgeber:innen (Kollektivversicherung) hingewiesen werden. Betroffene Personen müssen daher nicht durch die GKK informiert werden, wenn ihre Daten nicht direkt bei ihnen eingeholt werden.

Macht die betroffene Person ihre Personendaten dem Verantwortlichen von sich aus direkt zugänglich, gilt diese als informiert.

Falls sich der Zweck der Datenbearbeitung bei der GKK ändern sollte, müssen bereits informierte Personen erneut informiert werden.

5.1.9 Auftragsbearbeitung

Wenn Dienstleister:innen der GKK in deren Auftrag Personendaten einsehen (sog. Auftragsbearbeiter:innen), ist zu beachten, dass die gleichen Sorgfaltsanforderungen wie für die GKK selbst auch für die Auftragsbearbeiter:innen gelten. Auftragsbearbeiter:innen der GKK nehmen neben dem möglichen Einsehen, keine anderen Bearbeitungen von Daten betroffener Personen wahr. Geheimhaltung, Zweckbindung und Datensicherheit sind vertraglich sichergestellt.

5.1.10 Übermittlung von Personendaten ins Ausland

Die Übermittlung von Personendaten ins Ausland ist nur in Staaten zulässig, in denen durch den Bundesrat ein ähnlich hohes Datenschutzniveau festgestellt wurde, wie in der Schweiz. Eine Einhaltung des Schweizer Datenschutzstandards kann zudem unter anderem durch den Abschluss zusätzlicher vertraglicher Vereinbarungen erreicht werden. Eine Weitergabe von Personendaten an Empfänger im Ausland durch die GKK erfolgt nur, wenn diese angemessenen Datenschutzgesetzen unterliegen.

Der Wirkungskreis der GKK ist auf das Staatsgebiet des Kantons Bern beschränkt. Somit bearbeitet die GKK ausschliesslich Personendaten von Arbeitnehmer:innen und Arbeitgeber:innen im Kanton Bern. Personendaten von betroffenen Personen werden einzig zur Identifikation derselben (Name, Adresse, Geburtsdatum, Sozialversicherungsnummer) an Ärztinnen, Ärzte oder Spitäler im Ausland abgegeben, einzig im Falle des Aufenthalts einer betroffenen Person bei diesen und ausschliesslich zum Zweck der Erlangung von Gesundheitsdaten bei Krankheit während einem entsprechenden Aufenthalt der betroffenen Person. Die Weiterleitung oder auch der Empfang durch die GKK solcher Daten folgt den sonstigen Datenschutzbestimmungen der Datenschutzerklärung GKK Bern.

5.2 Innerbetriebliche Prozesse

5.2.1 Anforderungen an Mitarbeiter:innen

Alle Mitarbeiter:innen der GKK sind dem Datenschutz verpflichtet. Sie werden namentlich darüber informiert, dass es untersagt ist, Personendaten für private Zwecke zu nutzen, an Unbefugte zu übermitteln oder sie Unbefugten zugänglich zu machen. Die Pflicht zur Wahrung der Vertraulichkeit und die vertragliche Geheimhaltungspflicht gelten über das Ende der Anstellung hinaus.

Auch innerhalb des Unternehmens ist darauf zu achten, dass nur die Mitarbeiter:innen Zugriff auf Personendaten erhalten, die sie zur Erledigung ihrer Aufgaben für die GKK benötigen.

Alle Mitarbeiter:innen sollen zu Beginn ihrer Anstellung und nachfolgend regelmässig in Datenschutzthemen geschult und sensibilisiert werden.

5.2.2 Verzeichnis der Bearbeitungstätigkeiten

Die GKK führt Verzeichnisse der Bearbeitungstätigkeiten im Zusammenhang mit Personendaten. Darin werden festgehalten: Identität des Verantwortlichen bzw. des Auftragsbearbeiters, Bearbeitungszweck, Kategorien betroffener Personen, Empfängerinnen und Empfänger sowie das Datum der Bearbeitung. Das Verzeichnis sollte stets aktuell sein und einen Überblick über die datenschutzrelevanten Aktivitäten im Unternehmen verschaffen.

5.2.3 Datenschutz durch Technik sowie Datenschutz-Folgeabschätzung

Die zur Bearbeitung von Personendaten eingesetzten Systeme der GKK sind so gestaltet, dass der Datenschutz eingehalten werden kann. Die technischen und organisatorischen Massnahmen sind insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, entsprechend ausgestaltet (Privacy by Design).

Der Verantwortliche hat die Standardeinstellung am Gerät bzw. an der Software so zu wählen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt. Dies betrifft bspw. das Akzept von Cookies auf der Website.

Die GKK hat eine Datenschutz-Folgeabschätzung (DSFA) erstellt und dokumentiert.

5.3 Rechte der betroffenen Personen

5.3.1 Auskunftsrecht

Auf Anfrage ist einer betroffenen Person mitzuteilen, ob von der GKK Personendaten über sie bearbeitet werden. Sofern dies der Fall ist, hat die betroffene Person einen Anspruch auf Auskunft über die entsprechenden Personendaten. Beim Auskunftsrecht geht es darum, in Erfahrung zu bringen, ob Personendaten bearbeitet werden und wenn ja, welche, sodass die betroffene Person ihre weiteren Rechte geltend machen kann. Dazu gehören neben den bearbeiteten Personendaten auch Angaben zur Identität des Verantwortlichen, zum Bearbeitungszweck, zur Aufbewahrungsdauer, zur Datenherkunft und zu den Empfängern:innen.

Bei der Auskunftserteilung ist sicherzustellen, dass die Identität der betroffenen Person verifiziert wird. Weiter ist zu beachten, dass im Rahmen der Auskunftserteilung keine Personendaten Dritter offenbart werden. Die Auskunft ist in der Regel kostenlos und innert 30 Tagen zu erteilen.

5.3.2 Datenportabilität / Recht auf Datenherausgabe und Datenübertragung

Betroffene Personen können ihre Daten, die sie der GKK bekannt gegeben haben, in einem gängigen elektronischen Format herausverlangen.

5.3.3 Recht auf Berichtigung

Eine betroffene Person kann nach Art. 32 Abs. 1 DSG verlangen, dass unrichtige Personendaten berichtigt werden.

5.3.4 Recht auf Datenlöschung

Wenn Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden und keine gesetzliche Grundlage und kein überwiegendes privates Interesse der GKK oder Dritter besteht, kann die betroffene Person die Löschung ihrer Personendaten verlangen.

5.4 Zuständigkeiten und Verantwortung

In erster Linie sind diejenigen Mitarbeiter:innen für die Einhaltung der Vorgaben dieser Datenschutzrichtlinie verantwortlich, die jeweils mit der Datenbearbeitung betraut sind.

Alle Mitarbeiter:innen der GKK haben auf die Einhaltung dieser Datenschutzrichtlinie zu achten und auf diese Weise dazu beizutragen, dass bei der GKK einheitlich hohe Datenschutzstandards etabliert bleiben.

Werden gesetzliche datenschutzrechtliche Pflichten verletzt, drohen den Fehlbaren strafrechtliche (Busse bis CHF 250'000.-) und der GKK zivilrechtliche (bis hin zu Schadenersatz) Konsequenzen sowie Reputationsschäden. Strafrechtlich verantwortlich ist in erster Linie die natürliche Person, d.h. der:die vorsätzlich fehlbare Mitarbeiter:in. Datenschutzverletzungen können auch interne disziplinarische Konsequenzen haben.

5.5 Meldung bei Datenschutzverletzungen, Zusammenarbeit Aufsichtsbehörden

Die Mitarbeiter:innen haben dem Vorgesetzten bzw. dem Verantwortlichen unverzüglich Bericht zu erstatten, wenn sie Kenntnis von einem Verstoss gegen diese Datenschutzrichtlinie oder gesetzliche Bestimmungen haben, die sich auf den Schutz personenbezogener Daten beziehen.

Verletzungen der Datensicherheit (z.B. Offenlegung für Unbefugte, Datenverlust, Cyberangriff etc.), die für die Betroffenen zu einem hohen Risiko für ihre Persönlichkeit oder ihre Grundrechte führen, müssen von der GKK dem EDÖB «so rasch als möglich», also zeitnah, gemeldet werden.

6 Art, Kategorien und Schutz von Personendaten

6.1 Arten und Kategorien/ Sicherheitsstufen bearbeiteter Daten

Insbesondere können folgende Kategorien von Personendaten, die von betroffenen Personen oder Dritten bekannt gegeben worden sind, welche die GKK aus öffentlichen Quellen bezieht oder die sich aus der Vertragsabwicklung ergeben, durch die GKK bearbeitet werden:

6.1.1 Besonders schützenswerte Daten

Kategorie 1 (hoher Schutzbedarf)

Besonders schützenswerte Personendaten (gemäss Art. 5, Litt. c DSG) können für die Prüfung von Leistungsansprüchen, Ansprüchen gegenüber Dritten und die Erbringung der vertraglichen Leistungen bearbeitet werden.

a) Es handelt sich dabei bei der GKK vorwiegend um Gesundheitsdaten (allfällige Diagnosen, Daten zu Arbeitsunfähigkeiten wie Anzahl Krankheitstage, bereits bezogene Leistungen, Dauer der Krankheit) zu den betroffenen Personen, Antworten auf Fragen wie Sachverständigenberichte zur Gesundheit betroffener Personen und deren bisherigem Schadenverlauf sowie in Ausnahmefällen um Daten über betreibungsrechtliche Massnahmen von Behörden oder Daten über Massnahmen der sozialen Hilfe.

b) Die GKK bearbeitet keine Daten über die Intimsphäre, die Zugehörigkeit zu einer Rasse oder Ethnie, biometrische oder genetische Daten oder Daten über religiöse, weltanschauliche, politische Ansichten oder Tätigkeiten, über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen (ausser betreibungsrechtliche Massnahmen von Behörden) von betroffenen Personen.

Die unter a) genannten Personendaten werden bei der GKK ausschliesslich zur Bemessung der Prämien und zur Erbringung von vertraglichen Leistungen bearbeitet oder um die allenfalls daraus resultierenden rechtlichen Ansprüche der GKK durchzusetzen. Die Bearbeitung dieser Daten erfolgt zur Durchführung eines Vertrags. Sofern gesetzlich vorgeschrieben, wird vorab die schriftliche Einwilligung der betroffenen Personen eingeholt, für die Beschaffung von Gesundheitsdaten immer.

6.1.2 Schützenswerte Daten

Kategorie 2 (mittlerer Schutzbedarf)

2a) Geheime Daten
Vereinbartes Prämienmodell und Prämienzahlungen (Datum und Höhe), Höhe der versicherten Taggelder und Auszahlungsbeträge (inkl. Datum), Bonitätsdaten, Bankdaten der Versicherten wie insbesondere Angaben zur Bankverbindung für die Abwicklung der späteren Zahlungen (z. B. Kontonummer), AHV-Einkommensdaten, Prämienausstände, deckungsfreie Zeiträume, Mahnungen.

2b) Vertrauliche Daten
Angaben zur versicherten Person und/oder zum:r Vertragspartner:in bzw. zu Kontaktpersonen und Mitarbeitenden von Vertragspartnern:innen, Unternehmen, anderen Sozialversicherungen und Behörden, z. B. Name, Adresse, Geburtsdatum, Geschlecht, Nationalität, Sozialversicherungsnummer und ggf. die Beziehung zu anderen Personen und Unternehmen/ Arbeitgebern:innen, Webseitendaten wie Cookies und Logfiles.

Kategorie 3 (geringer oder kein Schutzbedarf)

2c) Interne Daten (geringer Schutzbedarf)
Angeschlossene Unternehmen, Versicherte, deren Namen, Adresse, Wohnort.

2d) Öffentliche Daten (kein Schutzbedarf)
Personendaten der Vertreter der leitenden Organe der GKK, im Rahmen der gesetzlichen Vorschriften sowie Namen der für die GKK tätigen Mitarbeiter:innen.

6.1.3 Ausschluss von Datenbearbeitungen

Die GKK bearbeitet keine Daten über die Intimsphäre, die Zugehörigkeit zu einer Rasse oder Ethnie, biometrische oder genetische Daten oder Daten über religiöse, weltanschauliche, politische Ansichten oder Tätigkeiten, über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen (ausser betreibungsrechtliche Massnahmen von Behörden) von betroffenen Personen.

6.2 Einsatzbereich und Zweck der Datenbearbeitung

Die GKK bearbeitet Personendaten ausschliesslich in der Durchführung der Kernprozesse «Customer Care», «Prämienabwicklung» und «Leistungsabwicklung».

6.2.1 Prozess Customer Care

Personendaten (von 20-30 Einzelversicherten, neben rund 110 Unternehmungen) der Kunden/ Versicherten werden vor Vertragsschluss in elektronischer und physischer Form beschafft, nach Vertragsschluss im Betriebssystem erfasst (Name, Adresse, Wohnort, Kategorisierung als „kollektiv“ oder „einzeln“ Versicherte. Diese werden später für die weiteren Hauptprozesse verwendet. Im Rahmen des Prozesses „Customer Care“ werden die Daten zu Informationszwecken verwendet. Nach Austritt des:r Kunden:in werden die Daten noch mindestens 10 Jahre gespeichert (gesetzliche Vorschrift). Werden die Daten danach nicht mehr benötigt, werden diese gelöscht, ohne Information an die betroffenen Personen. Auf Anforderung der betroffenen Personen werden die Daten berichtigt, nicht jedoch vor 10 Jahren nach Austritt gelöscht.

6.2.2 Prozess Prämienabwicklung

Personendaten (von 20-30 Einzelversicherten, neben rund 110 Unternehmungen) der Kunden/ Versicherten werden vor Vertragsschluss in elektronischer und physischer Form beschafft, nach Vertragsschluss im Betriebssystem erfasst (Name, Adresse, Wohnort, Kategorisierung als „kollektiv“ oder „einzeln“ Versicherte, Geburtsdatum, Sozialversicherungsnummer. Ferner werden die prämienrelevanten Vertragsdaten (Versicherungsmodell, Prämiensatz, Eintrittsdatum) sowie die versicherte Lohnsumme erfasst. Zur Erstellung der quartalsweisen Prämienrechnung werden die Daten verwendet. Ferner sind die Daten Basis für die aufsichtsrechtliche Berichterstattung an das Bundesamt für Gesundheit. Nach Austritt des:r Kunden:in werden die Daten noch mindestens 10 Jahre gespeichert (gesetzliche Vorschrift). Werden die Daten danach nicht mehr benötigt, werden diese gelöscht, ohne Information an die betroffenen Personen. Auf Anforderung der betroffenen Personen werden die Daten berichtigt, nicht jedoch vor 10 Jahren nach Austritt gelöscht.

6.2.3 Prozess Leistungsabwicklung

Personendaten (von 20-30 Einzelversicherten, neben rund 110 Unternehmungen) der Kunden/ Versicherten werden vor Vertragsschluss in elektronischer und physischer Form beschafft, nach Vertragsschluss im Betriebssystem erfasst (Name, Adresse, Wohnort, Kategorisierung als „kollektiv“ oder „einzeln“ Versicherte, Geburtsdatum, Sozialversicherungsnummer. Ferner werden die leistungsrelevanten Vertragsdaten (Versicherungsmodell, versicherter Lohn, Eintrittsdatum), Daten zu Arbeitsunfähigkeiten (Anzahl Krankheitstage, bereits bezogene Leistungen, Taggeld, Auszahlungsbetrag), sowie die Bankdaten der Kunden zur Auszahlung der Leistungen erfasst. Zur Erstellung der monatlichen Leistungsabrechnungen werden die Daten verwendet. Ferner sind die Daten Basis für die aufsichtsrechtliche Berichterstattung an das Bundesamt für Gesundheit. Bei Unklarheit der Leistungspflicht der GKK oder zur Bemessung der Leistungen werden in gewissen Fällen (rund 20 pro Jahr) Akten zum

Gesundheitszustand der Leistungsberechtigten bei anderen Sozialversicherern oder Ärzten der Versicherten beschafft. Diese Daten werden gespeichert und elektronisch abgelegt (nicht im Betriebssystem). Nach Austritt der betroffenen Personen werden die Daten noch mindestens 10 Jahre gespeichert (gesetzliche Vorschrift). Werden die Daten danach nicht mehr benötigt, werden diese gelöscht, ohne Information an die betroffenen Personen. Auf Anforderung der betroffenen Personen werden die Daten berichtigt, nicht jedoch vor 10 Jahren nach Austritt gelöscht.

6.2.4 Ausschluss von Einsatzbereichen oder Zwecken der Datenbearbeitung

Die GKK bearbeitet keine Personendaten zu Marketingzwecken, zum Versand von Newsletters, zum Versand via Webseite oder E-Mail-Notifikationen von Informationen und enthält sich auch vollumfänglich von automatischen Kontaktaufnahmen, Meldungen oder Versänden. Die GKK betreibt kein Profiling, Personen-Scanning und versendet keine automatisierten Einzel-entscheidungen, fällt auch keine automatischen Einzelentscheidungen. Die GKK betreibt keine automatisierte Bearbeitung von Personendaten und analysiert keine persönlichen Aspekte oder das Verhalten von Personen. Die GKK bearbeitet keine Personendaten für Risikoprüfungen, zur Definition von Prämien via Risikoprofil, für Bonitätsprüfung, für die Durchführung von Kundenumfragen sowie deren Auswertung, erstellt keine Kundensegmente und -profile und bearbeitet keine Personendaten zur Überwachung von Personen oder Bereichen, bzw. öffentlich zugänglichen Bereichen oder zum Ausspionieren des Verhaltens oder des Aufenthaltsortes von Personen und auch nicht zur Verwendung, bzw. Weiterbearbeitung automatisch erfasster Daten über die Webseite.

6.3 Dokumentation und Art der Ablage der verwendeten Daten

Daten der Kategorie 1 (hoher Schutzbedarf)

- Entsprechende Daten (Daten über die Gesundheit mit medizinisch, diagnostischem Inhalt über versicherte Personen) werden physisch (in Papierform – von Ärtzten:innen) oder elektronisch (auf CD – von anderen Sozialversicherungen) und nur in Ausnahmefällen beschafft, zur Kenntnis genommen und gespeichert und nach Abklärung der Sachverhalte und Tatbestände vernichtet, sobald diese zur Erfüllung der geschäftlichen Pflichten der GKK nicht mehr benötigt werden. Solche Daten werden bei der GKK gespeichert, nicht anderweitig bearbeitet und nur an gesetzlich Berechtigte weitergeleitet.
- Entsprechende Daten werden einzig im Falle unklarer oder unvollständiger Angaben auf den Arbeitsunfähigkeitsausweisen der behandelnden Ärzte:innen oder Heilungsinstituten oder anderen Versicherungsanstalten der versicherten Personen gemäss Art 28, Abs. 3 ATSG angefordert.
- Solche Fälle sind:
    - Offensichtlich unvollständige Abklärungen seitens der Unfallversicherer oder inkonsistenter Angaben von Ärzten oder Heilinstituten der versicherten Personen, Unfall-, Krankenpflege- und/oder Arbeitslosenversicherungen zur Frage, ob die Ursache für eine Arbeitsunfähigkeit auf einen Unfall oder eine Krankheit zurückzuführen ist.
    - Unklare oder potentiell irreführende Angaben darüber, ob die Ursache für eine Arbeitsunfähigkeit auf einen Unfall oder eine Krankheit zurückzuführen ist, führen zur Einforderung per Standardschreiben einer groben Diagnose (Verletzung und Körperteil/ Erkrankungsart), zwecks Prüfungs- und Beurteilungsbefähigung der GKK, ob die Arbeitsunfähigkeit durch einen Unfall/ eine Berufskrankheit entstanden ist oder ob es sich bei der Ursache der Arbeitsunfähigkeit um eine Krankheit im Sinne von Art 1a KVG i.V.m. Art. 3 und Art. 4 ATSG handelt. Ist diese Frage aufgrund ungenügender Angaben nicht zu beantworten, fordert die GKK regelmässig einen ausführlicheren Bericht bei der/dem behandelnden Ärztin/Arzt, bzw. anderen Versicherungsanstalt an oder zieht gemäss Art. 57 KVG

und Art. VII, Ziff. 2 des Versicherungsreglements der GKK einen zweiten Vertrauensarzt bei. Gemäss Art 28, Abs. 3 ATSG sind die beteiligten Stellen zur Erteilung von Auskünften, die für die Abklärung von Leistungsansprüchen erforderlich sind verpflichtet. Ferner dürfen gemäss Art. 57, Abs. 2 KVG nur diejenigen Angaben gemacht werden, die notwendig sind, um über die Leistungspflicht zu entscheiden, die Vergütung festzusetzen, den Risikoausgleich zu berechnen oder eine Verfügung zu begründen. Dafür, dass die GKK diese Angaben über eine versicherte Person in casu einfordern (und selbst weiterleiten) darf, unterzeichnen alle bei der Versicherung Leistungsberechtigte eine Einwilligung mit Vollmachtserteilung zugunsten der GKK, mit welcher sie Ärzte, Krankenkassen und öffentliche Versicherungsträger sowie unsere Kasse ermächtigen, über ihren Gesundheitszustand Auskunft zu erteilen.

! Merkpunkt:

- Fehlende Angaben darüber, ob die Ursache für eine Arbeitsunfähigkeit auf einen Unfall oder eine Krankheit zurückzuführen ist, führen zur Einforderung eines korrekten Arbeitsunfähigkeitsausweises mit den fehlenden Angaben, nicht zur Einforderung medizinisch diagnostischer oder therapeutischer Daten.
- Fehlende Angaben des Grades der Arbeitsunfähigkeit führen zur Einforderung eines korrekten Arbeitsunfähigkeitsausweises mit den fehlenden Angaben, nicht zur Einforderung medizinisch diagnostischer oder therapeutischer Daten.
- Fehlende Angaben zu Beginn, Dauer und Ende der Arbeitsunfähigkeit führen zur Einforderung eines korrekten Arbeitsunfähigkeitsausweises mit den fehlenden Angaben, nicht zur Einforderung medizinisch diagnostischer oder therapeutischer Daten.

Daten der Kategorie 2 (mittlerer Schutzbedarf)

- Entsprechende Daten werden physisch (in Papierform) und elektronisch in Arbeitsdokumenten und in der eigens für die GKK geschaffenen Applikation (Software) aufgenommen, bearbeitet, zwecks Weiterleitung exportiert und daraus zwecks endgültiger Vernichtung entnommen. Die Dokumentation erfolgt in Arbeitsdokumenten
  (a) Stammdatenablage mit Lohnsummen- und Gehaltsangaben, Zahlungsverbindungen, Prämien und Leistungen, Arbeitgeberangaben in elektronischer Form,
  b) Korrespondenz mit anderen Versicherern, Zahlungsanweisungen und Zahlungseingangsbelege, Debitorenrechnungen, Taggeldabrechnungen in elektronischer und physischer Form,
  c) Taggeldausweise, Arbeitsunfähigkeitsausweise, in physischer Form)

Daten der Kategorie 3 (geringer oder kein Schutzbedarf)

- Entsprechende Daten werden physisch (in Papierform) und elektronisch in Arbeitsdokumenten und in der eigens für die GKK geschaffenen Applikation (Software) sowie per Webseite der GKK aufgenommen, bearbeitet, zwecks Weiterleitung exportiert und daraus zwecks endgültiger Vernichtung entnommen. Die Dokumentation erfolgt in Arbeitsdokumenten
  (a) Stammdatenablage mit Anschriften, Namen, Adressen, Ansprechpersonen, Geburtstagen der versicherten Personen, Logfiles mit Erhebung der IP-Adresse des Computers der Besucher:innen unserer Webseite, die Anfrage deren Browser sowie die Zeit dieser Anfrage, den Status und die übertragene Datenmenge im Rahmen der Anfragen, Produkt- und Versionsinformationen über den verwendeten Browser und das Betriebssystem des Computers der Besucher:innen unserer Webseite und Buchungen der Rechnungslegung in elektronischer Form,
  b) Korrespondenz in elektronischer und physischer Form,
  c) keine Daten in nur physischer Form)

7 Dokumentations- und Datenbearbeitungsmittel, Verzeichnisse, Zuständigkeiten

7.1 Struktur Ablage- und Datenbearbeitungsmittel

Bei der GKK werden Daten einerseits in physischer Form (Papier) und andererseits in elektronischer Form bearbeitet.

7.2 Physische Ablage- und Datenbearbeitungsmittel

Wie in Kapitel 6.3 oben dargelegt, werden folgende Daten bei der GKK in physischer Form bearbeitet und gespeichert:

Daten der Kategorie/ Sicherheitsstufe 1

- Schriftliche Korrespondenz mit Kunden, die fälschlicherweise Informationen zur Gesundheitssituation einer versicherten Person enthalten
- Schriftliche Korrespondenz mit versicherten Personen, die fälschlicherweise Informationen zur Gesundheitssituation einer versicherten Person enthalten
- Schriftliche Korrespondenz mit Ärzten:innen und Heilbehandlungsinstituten von versicherten Personen mit Informationen zur Gesundheitssituation einer versicherten Person (Arztberichte)
- Schriftliche Korrespondenz mit Unfall-, Krankenpflege-, und Arbeitslosenversicherungen von versicherten Personen mit Informationen zur Gesundheitssituation einer versicherten Person (Informationen über konkrete gesundheitsrelevante Folgen eines Unfalls oder einer Krankheit einer versicherten Person)

Die oben genannten Dokumente und Informationen werden der GKK fälschlicherweise zugestellt oder von der GKK per E-Mail, Telefon oder einfachem Brief durch den/die zuständige/n Sachbearbeiter/in der Geschäftsstelle angefordert/ beschafft. Briefe werden abgelegt. Nach Eingang der erhobenen Daten/Dokumente, werden diese physisch, in der Form von in Ordnern bis zur definitiven Klärung der für die GKK relevanten Sachverhalte in den Büroräumlichkeiten der Geschäftsstelle bei dem/der zuständigen Sachbearbeiter/in archiviert. Nach der definitiven Klärung der Sachverhalte, werden Daten der Kategorie/ Sicherheitsstufe 1 bei der GKK sicher verwahrt oder durch den/die zuständige/n Sachbearbeiter/in der Geschäftsstelle vernichtet.

Zuständigkeit für die Erhebung, Aufnahme, Speicherung, Weiterreichung und Archivierung der oben genannten Dokumente und Informationen: Sachbearbeiter/in GKK unter Anweisung des Geschäftsführers.

Daten der Kategorie/ Sicherheitsstufe 2

- Schriftliche Korrespondenz mit Kunden mit mittelmässig schützenswertem Inhalt
- Schriftliche Korrespondenz mit versicherten Personen mit mittelmässig schützenswertem Inhalt
- Schriftliche Korrespondenz mit Ärzten:inne und Heilbehandlungsinstituten von versicherten Personen mit mittelmässig schützenswertem Inhalt
- Schriftliche Korrespondenz mit Unfall-, Krankenpflege-, und Arbeitslosenversicherungen von versicherten Personen mit mittelmässig schützenswertem Inhalt
- Zahlungsanweisungen an Geldinstitute, bei denen die GKK Konten unterhält
- Zahlungseingangsbelege von Geldinstituten, bei denen die GKK Konten unterhält
- Debitorenrechnungen
- Taggeldabrechnungen in physischer Form

- Taggeldausweise
- Arbeitsunfähigkeitsausweise
- Schriftliche Korrespondenz mit IT-Lieferanten der GKK welche Informationen über die Systeme, deren Konfiguration und Zugangsdaten enthält.

Die oben genannten Dokumente und Informationen werden bei der GKK per E-Mail, Telefon oder einfachem Brief durch den/die zuständige/n Sachbearbeiter/in der Geschäftsstelle angefordert/ beschafft oder elektronisch geschaffen und ausgedruckt. Briefe werden abgelegt. Nach Eingang /Erschaffung der erhobenen Daten/Dokumente, werden diese physisch, in der Form von in Ordnern abgelegten Dokumenten in den Büroräumlichkeiten der Geschäftsstelle bei dem/der zuständigen Sachbearbeiter/in archiviert und sicher verwahrt.

Zuständigkeit für die Erhebung, Aufnahme, Speicherung, Weiterreichung und Archivierung der oben genannten Dokumente und Informationen: Sachbearbeiter/in GKK unter Anweisung des Geschäftsführers.

Daten der Kategorie/ Sicherheitsstufe 3

- Schriftliche Korrespondenz mit Kunden mit geringfügig schützenswertem Inhalt
- Schriftliche Korrespondenz mit versicherten Personen mit geringfügig schützenswertem Inhalt
- Schriftliche Korrespondenz mit Ärzten und Heilbehandlungsinstituten von versicherten Personen mit geringfügig schützenswertem Inhalt
- Schriftliche Korrespondenz mit Unfall-, Krankenpflege-, und Arbeitslosenversicherungen von versicherten Personen mit geringfügig schützenswertem Inhalt
- Öffentliche Daten ohne schützenswerten Inhalt

Ferner ohne Sammlungen von Personendaten:

- Protokolle und Aktennotizen der Vorstands- und Mitgliederversammlungen der GKK
- Schriftliche Korrespondenz mit Lieferanten der GKK (Büromaterialien, IT, Drucksachen, Telekommunikation,…)
- Schriftliche Korrespondenz mit Geldinstituten, bei denen die GKK Konten oder Analgendepots unterhält mit geringfügig schützenswertem Inhalt
- Schriftliche Korrespondenz zwischen den Organen der GKK (insbesondere Geschäftsstelle – Kontrollstelle) mit geringfügig schützenswertem Inhalt
- Jahresabschlüsse und Jahresberichte, öffentliche oder interne Konzepte und Richtlinien, Reglemente, etc.

Die oben genannten Dokumente und Informationen werden bei der GKK per E-Mail, Telefon oder einfachem Brief durch den/die zuständige/n Sachbearbeiter/in der Geschäftsstelle angefordert/ erhoben oder elektronisch geschaffen und ausgedruckt. Briefe werden abgelegt. Nach Eingang /Erschaffung der erhobenen Daten/Dokumente, werden diese physisch, in der Form von in Ordnern abgelegten Dokumenten in den Büroräumlichkeiten der Geschäftsstelle bei dem/der zuständigen Sachbearbeiter/in archiviert und sicher verwahrt.

Zuständigkeit für die Erhebung, Aufnahme, Weiterreichung und Archivierung der oben genannten Dokumente und Informationen: Sachbearbeiter/in GKK unter Anweisung des Geschäftsführers.

7.3 Elektronische Ablage- und Datenverarbeitungsmittel, IT-gestützte Prozesse

Wie in Kapitel 6.3 oben dargelegt, werden folgende Daten bei der GKK in elektronischer Form bearbeitet und archiviert:

Daten der Kategorie/ Sicherheitsstufe 1

Daten der Kategorie/ Sicherheitsstufe 1 können durch den/die zuständige/n Sachbearbeiter/in der GKK via E-Mail, Telefon oder einfachem E-Brief angefordert werden. Diese Anforderungen enthalten keine Daten der Kategorie/ Sicherheitsstufe 3.

Daten der Kategorie/ Sicherheitsstufe 1 werden bei der GKK auch in elektronischer Form aufgenommen, gespeichert, eingesehen und archiviert. Weitere Bearbeitung der besonders schützenswerten Daten (verändern, weiterreichen) erfolgt bei der GKK mit diesen nicht.

Zuständigkeit für das korrekte Verfahren der oben genannten Dokumente und Informationen, gemäss dieser Weisung/Regelung: Sachbearbeiter/in GKK unter Anweisung und Aufsicht des Geschäftsführers/ Verantwortlichem Datenschutz.

Daten der Kategorie/ Sicherheitsstufe 2

- Schriftliche Korrespondenz mit Kunden mit mittelmässig schützenswertem Inhalt per E-Mail und in der elektronischen Datenablage in Microsoft Outlook Local Storage und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK
- Schriftliche Korrespondenz mit versicherten Personen mit mittelmässig schützenswertem Inhalt per E-Mail und in der elektronischen Datenablage in Microsoft Outlook Local Storage und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK
- Schriftliche Korrespondenz mit Ärzten und Heilbehandlungsinstituten von versicherten Personen mit mittelmässig schützenswertem Inhalt (Arbeitsunfähigkeitsbestätigungen) per E-Mail und in der elektronischen Datenablage in Microsoft Outlook Local Storage und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK
- Schriftliche Korrespondenz mit Unfall-, Krankenpflege-, und Arbeitslosenversicherungen von versicherten Personen mit mittelmässig schützenswertem Inhalt (Daten zum Grad, der Dauer, dem Beginn und dem Ende und der Ursache Krankheit oder Unfall einer Arbeitsunfähigkeit einer versicherten Person) per E-Mail und in der elektronischen Datenablage in Microsoft Outlook Local Storage und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK
- Stammdaten der Kunden und der versicherten Personen wie Anschrift, Firma, Name, Adresse, Ort, Geburtsdaten, Anstellungsort mit Lohnsummen je Kunde oder AHV-Bruttolöhnen von versicherten Personen in der Software „GKK-Applikation“ durch den/die zuständige/n Sachbearbeiter/in der Geschäftsstelle der GKK
- Zahlungsanweisungen an Geldinstitute, bei denen die GKK Konten unterhält per elektronischem Datentransfer aus und in der Software „GKK-Applikation“ durch den/die zuständige/n Sachbearbeiter/in der Geschäftsstelle der GKK
- Zahlungseingangsbelege von Geldinstituten, bei denen die GKK Konten unterhält per elektronischem Datentransfer in die Software „GKK-Applikation“ und die Rechnungswesen-Applikation Infoniqa One 50 Finanz, durch den/die zuständige/n Sachbearbeiters/in der Geschäftsstelle der GKK
- Debitorenrechnungen in der Software „GKK-Applikation“ durch den/die zuständige/n Sachbearbeiters/in der Geschäftsstelle der GKK
- Errechnete Prämien der Kunden und Taggeldleistungen zu Gunsten der versicherten Personen in der Software „GKK-Applikation“ durch den/die zuständige/n Sachbearbeiter/in der Geschäftsstelle der GKK
- Taggeldausweise aus der Software „GKK-Applikation“ durch den/die zuständige/n Sachbearbeiter/in der Geschäftsstelle der GKK
- Sicherheitsprotokolle durch die IT-Lieferanten der GKK per Mail durch den/die zuständige/n Sachbearbeiter/in der Geschäftsstelle der GKK

Die oben aufgeführten Daten und Informationen werden bei der GKK per E-Mail, Telefon oder einfachem E-Brief durch den/die zuständige/n Sachbearbeiter/in der Geschäftsstelle angefordert/ erhoben oder elektronisch in E-Dokumenten (Microsoft Word, Excel) oder in der Software „GKK-Applikation“ bearbeitet und archiviert. Nach Beschaffung der erhobenen Daten/Dokumente, werden diese auf dem hauseigenen Server, auf dem persönlichen Laufwerk und dem PC des/der zuständigen Sachbearbeiter/in in den Büroräumlichkeiten der Geschäftsstelle gespeichert und archiviert. Ein Zugriff über das Internet von aussen oder von ausserhalb der Geschäftsstelle mittels virtuellem Arbeitsplatz oder ähnlichem ist nicht existent. Zugriff hat der Geschäftsführer/ Verantwortlicher Datenschutz der GKK.

Zuständigkeit für die Erhebung, Aufnahme, Bearbeitung, Speicherung, Weiterreichung und Archivierung der oben genannten Dokumente und Informationen: Sachbearbeiter/in GKK unter Anweisung und Aufsicht des Geschäftsführers.

Daten der Kategorie/ Sicherheitsstufe 3

- Schriftliche Korrespondenz mit Kunden mit geringfügig schützenswertem Inhalt per E-Mail und in der elektronischen Datenablage in Microsoft Outlook Local Storage und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK
- Schriftliche Korrespondenz mit versicherten Personen mit geringfügig schützenswertem Inhalt per E-Mail und in der elektronischen Datenablage in Microsoft Outlook Local Storage und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK
- Schriftliche Korrespondenz mit Ärzten und Heilbehandlungsinstituten von versicherten Personen mit geringfügig schützenswertem Inhalt per E-Mail und in der elektronischen Datenablage in Microsoft Outlook Local Storage und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK
- Schriftliche Korrespondenz mit Unfall-, Krankenpflege-, und Arbeitslosenversicherungen von versicherten Personen mit geringfügig schützenswertem Inhalt per E-Mail und in der elektronischen Datenablage in Microsoft Outlook Local Storage und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK

Ferner ohne Sammlungen von Personendaten:

- Protokolle und Aktennotizen der Vorstands- und Mitgliederversammlungen der GKK per E-Mail und in der elektronischen Datenablage in Microsoft Outlook Local Storage und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK
- Schriftliche Korrespondenz mit Lieferanten der GKK (Büromaterialien, IT, Drucksachen, Telekommunikation, …) per E-Mail und in der elektronischen Datenablage in Microsoft Outlook Local Storage und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK
- Schriftliche Korrespondenz mit Geldinstituten, bei denen die GKK Konten oder Anlagendepots unterhält mit geringfügig schützenswertem Inhalt per E-Mail oder elektronisch-automatischem Datentransfer (E-ESR) und in der elektronischen Datenablage in Microsoft Outlook Local Storage und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK

- Schriftliche Korrespondenz zwischen den Organen der GKK (insbesondere Geschäftsstelle – Kontrollstelle) mit geringfügig schützenswertem Inhalt per E-Mail und in der elektronischen Datenablage in Microsoft Outlook Local Storage und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK
- Jahresabschlüsse und Jahresberichte, Konzepte und weitere öffentliche Dokumente, Reporting an die Aufsichtsbehörde BAG per E-Mail und in der elektronischen Datenablage in Microsoft Outlook Local Storage und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK
- Logfiles und Registrierung der IP-Adressen und weiteren Maschinendaten der Besucher:innen der Webseite der GKK Bern mit geringfügig oder nicht schützenswertem Inhalt

Die oben aufgeführten Daten und Informationen werden bei der GKK per E-Mail, Telefon oder einfachem E-Brief durch den/die zuständige/n Sachbearbeiter/in der Geschäftsstelle beschafft oder erschaffen oder elektronisch in E-Dokumenten (Microsoft Word, Excel) oder in der Software „GKK-Applikation“ bearbeitet und archiviert. Nach Eingang /Erschaffung der erhobenen Daten/Dokumente, werden diese auf dem hauseigenen Server, auf dem Laufwerk und dem PC des/der zuständigen Sachbearbeiters/in in den Büroräumlichkeiten der Geschäftsstelle gespeichert und archiviert. Ein Zugriff über das Internet von aussen oder von ausserhalb der Geschäftsstelle mittels virtuellem Arbeitsplatz oder ähnlichem ist nicht existent. Zugriff hat der Geschäftsführer/ Verantwortlicher Datenschutz.

Zuständigkeit für die Bearbeitung und Archivierung der oben genannten Dokumente und Informationen: Sachbearbeiter/in GKK unter Anweisung und Aufsicht des Geschäftsführers.

Verzeichnisse der elektronischen Datenablage der GKK sind folgende:
- GKK-Applikation (Verantwortung: Geschäftsführer/ Verantwortlicher Datenschutz, enthaltend Daten von Firmen und Personen: Geheime Daten (2a), Vertrauliche Daten (2b) und interne Daten (2c). Im CRM-Tool sind Fragmente von besonders schützenswerten Daten enthalten. Für die GKK-Applikation sind daher die höchsten Massnahmen puncto Datensicherheit angewendet. Daten werden täglich bearbeitet. Empfänger der Daten sind ausschliesslich die Sachbearbeiter:innen GKK und der Geschäftsführer. Besonders schützenswerte Daten werden nicht verändert und nicht weitergeleitet.)
- GKK-Datenablage Server (Verantwortung: Geschäftsführer/ Verantwortlicher Datenschutz, enthaltend Daten von Firmen und Personen: Geheime Daten (2a), Vertrauliche Daten (2b) und interne Daten (2c). In der GKK-Datenablage sind besonders schützenswerten Daten enthalten. Für die GKK-Datenablage sind daher die höchsten Massnahmen puncto Datensicherheit angewendet. Daten werden täglich bearbeitet. Empfänger der Daten sind die Sachbearbeiter:innen GKK und der Geschäftsführer. Besonders schützenswerte Daten werden nicht verändert und nicht weitergeleitet.)
- GKK Microsoft Outlook Local Storage (Verantwortung: Geschäftsführer/ Verantwortlicher Datenschutz, enthaltend Daten von Firmen und Personen: Geheime Daten (2a), Vertrauliche Daten (2b) und interne Daten (2c). In der GKK Outlook-Applikation sind keine besonders schützenswerten Daten enthalten. Angewendet werden Massnahmen mittlerer Strenge puncto Datensicherheit. Daten werden täglich bearbeitet. Empfänger der Daten sind die Sachbearbeiter:innen GKK und der Geschäftsführer.)
- GKK-Rechnungslegung in Infoniqa One 50 Finanz (Verantwortung: Geschäftsführer/ Verantwortlicher Datenschutz, enthaltend Daten von Firmen und Personen: Geheime Daten (2a), Vertrauliche Daten (2b) und interne Daten (2c). In der GKK-Rechnungs-legungs-Applikation Infoniqa One 50 Finanz sind keine besonders schützenswerten Daten enthalten. Angewendet werden Massnahmen mittlerer Strenge puncto Datensicherheit. Daten werden wöchentlich bearbeitet. Empfänger der Daten sind die Sachbearbeiter:innen GKK und der Geschäftsführer sowie die Drittfirma Gewerbetreuhand AG Bern, welche der GKK Rechnungslegungs-Support liefert.)

Folgende Hauptprozesse der Kernprozesse der GKK sind in dem Sinne IT-gestützt, als dass die IT-Automation der integrierten Systeme „GKK-Applikation“ und die Rechnungswesen-Applikation Infoniqa One 50 Finanz die Prozesse sowie die elektronische Ablage unterstützen:

Abbildung 5: Hauptprozesse und IT-Unterstützung

Die Hauptprozesse ohne gelbe Färbung (inkl. aller Einzelentscheidungen), werden ohne integrierte IT-Unterstützung vorgenommen. Einfache, elektronisch erstellte Dokumente oder E-Mails werden elektronisch und/oder in Papierform gespeichert und archiviert.

7.3.1 IT-Architektur

Die folgende Abbildung zeigt die Komponenten der IT-Systeme und IT-Umsysteme der GKK, wobei die blau hinterlegten Komponenten die Datenträger der GKK-internen Systeme, die rosa hinterlegten Komponenten assoziierte, aussenstehende Umsysteme darstellen.

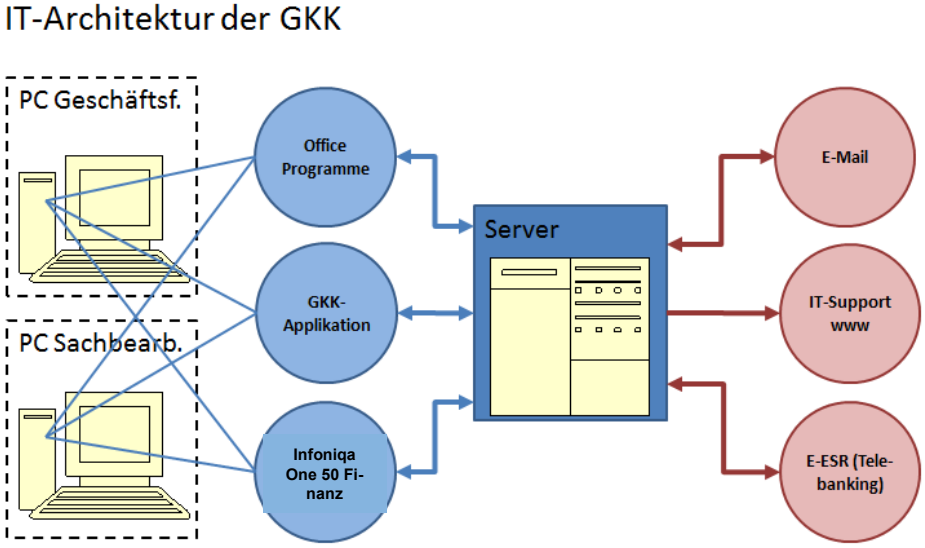

Abbildung 6: IT-Architektur GKK

Die gelblich eingefärbten Symbole stellen Hardware dar, die anderen Komponenten mit blauer bzw. rosafarbener Hinterlegung Software, die eckige blaue Komponente steht für den Server und das Betriebssystem.
Die Pfeile stehen für Schnittstellen, über welche Daten von einer Komponente in eine andere übertragen werden. Die Pfeilrichtungen zeigen an, ob eine Komponenten Informationen an eine andere liefert oder empfängt oder beides. Sicherheitstechnisch ist hierbei von Belang, dass der Server der GKK nur dann Datenempfang aus dem Internet zulässt, wenn ein solcher angefordert und abgerufen wird. Der GKK-Server ist nicht im Internet öffentlich zugänglich sondern als Binnensystem ausgestaltet. Auf diesen kann von ausserhalb der GKK-Systeme nur durch stark verschlüsselte Sicherheitszertifikate zugegriffen werden (IT-Server-Support).

7.3.2 Hardware und Betriebssystem

Die Hardware besteht aus dem Server und den PCs je Arbeitsplatz.

Daten werden über die PCs auf dem Server aufgerufen und können mittels der gängigen Software bearbeitet und gespeichert werden.

Der Server verfügt über eine integrierte Backup-Harddisk zum Schutze vor Datenverlust.

Der Server ist mit einem integrierten Sicherheitssystem gegen Malware aus dem Internet ausgerüstet. Eine VPM-Verschlüsselung sichert den Zugang vom Server gegen Zugriffe von ausserhalbstehenden Systemen.

Bei Bedarf können dem Server Sicherheitsprotokolle über jeden Zugriff (mit Identifikation der zugreifenden Stelle, Datum, Bearbeitungsmenge) entnommen werden.

Beschreibung des Servers durch den Hersteller:

Symantec Endpoint Protection Small Business Edition

Symantec Endpoint Protection Small Business Edition, managed on-premise, protects your computers and servers with the most effective small business antivirus, anti-malware technologies available in a single, integrated solution. It will not slow you down or swallow up system resources. From the world leader in security, Symantec's Mac and PC security software solution allows you to stay focused on growing your business knowing that your data is safe from cybercriminals.

Key Features

- Symantec Insight and SONAR technologies detect new and rapidly mutating malware, stopping malicious behavior, including new and previously unknown threats.
- Comprehensive small business antivirus protection – and defense against worms, Trojans, spyware, bots, zero-day threats and root kits.
- Rules-based firewall engine, Browser Protection and Generic Exploit Blocking (GEB) shields systems from drive-by downloads and from network based attacks.
- Centrally manages servers, PCs and Macs; consolidates antivirus, antispyware, desktop firewall, and Intrusion Prevention on a single agent.

Key Benefits

- **Fastest**[1] Increase productivity with small business antivirus and security software that won't slow you down, get in your way, or swallow up system resources.
- **Most Effective**[2] Protect your business with the most-effective threat detection technology so you can focus your attention on growing your business.
- **Simple** Save time and costs with a single console that provides Mac and PC security for all your computers and servers.

Das verwendete Betriebssystem ist Microsoft Windows 2019.

Auf der Webseite der GKK sind keine Personendaten enthalten, bis auf die kurzzeitig gespeicherten Logfiles von Besucher:innen der Webseite, welche keinen direkten Rückschluss auf eine natürliche Person gewähren.

7.3.3 Software

An den Arbeitsplätzen des:der zuständigen Sachbearbeiters:in und des Geschäftsführers stehen folgende Applikationen zum Zugriff, der Anpassung und Bearbeitung der GKK-Daten zur Verfügung:

- GKK-Applikation (Hauseigene Applikation zur operativen Administration der Krankentaggeldversicherung der GKK (Kerngeschäft). Hier werden alle Geschäftsdaten bis auf Korrespondenz und Buchhaltung geführt.

  Kunden- und versichertenspezifische Daten werden nur folgende geführt: Anschrift, Firma, Namen, Adresse, Lohnsummen, Prämien, Bruttogehälter versicherter Personen, Taggeldleistungen, Anzahl Tage Arbeitsunfähigkeit, Zahladressen, Zahlungseingänge, Auszahlungen. Daten über medizinisch diagnostische oder rechtliche Sachverhalte, wie auch Daten über das Kundenverhalten sind in der GKK-Applikation nur in Fragmenten im CRM-Tool enthalten)

- Infoniqa One 50 Finanz(Software für das Rechnungswesen der GKK ohne Personendaten)

- Microsoft Office-Programme: Word und Excel. (Hier werden Daten der einfachen Korrespondenz, wie auch Daten über Personen bearbeitet. Medizinisch diagnostische oder rechtliche Sachverhalte im Zusammenhang mit Kunden oder versicherten Personen, wie auch Daten über das Kundenverhalten werden zur Abklärung von Leistungspflichten der GKK ebenfalls bearbeitet.)

7.3.4 Die GKK-Applikation

Das Herzstück des Tagesgeschäftes ist wie oben aufgeführt die hauseigene GKK-Applikation. Diese ist ein Datenbank-basiertes Tool und führt die automatisierten Kernprozesse der GKK aus.

Der Aufbau orientiert sich auch an den Prozessen. Eine Hauptmaske ist für den Prozess „Abwicklung Prämien (Mittelzufluss)“ eine für den Prozess „Abwicklung Leistungen (Mittelabfluss) angelegt. Die einzelnen Funktionen je Prozess sind über den Navigationsbereich am linken Maskenrand abrufbar:

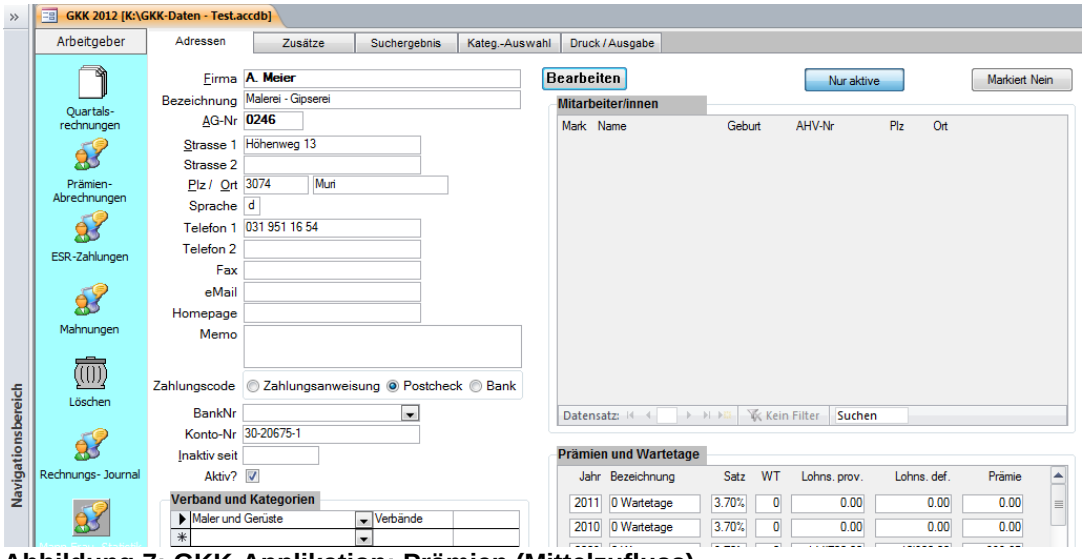

Abbildung 7: GKK-Applikation: Prämien (Mittelzufluss)

Sämtliche, in der Applikation für den betreffenden Prozess erhobenen, aufgenommenen, bearbeitbaren, weiterreichbaren und archivierbaren Datenobjekte sind auf der abgebildeten

Maske „Quartalsrechnungen“ ersichtlich. Ausnahme: Lohnsummenangabe, Prämienberechnung, Fälligkeitsdaten und Zahlungseingangsdaten (auf den Masken „Prämienabrechnungen“, „ESR-Zahlungen“, „Mahnungen“, „Rechnungsjournal“ und „Kontoblatt“ enthalten).

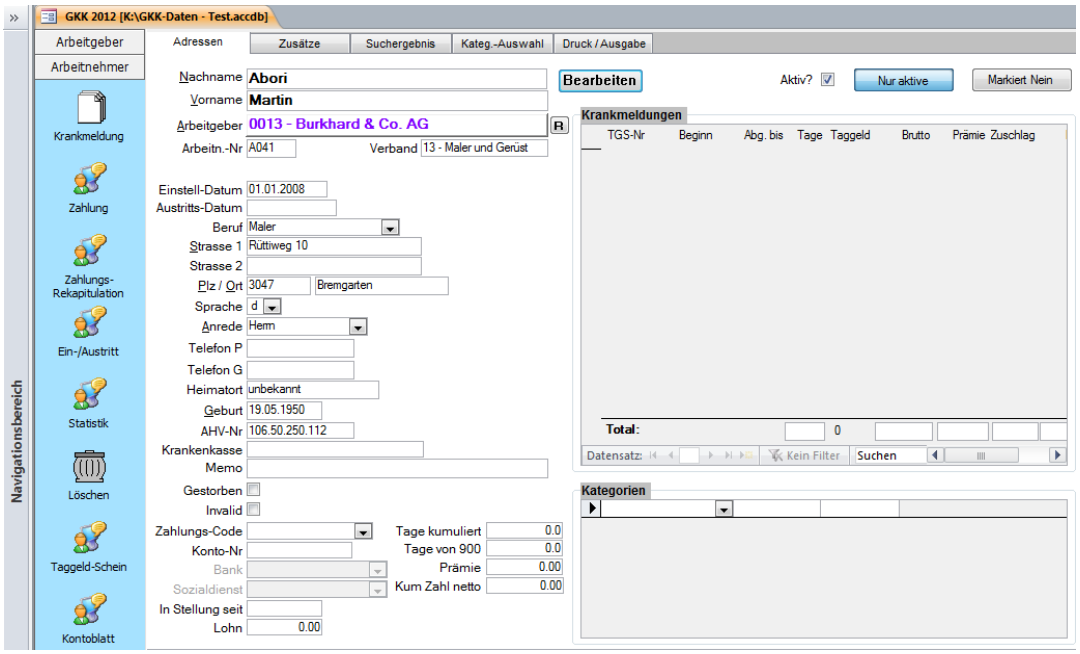

Abbildung 8: GKK-Applikation: Leistungen (Mittelabfluss)

Sämtliche, in der Applikation für den betreffenden Prozess erhobenen, aufgenommenen, bearbeitbaren, weiterreichbaren und archivierbaren Datenobjekte sind auf der Maske Krankmeldung ersichtlich. Ausnahme: Anzahl Tage Arbeitsunfähigkeit, Grad der Arbeitsunfähigkeit, Taggeldberechnung, Eintritte und Austritte, Fälligkeitsdaten und Auszahlungsdaten (auf den Masken „Zahlung“, „Zahlungs-Rekapitulation“, „Ein-/Austritt“, „Statistik “, „Taggeldschein“ und „Kontoblatt“ enthalten).

7.4 Sicherung der Dokumentations- und Datenbearbeitungsmittel

Schutzbedarf (s. Kapitel 6 und 7 oben):

Der Grossteil der bearbeiteten, gespeicherten und archivierten Daten unterliegt einem geringen Schutzbedarf (Kategorie/ Sicherheitsstufe 3).

Ein weiterer substantieller Teil der erhobenen, bearbeiteten, gespeicherten, weitergereichten, und archivierten Daten unterliegt einem Mittleren Schutzbedarf (Kategorie/ Sicherheitsstufe 2).

Ein marginaler Teil der beschafften, eingesehenen und gespeicherten (nicht anderweitig bearbeiteten) Daten unterliegt einem hohen Schutzbedarf (Kategorie/ Sicherheitsstufe 1).

Zu unterscheiden ist die organisatorische von der technischen (IT-bezogenen) Sicherung der Daten.

7.4.1 Organisatorische Sicherung

Zugang, Bearbeitung, Speicherung, Archivierung, Vernichtung

Die Datensammlungen der GKK befinden sich ausschliesslich in den Büroräumlichkeiten der Geschäftsstelle. Die Liegenschaft an der Neuengasse 20 verfügt über einen räumlichen Zugang (Treppenhaus).

Der Hauszugang ist mit einer abschliessbaren Türe versehen. Diese ist nur zu Bürozeiten (08:00 bis 17:00) ohne Schlüssel zugänglich. Der Personenkreis der mit Schlüssel Zugang hat ist bekannt. Das Stockwerk, auf dem sich die Büroräumlichkeiten der GKK befinden, ist mit einer gesicherten Türe mit automatischem Schliessmechanismus vom Treppenhaus getrennt. Diese Türe ist nur während den Büroblockzeiten (08:00 bis 11:30 und 13:30 bis 16:30) nicht verriegelt. Ansonsten ist sie mit einem code- und schlüsselgesicherten Schliesszylinder verschlossen. Der zugangsberechtigte Personenkreis ist auf 15 bekannte Personen eingeschränkt, welche einer vertraglichen Geheimhaltungspflicht unterstellt sind.

Die Datenablagen der GKK befinden sich in physischer Form in einem Büroraum mit zwei Mitarbeiter:innen, der datentragende Server in einem abschliessbaren Wandschrank. Letzterer wird nur bei Störungen durch den Lieferanten (Comtool GmbH, Herr R. Flückiger) oder den zuständigen Mitarbeitern:innen der GKK) geöffnet. Neben diesen Personen besitzt auch der Geschäftsführer/ Verantwortlicher Datenschutz einen Schlüssel.

Während den Büroblockzeiten sind sämtliche Datenablagen dauernd durch Mitarbeiter:innen der GKK und der Gewerbetreuhand AG Bern überwacht. Ein unbemerktes Eindringen einer nicht berechtigten Person in die Räumlichkeiten der Datenablagen kann damit ausgeschlossen werden.

Ausserhalb der Büroblockzeiten sind die oben erwähnten Hauseigangs- und Stockwerktrennungstüre verriegelt und Dritten nicht offen.

Die Dokumentenablagen (Ordner, Papiere) sind folgendermassen aufbewahrt:

- Die aktuellen Ordner des laufenden Jahres zur Vornahme des Tagesgeschäfts, stehen neben vielen andern, nicht der GKK zugehörigen Ordnern, hinter dem Arbeitsplatz des:der zuständigen Sachbearbeiters:in in einem Regal.
- Die Ordner mit Dokumenten abgeschlossener Jahre befinden sich in einem abgeschlossenen, tagsüber durch andere Mitarbeiter:innen kontrollierbaren Schrank.

Die Gefahr, dass unberechtigte Dritte, selbst mit entsprechender Absicht, an schützenswerte oder gar besonders schützenswerte Daten gelangen, kann ausgeschlossen werden.

In den oben beschriebenen Räumlichkeiten sind die Datenablagen verwahrt.

Weitergabe von Daten

Daten, welche die GKK bearbeitet, speichert und archiviert, werden nur von der:dem zuständigen Sachbearbeiter:in der GKK) und dem Geschäftsführer weitergereicht. Eine Weiterreichung geschieht durch manuelle Vornahme eines Transfers per E-Mail, mündlich, mit schriftlicher Korrespondenz unter kontrollierten Verhältnissen (der Zahlungsverkehr wird mittels elektronischem Datentransfer (manuelle Auslösung) vorgenommen).

Datenvernichtung

Daten werden nur durch den:die zuständige Sachbearbeiter:in unter Aufsicht des Geschäftsführers vernichtet. Für die Vernichtung von Daten mit geringem und mittlerem Schutzbedarf dient ein Altpapiercontainer im Lager- und Postverarbeitungsraum neben den Büroräumlichkeiten. Dokumente mit Daten mit hohem Schutzbedarf, werden mittels Aktenvernichter unleserlich gemacht (Standort im selben Raum wie der Altpapiercontainer).

Zuständigkeiten

Server: IT-Beauftragter GKK, Comtool GmbH, Herr R. Flückiger (Hardware- und Betriebssystemlieferant der GKK), Geschäftsführer:in GKK.

Alle weiteren physischen Datenaufbewahrungsmittel (Ablagen physischer Datenträger und PCs mit Zugriff auf die GKK-Daten: Sekretär:in und Sachbearbeiter:in GKK, Geschäftsführer:in GKK).

7.4.2 Technische Sicherung

Unter Ziffer 7.3 ist detailliert beschrieben, welche Daten in elektronischer Form bearbeitet, gespeichert, archiviert und vernichtet werden sowie die IT-Architektur mit den angeschlossenen und verwendeten Umsystemen (auch Systeme von Dritten) dargestellt.

Zur technischen (im Gegensatz zur physischen) Sicherung der in diesem System ausgetauschten Daten, sind verschiedene Sicherheitsvorkehrungen getroffen. Diese werden hier in der Folge als Sicherheits-Gates bezeichnet und sind in der folgenden Abbildung 9 (IT_Architektur und Sicherheit GKK) ausgewiesen. Die Darstellung zeigt, dass jeder Informationsfluss von den genutzten Arbeitsmitteln der zuständigen Mitarbeiter:innen der GKK zu einer aussenstehenden Stelle mindestens zwei Sicherheits-Gates, für die Kernapplikation der GKK sogar vier Sicherheits-Gates zu überwinden hat:

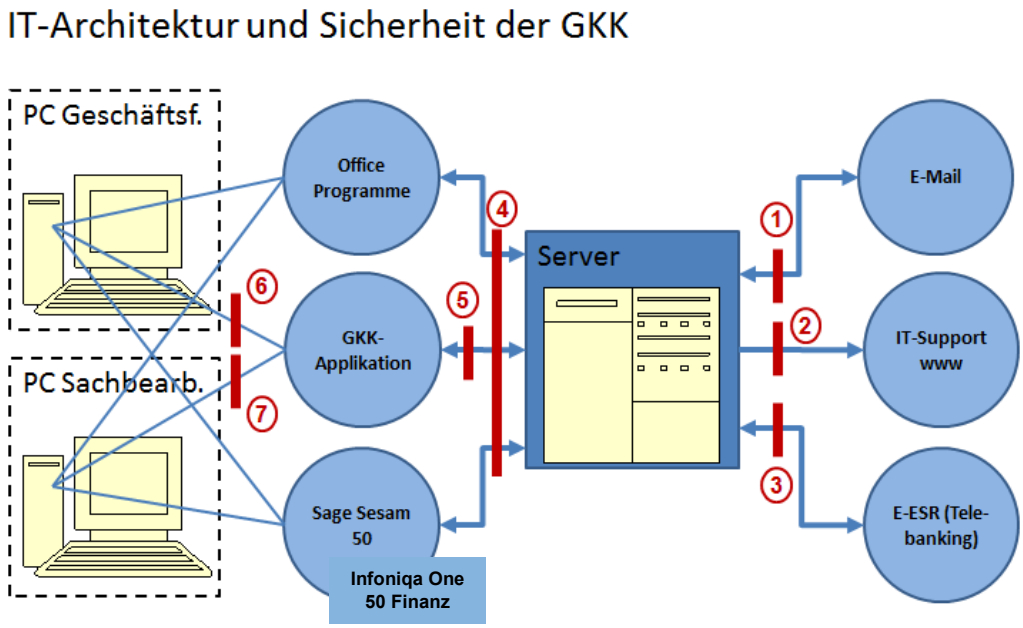

Abbildung 9: IT_Architektur und Sicherheit GKK

Sicherheits-Gates:

1 Elektronische Korrespondenz (möglich mit Anhängen mit Grössenbeschränkung auf max. 10MB) gelangt von aussen zum Server der GKK über ein integriertes System von Firewalls und Antivirussoftware. In den letzten zehn Jahren, seit dem Ersteinsatz dieses Systems ist ein einziges Mal Malware in der Form eines „Wurms“ in den Server und das Betriebssystem der GKK eingedrungen. Der Schaden wurde rasch behoben, die Lücke in der Abwehrsoftware geschlossen. Als Massnahme gegen wiederholtes Aufkommen dieses oder ähnlich gelagerter Probleme wurde die Weisung erlassen: „Anhänge in Mails von unbekannten Absendern werden nicht geöffnet“.

2 Sicherheitsgate 2 umschreibt die Schnittstelle zwischen elektronischen Kommunikationssystemen ausserhalb des Datenverarbeitungssystems der GKK wie das Internet und eine bei Supportbedarf nur unter Mitwirkung der GKK-Mitarbeiter:innen freizugebende Zugriffsmöglichkeit für Softwarelieferanten der GKK (AR Solutions, Ackermann für Infonica, Herr Eduard Lochbronner - Entwickler der GKK-Applikation. Der Server der GKK ist nicht öffentlich auf dem Internet zugänglich. Dieselben Firewalls und Antivirusprogramme wie für Gate 1 schützen den Server und das Betriebssystem der GKK vor Zugriffen durch unberechtigte Dritte. Rein theoretisch könnte über das Internet der

Server durch eine Attacke eines versierten Hackers zufälligerweise geortet und ein Zugang zum Server erstellt werden. Die Bezeichnung und die Sicherheitsprotokolle des Servers lassen allerdings keine Rückschlüsse auf das Geschäft der GKK auf dem betreffenden Server zu.

3 Um Taggeldleistungen auszuzahlen und Eingänge von Prämienzahlungen der Kunden zuzuordnen, bedient sich die GKK einer elektronischen Datenschnittstelle mit der Valiant Bank AG. Taggeldleistungen werden per E-Zahlungsauftrag an diese übertragen und überwiesen, Zahlungseingänge per Datenfile von der Valiant Bank AG gemeldet und in die GKK-Applikation eingelesen. Beide Informationsflüsse werden in einem absolut geschützten Datenkanal abgehandelt.

4 Zugriff zu den Daten auf dem Server wird nur über den dort vorhandenen Applikationen gewährt. Diese sind mit Sicherheitszertifikaten vor dem Zugriff von unberechtigten Personen geschützt.

5 Um auf die Daten der Kernapplikation der GKK zugreifen zu können, muss erstens die Applikation als Software auf einem PC installiert sein (nur bei den PCs der GKK-Datenbearbeitenden und dem Geschäftsführer der Fall) und zweitens eine Benutzeridentifikation abgegeben werden (individueller Benutzername und Passwort).

6 und 7 Zugriff zu den Daten auf dem Server wird nur durch Eingabe eines individuellen Benutzernamen und Passwortes gewährt (Standardsicherung).

Datenbeschaffung, -vernichtung

Wie unter Ziffer 7.3 oben beschrieben, werden Daten der GKK (bis auf die Daten des elektronischen Datentransfers mit Valiant Bank AG - s. Sicherheitsgate 3) nur per Telefon, E-Mail und Brief erhoben. Der Verzicht auf eine weitere IT-integrierte, automatische Datenerhebung reduziert das Sicherheitsrisiko erheblich und erfordert, bis auf den Schutz des E-Mailkanals, keine technische Datenerhebungs-Sicherheitsmassnahme. Die Vernichtung nicht mehr benötigter Personendaten erfolgt nach den Datenschutzgrundlagen gemäss Ziffer 5.1.5.

Sicherung der gespeicherten und archivierten Daten

Neben den oben beschriebenen Datensicherungen bei der Beschaffung, Erschaffung, Veränderung, Weiterleitung von Daten („Sicherheits-Gates“ oben), sind bei der GKK Sicherungen gegen Datenverlust mit den Server- und NAS- Backups (s. Ziffer 7.3.2 oben) eingerichtet. Zudem verfügt die GKK über ein Cloud-Backup der gesamten Daten, auf der in der Schweiz allokierten Backup-Firma Mount10 AG. Die Sicherung genügt höchsten Standards mit dem Abonnement Immutable Cloud Backup. Der Provider Mount10 AG stipuliert u.A.:
Mit Ihrem MOUNT10-Paket sichern Sie sich gegen folgende 10 Punkte ab:

1. Jegliche physische Einwirkung auf Ihre Backup-Infrastruktur; die Daten liegen garantiert ausschliesslich in der Schweiz und zwar im SWISS FORT KNOX I + II
2. Fehlmanipulationen der eigenen Mitarbeiter
3. Unbefugter Zugriff auf private und sensible Daten
4. Vergessen von Datensicherungen
8. Zugriffsverzögerungen im Falle von Ferienabwesenheiten oder bei Ausfall der eigenen Infrastruktur, dank des kostenlosen Supports 24/7 – aus der Schweiz
9. Zeitverzögerungen beim Wiederaufsetzen von geschäftskritischen Servern
10. Unsicherheiten mit Kleinanbietern, da Sie mit der MOUNT10 AG auf den Marktführer setzen

7.4.3 Kontrolle der Sicherungsmassnahmen

Allgemeines und Grundsätzliches zur Kontrolle der Sicherungsmassnahmen

Wie in Ziffer 4.4.2 oben beschrieben, handelt es sich bei der GKK um eine Branchenlösung in der Krankentaggeldversicherung für die Bau- und Baunebenbranchen im Kanton Bern, insbesondere die Maler- und Gipserunternehmen in der Region Bern, um eine Kleinstversicherung.

Für die Ausführung der Hauptprozesse und des operativen Tagesgeschäfts (gemäss Ziffer 4.2, Abbildung 2 oben), sind auf der Geschäftsstelle der:die Sachbearbeiter:innen alleine zuständig. Bei ausserordentlichen Fragestellungen ziehen diese den Geschäftsführer/ Verantwortlicher Datenschutz bei. Diesem obliegen in direkter Zuständigkeit in Bezug auf das Tagesgeschäft und die Ausführung der Hauptprozesse der GKK nur ausserordentliche Aufgaben, ferner die vereinsorganisatorischen Aufgaben (gemäss Aufführung in Ziffer 4.4.2 oben).

Durch den eingeschränkten Umfang der Geschäftstätigkeit, ist diese relativ einfach zu überblicken und zu kontrollieren. Vorliegen entstandener Fehler in der Ausführung des Tagesgeschäfts oder dem Umgang mit Personendaten, werden innerhalb Monatsfrist ohne Meldung durch betroffene Personen oder berechtigte Dritte autonom wahrgenommen und sind einfach zu identifizieren. Zu deren Behebung bedarf es nur in ausserordentlichen Sonderfällen einschneidender Massnahmen und Eingriffen. Bei Meldungen von möglichen Datenschutzverletzungen wird innerhalb von 48 Stunden reagiert.

Zugangskontrolle

Aus dem unter dem Vortitel oben Gesagten ist abzuleiten, dass es neben der physischen Kontrolle durch die Zutrittsbeschränkungen zu den Büroräumlichkeiten und der Sichtkontrolle wenigen stetig vorzunehmenden Zugangskontrollen bedarf. Die Mitarbeiter:innen der GKK Bern haben die Möglichkeit, im Homeoffice mittels gesichertem remote access-Zugang zu arbeiten. Dies wird in den Zugangsprotokollen des Servers verzeichnet und ist jederzeit bei Bedarf nachvollziehbar. Gearbeitet wird ausschliesslich auf betriebseigenen Geräten und zu normalen Büro-Gleitarbeitszeiten zwischen 07:00 und 20:00 Uhr. Auf elektronischem Weg vorgefallene Datenzugriffe durch unberechtigte Dritte auf die Daten der Kategorien/ Sicherheitsstufen 2 und 3, sind bei Bedarf durch die Server-Zugriffsprotokolle kontrollierbar. Werden keine Veränderungen an den bearbeiteten und archivierten Daten vorgenommen, wird ein Zugriff durch unberechtigte Dritte nicht automatisch erkannt. Bei Veränderung dieser Daten jedoch schon. Diese Situation verlangt insofern nach keiner Massnahme als es sich bei den auf diesem Wege einsehbaren Daten nicht um solche mit hohem Schutzbedarf handelt. Besonders schützenswerte Daten werden durch die GKK nur - und nur in Ausnahmefällen - beschafft, eingesehen und archiviert, desweitern nicht bearbeitet. Sollten solche Daten durch betrügerische Zugriffe eingesehen werden, wird dies umgehend den betroffenen Personen eröffnet. Für allfälligen diesen daraus erwachsenden Schaden ist die GKK haftpflichtig und dafür versichert.

Datenträgerkontrolle

Die physischen Datenträger unterliegen einer dauernden Kontrolle durch deren Benutzung. Besondere ergänzende Massnahmen zur Kontrolle sind daher nicht notwendig. Die elektronischen Datenträger (GKK-Applikation, Mail-Archiv, Backup) unterliegen durch deren dauernde Benutzung einer latenten Funktions- und Integritätskontrolle.

Transportkontrolle

Die Daten der GKK werden physisch nur innerhalb der Büroräumlichkeiten der GKK transportiert. Die Daten im elektronischen System der GKK werden gemäss den Darlegungen unter Ziffer 7.3.1 und 7.4.2 transportiert und gesichert. Fehler beim Transport dieser Daten werden durch Rückmeldung der Datenadressaten (kann auch die GKK selbst sein), welche auf die Ankunft der Daten warten, aufgedeckt und bereinigt. Jeder Datentransport unterliegt damit einer sofortigen, umfassenden Erfolgskontrolle.

Bekanntgabekontrolle

Fehler bei der Bekanntgabe der Daten der GKK werden durch Rückmeldung der Datenadressaten (kann auch die GKK selbst sein), welche stets auf die Ankunft der Daten warten,

aufgedeckt und bereinigt. Jede Datenbekanntgabe unterliegt damit einer sofortigen, umfassenden Erfolgskontrolle.

Speicherkontrolle

Geschäftliche Daten der GKK, werden zwecks weiterer Bearbeitung oder Archivierung gespeichert.

Die Kontrolle der Speicherung zwecks weiterer Bearbeitung ist eine latente. Fehler bei der Speicherung der zu bearbeitenden Daten der GKK werden immer umgehend aufgedeckt und bereinigt.

Physisch gespeicherte und archivierte Daten der GKK unterliegen neben möglichen Einflüssen von Elementarereignissen keinen Beschädigungsrisiken. Damit erübrigt sich eine Kontrolle.

Elektronisch gespeicherte und archivierte Daten der GKK befinden sich auf dem hauseigenen Server, der Backup-Harddisk, dem Cloud-Backup und den Mail-Ablagen der Mitarbeiter:innen der GKK. Sollten sich Probleme bei der Speicherung derselben ergeben, sind diese stets mit anderen Symptomen in den elektronischen Arbeitsmitteln der GKK verbunden. Solche behindern die tägliche Arbeit, was stets umgehend wahrgenommen und bereinigt wird.

Benutzer- und Zugriffskontrolle

Die Nachvollziehbarkeit der Benutzer von physisch erhobenen, gespeicherten, bearbeiteten, archivierten und weitergereichten Daten der GKK ist mittels Unterzeichnung oder Kürzel der Benutzer gewährleistet. Auf eine physische, latente Kontrolle der Benutzer kann aus dem unter dem Vortitel „Allgemeines und Grundsätzliches zur Kontrolle der Sicherungsmassnahmen“ oben Dargelegten verzichtet werden.

Jede Bearbeitung der elektronisch bearbeiteten und archivierten Daten der GKK wird in der GKK-Applikation, Infoniqa One 50 Finanz und den Mailprogrammen der Benutzer und Mitarbeiter/innen der GKK und auf dem hauseigenen Server protokolliert und kann bei Bedarf nachvollzogen werden.

Sollten sich Probleme im Bestand und den benutzten Daten der GKK in elektronischer Form ergeben, sind diese stets mit anderen Symptomen in den elektronischen Arbeitsmitteln der GKK verbunden. Solche behindern die tägliche Arbeit, was stets umgehend wahrgenommen und bereinigt wird. Sicherheitskopien werden vom Server und von der Cloud-Backup-Lösung automatisch erstellt.

Eingabekontrolle

Erhobene und eingegebene Daten, welche zur Bearbeitung, Speicherung, Archivierung und Weitergabe bei der GKK verwendet werden, unterliegen einer steten, ausnahmslosen und umgehenden Kontrolle durch den:die Sachbearbeiter:in der GKK. Schadhafte oder gefährliche Daten werden nicht in die Datensysteme der GKK integriert.