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 Datensicherheit der Gewerblichen Krankenkasse Bern

Erstellt: 15.11.2012, erstes Dokument
Autor: Leonhard Sitter
Fachgebiet: Organisation, Prozesse und Datensicherheit
Ausgabe: 4 vom 07.05.2019
Klassifikation: öffentlich
Verteiler: Deniz Anselmo, Franziska Grossenbacher, 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

Inhalt

Abbildungsverzeichnis

1 Abkürzungsverzeichnis

ATSG	Allgemeiner Teil des Sozialversicherungsrechts des Bundes
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz
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
VDSG	Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz
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 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 (VDSG) dienen.

2.2 Art des Dokuments

Das Dokument vereint mehrere Funktionen zugleich. Es ist Konzept und Umsetzungsdokumentation 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 von Art. 11 VDSG in Verbindung mit Art. 7 DSG)
- Geschäfts- und Zuständigkeitenordnung der GKK

3 Ausgangslage und Rechtsform

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 für die Branche der Maler- und Gipserunternehmen in der Region Bern.

Auszug aus den Statuten der GKK vom 07. Mai 2019:

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 Arbeitnehmer/innen seiner Mitglieder an diese aus. Die damit verbundenen Risiken sichert die GKK mit finanziellen Reserven in Form von Geldanlagen 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, überdurchschnittlicher Kulanz und Dienstleistungen bei günstigen Prämien. Unsere Kunden spüren die Kompetenz und Zuvorkommenheit unserer Mitarbeiter.

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 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.

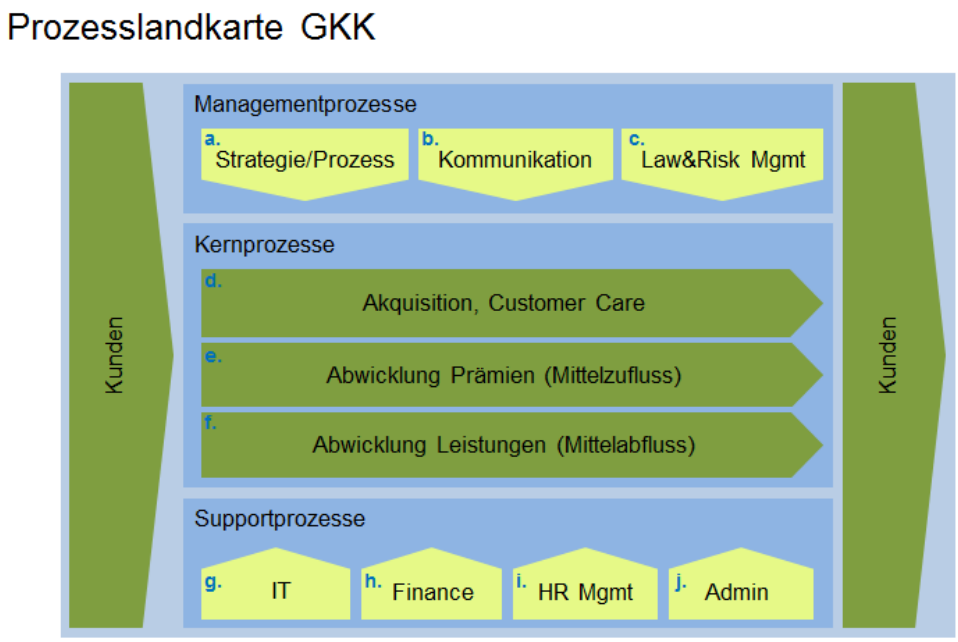

Abbildung 1: Prozesslandkarte GKK

In den Kernprozessen entsteht die Wertschöpfung der GKK und werden geschäftliche Daten erhoben, eingesehen, transportiert, bearbeitet, weitergegeben und vernichtet. Die Führungsprozesse (Managementprozesse) und die Unterstützungsprozesse (Supportprozesse) sind lediglich zur Organisation und Funktionalität der Kernprozesse und der darin verwendeten 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 07.05.2019):

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 persönlichen Daten von Kunden, Mitgliedern oder Versicherten.

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

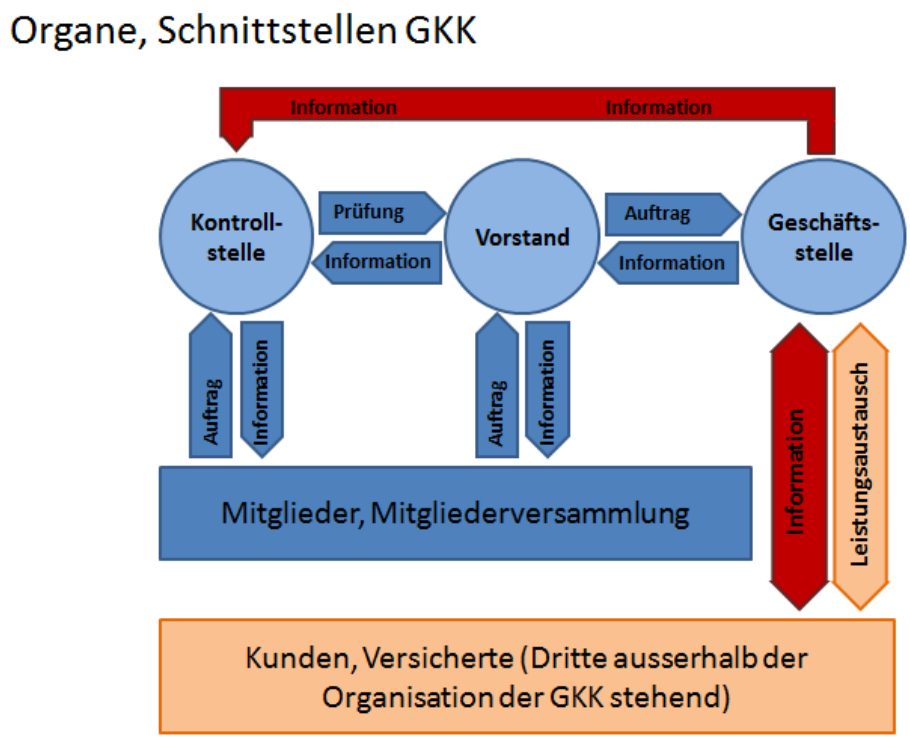

Abbildung 3: Organe, Schnittstellen GKK

In Abbildung 3 sind die oben beschriebenen Organe und zusätzlich die Kunden und die Versicherten als ausserhalb der 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 3 DSG von besonders schützenswerter Natur 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 (im Sinne von Art 4, Abs. 1, Litt. a) VDSG), wie Versicherungsleistungen zum Ausgleich von finanziellen Einbussen durch Erwerbsausfälle aufgrund von Krankheit und Unfall.

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)
- Ärzte und heilbehandelnde Institutionen, die Arbeitsunfähigkeitsausweise erstellen
- 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 (auf eine Wiedergabe wird hier verzichtet). Damit verantwortet diese gegenüber sämtlichen Ansprechgruppen ausserhalb der Unternehmung die unternehmerische Tätigkeit der GKK.

Der Vorstand ist das ausführende 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.

Die Kontrollstelle überprüft zu Handen der Mitgliederversammlung die Geschäftstätigkeit des Vorstandes. Zu ihrer Information greift sie auf die operative Geschäftsführung durch die Geschäftsstelle zurück. Mittels Revisionsbericht, 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.

4.4 Geschäftsstelle

Die Geschäftsstelle als Organ der GKK, welches die operativen Tätigkeiten des Unternehmens ausführt, ist die einzige Stelle innerhalb der GKK, welche schützenswerte Daten im Sinne des DSG erhebt, aufnimmt, bearbeitet, archiviert und vernichtet. Daher sind die Organisation und die Tätigkeiten der Geschäftsstelle hier besonders offenzulegen.

4.4.1 Organisationseinheiten, organisatorische Schnittstellen und Dateneinsicht

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

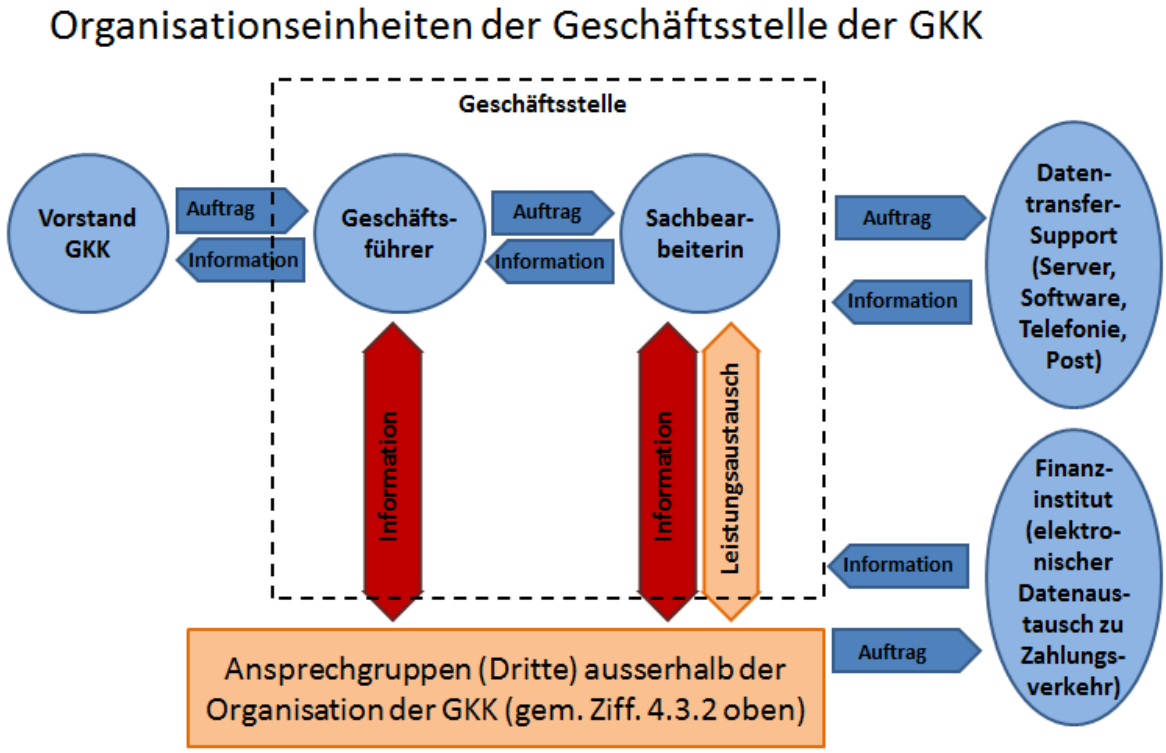

Abbildung 4: Organisationseinheiten, Schnittstellen der Geschäftsstelle GKK

Wie auf Abbildung 4 zu sehen ist, können innerhalb der Unternehmung GKK nur der Geschäftsführer und die Sachbearbeiter/innen die Daten der Kunden und der Versicherten, sowie von deren Ärzten und deren Arbeitslosen-, Unfall- und Krankenpflege- und weiteren Sozalversicherern einsehen. Daten mit besonderem Schutzbedarf werden auch nur zwischen diesen Organisationseinheiten der GKK mit den betreffenden Stellen ausserhalb der Unternehmung ausgetauscht.

4.4.2 Aufgaben, Kompetenzen und Verantwortlichkeiten

Der Geschäftsführer 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 die 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 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
- 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
- Erstellung des Jahresberichts
- 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 Art und Kategorien der erhobenen und verwendeten Daten

5.1 Arten und Kategorien/ Sicherheitsstufen verwendeter Daten

1. Kategorie/ Sicherheitsstufe (geringer Schutzbedarf):
    - Daten wie Anschrift, Firma, Ansprechpersonen der Kunden (der GKK angeschlossene, versicherte Unternehmen)
    - Daten wie Name, Anschrift, Adresse, Geburtsdatum der versicherten Personen
    - Buchungen (ohne Rückschlussmöglichkeit auf Personen)

2. Kategorie/ Sicherheitsstufe (mittlerer Schutzbedarf):
    - Daten über Zahlungsverbindungen, AHV-Bruttolohnsummen, Debitorenrechnungen, Leistungserhalt, Prämienbezahlungen der Kunden (der GKK angeschlossene, versicherte Unternehmen)
    - Daten über Zahlungsverbindungen, Zahlungsanweisungen und Arbeitgeber sowie Bruttogehälter, Arbeitsunfähigkeitsausweise der versicherten Personen

3. Kategorie/ Sicherheitsstufe (hoher Schutzbedarf):
    - Daten über die Gesundheit mit medizinisch, diagnostischem Inhalt über versicherte Personen

4. Kategorie/ Sicherheitsstufe (sehr hoher Schutzbedarf):
    - Keine entsprechenden Daten

5.2 Dokumentation und Art der Ablage der verwendeten Daten

Daten der Kategorie 1

- 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 Anschriften, Namen, Adressen, Ansprechpersonen, Geburtstagen der versicherten Personen und Buchungen in elektronischer Form,
  b) Korrespondenz in elektronischer und physischer Form,
  c) keine Daten in nur physischer Form)

Daten der Kategorie 2

- 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 andern Versicherern, Zahlungsanweisungen und –eingangsbelege, Debitorenrechnungen, Taggeldabrechnungen in elektronischer und physischer Form,
  c) Taggeldausweise, Arbeitsunfähigkeitsausweise, in physischer Form)

Daten der Kategorie 3

- Entsprechende Daten (Daten über die Gesundheit mit medizinisch, diagnostischem Inhalt über versicherte Personen) werden nur physisch (in Papierform) und nur in Ausnahmefällen erhoben und abgelegt und nach Abklärung der Sachverhalte und Tatbestände vernichtet. Solche Daten werden bei der GKK nicht bearbeitet, jedoch archiviert und nur an gesetzlich Berechtigte weitergeleitet.
- Entsprechende Daten werden einzig im Falle unklarer oder unvollständiger Angaben auf den Arbeitsunfähigkeitsausweisen der behandelnden Ärzte oder Heilungsinstituten oder andern 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 Gesundheitserklärung, 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 4 werden bei der GKK weder erhoben, gehalten oder bearbeitet.

6 Dokumentations- und Datenverarbeitungsmittel, Zuständigkeiten

6.1 Struktur Ablage- und Datenverarbeitungsmittel

Bei der GKK werden Daten einerseits in physischer Form (Papier) und andererseits in elektronischer Form abgelegt, gespeichert und archiviert.

Be- und verarbeitet werden erhobene und geschaffene Daten ausschliesslich in elektronischer Form.

6.2 Physische Ablage- und Datenverarbeitungsmittel

Wie in Kapitel 5.2 oben dargelegt, werden folgende Daten bei der GKK in physischer Form erhoben, geschaffen, abgelegt, gespeichert (nicht bearbeitet) und archiviert:

Daten der Kategorie/ Sicherheitsstufe 1

- 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

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 Anlagendepots unterhält mit geringfügig schützenswertem Inhalt
- Schriftliche Korrespondenz zwischen den Organen der GKK (insbesondere Geschäftsstelle – Kontrollstelle) mit geringfügig schützenswertem Inhalt
- Jahresabschlüsse und Jahresberichte

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, 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 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/ 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, 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, 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 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 bei der GKK per E-Mail, Telefon oder einfachem Brief durch den/die zuständige/n Sachbearbeiter/in der Geschäftsstelle angefordert/ erhoben. 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 abgelegt. Nach der definitiven Klärung der Sachverhalte, werden Daten der Kategorie/ Sicherheitsstufe 3 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.

6.3 Elektronische Ablage- und Datenverarbeitungsmittel, IT-gestützte Prozesse

Wie in Kapitel 5.2 oben dargelegt, werden folgende Daten bei der GKK in elektronischer Form erhoben, geschaffen, abgelegt, gespeichert, bearbeitet und archiviert:

Daten der Kategorie/ Sicherheitsstufe 1

- Schriftliche Korrespondenz mit Kunden mit geringfügig schützenswertem Inhalt per E-Mail und in der elektronischen Datenablage in Microsoft Outlook-Express 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-Express 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-Express 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-Express 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-Express 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-Express 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-Express 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-Express und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/in der Geschäftsstelle der GKK
- Jahresabschlüsse und Jahresberichte per E-Mail und in der elektronischen Datenablage in Microsoft Outlook-Express und/oder als elektronisches Dokument auf dem persönlichen Laufwerk des/der zuständigen Sachbearbeiters/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“ geschaffen, bearbeitet, gespeichert, eventuell weitergereicht und archiviert. Nach Eingang /Erschaffung der erhobenen Daten/Dokumente, werden diese auf dem hauseigenen Server, auf dem persönlichen Laufwerk und dem PC des/der zuständigen Sachbearbeiters/in in den Büroräumlichkeiten der Geschäftsstelle aufbewahrt und archiviert. Ein Zugriff über das Internet von aussen oder von ausserhalb der Geschäftsstelle mittels virtuellem Arbeitsplatz oder ähnlichem ist nicht existent. Zugriff hat auch der Geschäftsführer.

Zuständigkeit für die Erhebung, Aufnahme, Bearbeitung, 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 per E-Mail und in der elektronischen Datenablage in Microsoft Outlook-Express 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-Express 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-Express 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-Express 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 Sage Sesam 50, 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“ geschaffen, bearbeitet, gespeichert, eventuell weitergereicht und archiviert. Nach Eingang /Erschaffung 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 aufbewahrt und archiviert. Ein Zugriff über das Internet von aussen oder von ausserhalb der Geschäftsstelle mittels virtuellem Arbeitsplatz oder ähnlichem ist nicht existent. Zugriff hat noch der Geschäftsführer der GKK.

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

Daten der Kategorie/ Sicherheitsstufe 3

Daten der Kategorie/ Sicherheitsstufe 3 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 3 werden bei der GKK auch in elektronischer Form aufgenommen, gespeichert, weitergereicht oder archiviert, nicht jedoch bearbeitet.

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

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 Sage Sesam 50 die Prozesse unterstützen:

Abbildung 5: Hauptprozesse und IT-Unterstützung

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

6.3.1 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.

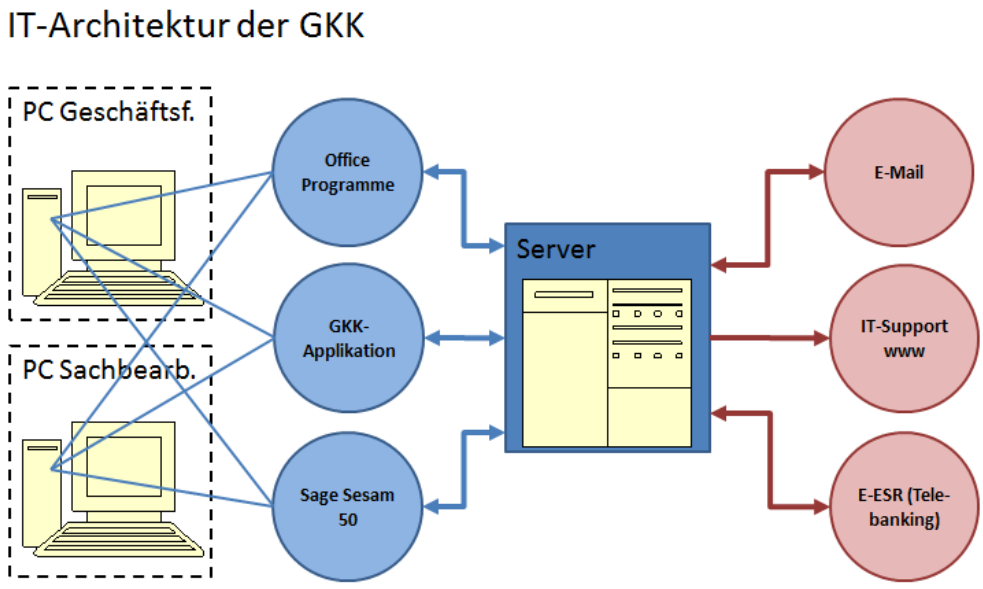

Abbildung 6: IT-Architektur GKK

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).

6.3.2 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 ausserhalb stehenden 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 2010.

6.3.3 Software

An den Arbeitsplätzen des/der zuständigen Sachbearbeiter/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 im Sinne eines customer relationship managements sind in der GKK-Applikation nicht enthalten)
- Sage-Sesam 50 (Software für das Rechnungswesen der GKK ohne Personendaten)
- Microsoft Office-Programme: Word und Excel. (Hier werden Daten der einfachen Korrespondenz, wie auch Daten über medizinisch diagnostische oder rechtliche Sachverhalte im Zusammenhang mit Kunden oder versicherten Personen, wie auch Daten über das Kundenverhalten im Sinne eines customer relationship managements bearbeitet.)

6.3.4 Die GKK-Applikation

Das Herzstück des Tagesgeschäftes ist wie oben aufgeführt die hauseigene GKK-Applikation. Diese ist ein Microsoft Access – 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:

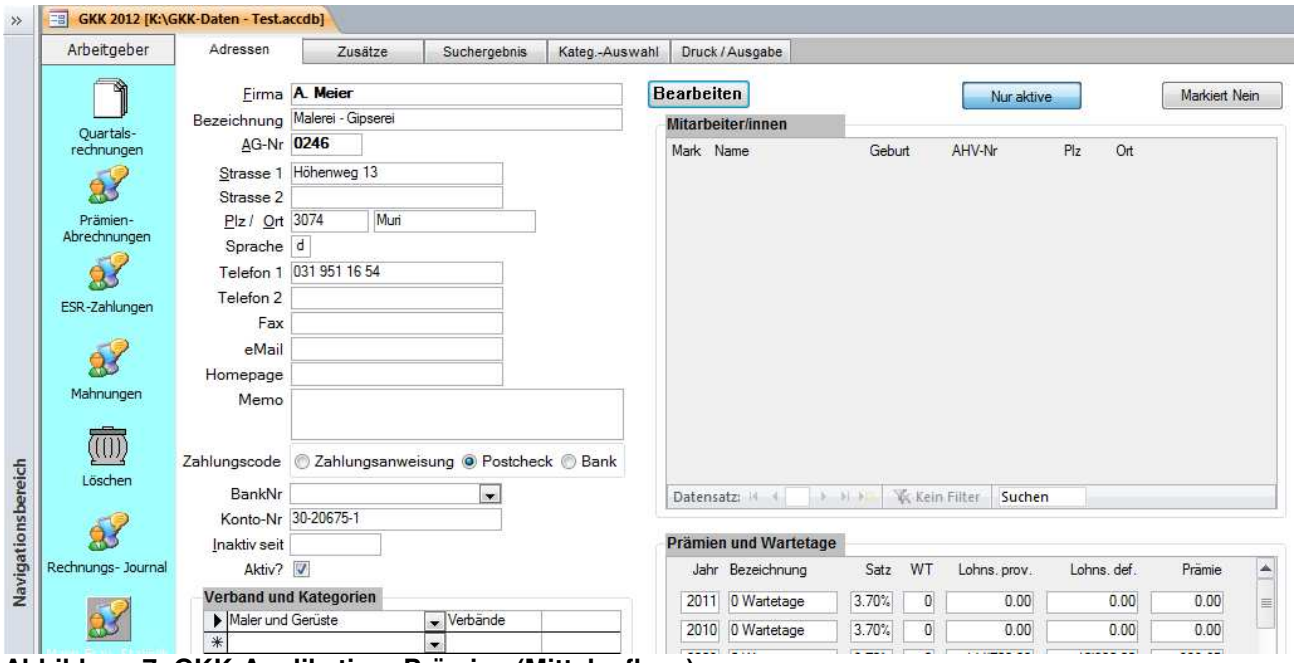

Abbildung 7: GKK-Applikation: Prämien (Mittelzufluss)

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).

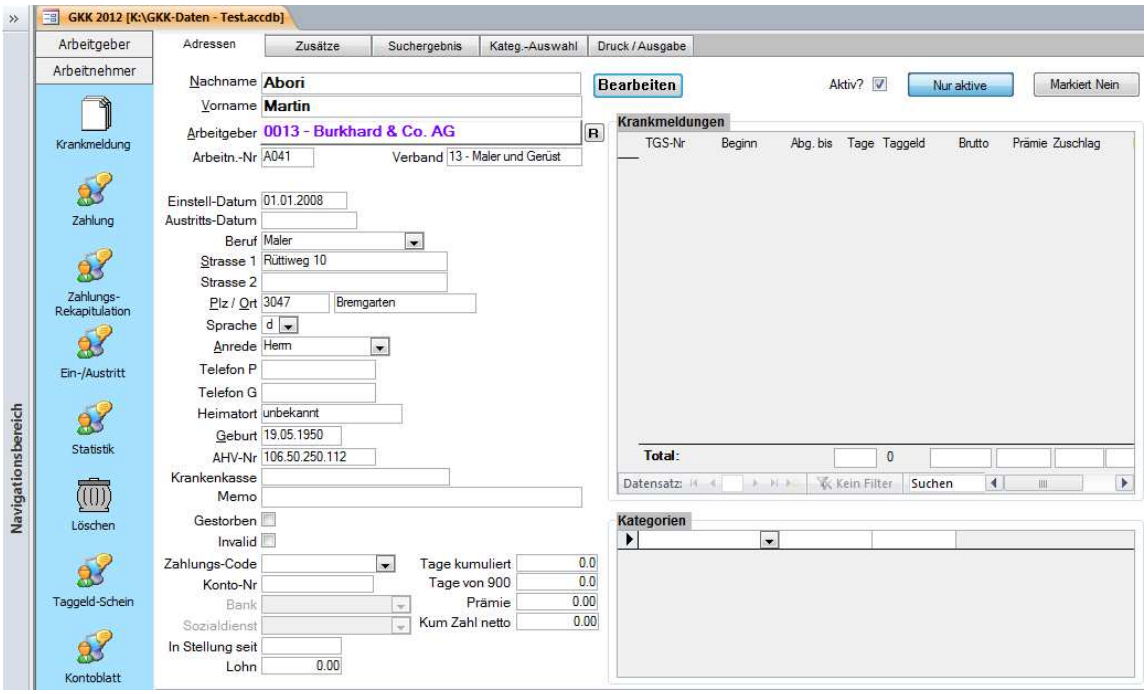

Abbildung 8: GKK-Applikation: Leistungen (Mittelabfluss)

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).

6.4 Sicherung der Dokumentations- und Datenverarbeitungsmittel

Schutzbedarf (s. Kapitel 5 und 6 oben):

Der Grossteil der erhobenen, geschaffenen, bearbeiteten, gespeicherten, weitergereichten, archivierten Daten unterliegt einem geringen Schutzbedarf (Kategorie/ Sicherheitsstufe 1).

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

Ein marginaler Teil der erhobenen, gespeicherten, weitergereichten Daten unterliegt einem hohen Schutzbedarf (Kategorie/ Sicherheitsstufe 3).

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

6.4.1 Organisatorische Sicherung

Zugang, Bearbeitung, Speicherung, Verwahrung

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 12:00 und 13:30 bis 17:00) nicht verriegelt. Ansonsten ist sie mit einem code- und schlüsselgesicherten Schliesszylinder verschlossen. Der zugangsberechtigte Personenkreis ist auf 15 Personen eingeschränkt.

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 Mitarbeiter von KMU Stadt Bern) geöffnet. Neben diesen Personen besitzt auch der Geschäftsführer einen Schlüssel.

Während den Büroblockzeiten sind sämtliche Datenablagen dauernd durch Mitarbeiter von KMU Stadt Bern und der Gewerbe Treuhand 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 Ordner, hinter dem Arbeitsplatz des/der zuständigen Sachbearbeiter/in in einem Regal.
- Die Ordner mit Dokumenten abgeschlossener Jahre befinden sich in einem abgeschlossenen, tagsüber durch andere Mitarbeiter/innen kontrollierbaren Schrank im Hausflur.

Die Gefahr, dass unberechtigte Dritte, selbst mit entsprechender Absicht, an mittlere oder erhöht schutzbedürftige Daten kommen, ist marginal.

In den oben beschriebenen Räumlichkeiten sind die Datenablagen gespeichert/ abgelegt/ archiviert/ verwahrt. Weitere Verwahrungsorte existieren nicht.

Weitergabe von Daten

Daten, welche die GKK erhebt, schafft, bearbeitet, speichert, weiterreicht, 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 und den Geschäftsführer 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 KMU Stadt Bern, Comtool GmbH, Herr R. Flückiger (Hardware- und Betriebssystemlieferant von KMU Stadt Bern und der GKK), Geschäftsführer KMU Stadt Bern und GKK.

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

6.4.2 Technische Sicherung

Unter Ziffer 6.3 ist detailliert beschrieben, welche Daten in elektronischer Form erhoben, geschaffen, bearbeitet, gespeichert, weitergereicht, 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:

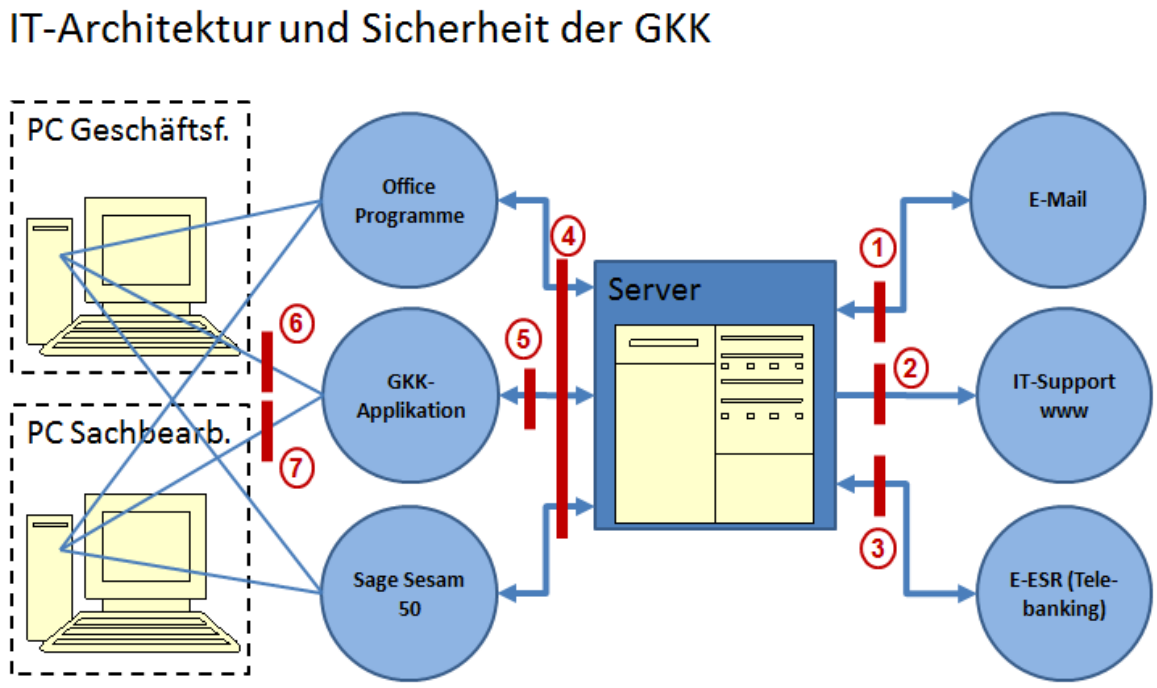

Abbildung 9: IT_Architektur und Sicherheit GKK

Sicherheits-Gates:

1 Elektronische Korrespondenz (möglich mit Anhängen ohne Grössenbeschränkung) gelangt von aussen zum Server der GKK über ein integriertes System von Firewalls und Antivirussoftware. In den letzten fünf 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 elektronischer Kommunikationssysteme 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 Sage Sesam 50, 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 Postfinance. Taggeldleistungen werden per E-Zahlungsauftrag an die Postfinance übertragen und überwiesen, Zahlungseingänge per Datenfile von der Postfinance 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 mittels 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). Die Anforderungen an die Passwörter der GKK-Datenbearbeitenden sind hoch. Ein Passwort muss aus mindestens acht Zeichen bestehen, mindestens einen Grossbuchstaben, mindestens eine Ziffer und mindestens ein Sonderzeichen aufweisen.

Erhebung

Wie unter Ziffer 6.3 oben beschrieben, werden Daten der GKK (bis auf die Daten des elektronischen Datentransfers mit Postfinance - s. Sicherheitsgate 3) nur per Telefon, E-Mail und Brief erhoben. Der Verzicht auf eine IT-integrierte, automatische Datenerhebung reduziert das Sicherheitsrisiko erheblich und erfordert, bis auf den Schutz des E-Mailkanals, keine technische Datenerhebungs-Sicherheitsmassnahme.

Zugang, Bearbeitung

(s. dazu „Sicherheits-Gates“ oben)

Speicherung, Verwahrung

(s. dazu „Sicherheits-Gates“ oben, zum Server und Backup s. Ziffer 6.3.2 oben).

Weitergabe von Daten

Wie die Datenerhebung, ist auch die Weitergabe von Daten auf die Übermittlung per Telefon, E-Mail und Brief beschränkt (Ausnahme auch hier: elektronischer Datentransfer mit Postfinance in einem absolut gesicherten Datenkanal - s. Sicherheitsgate 3). Der Verzicht auf eine IT-integrierte, automatische Datenweitergabe reduziert das Sicherheitsrisiko erheblich und erfordert, bis auf den Schutz des E-Mailkanals, keine technische Datenweitergabe-Sicherheitsmassnahme.

Datenvernichtung

Daten der Kategorie/ Sicherheitsstufe 1 und 2 werden elektronisch auf den persönlichen E-Mail-Accounts der GKK-Mitarbeiter/innen und auf dem Server gespeichert und nicht vernichtet. Daten der Kategorie/ Sicherheitsstufe 3 werden nicht elektronisch bearbeitet, gespeichert, archiviert.

6.4.3 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 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), ist auf der Geschäftsstelle der/die Sachbearbeiter/in alleine zuständig. Bei ausserordentlichen Fragestellungen zieht sie den Geschäftsführer 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 erhobenen, gespeicherten, bearbeiteten, archivierten, weitergereichten und vernichteten Daten, werden innerhalb Monatsfrist wahrgenommen und sind einfach zu identifizieren. Zu deren Behebung bedarf es nur in ausserordentlichen Sonderfällen einschneidender Massnahmen und Eingriffen.

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. Auf elektronischem Weg vorgefallene Datenzugriffe durch unberechtigte Dritte auf die Daten der Kategorien/ Sicherheitsstufen 1 und 2, sind bei Bedarf durch die Server-Zugriffsprotokolle kontrollierbar. Werden keine Veränderungen an den erhobenen, gespeicherten, bearbeiteten, archivierten, und vernichteten 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.

Datenträgerkontrolle

Die physischen Datenträger unterliegen einer dauernden Kontrolle durch deren Benutzung. Besondere 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.

Tranpsotkontrolle

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 6.3.1 und 6.4.2 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 und den Mail-Ablagen der Mitarbeiter/innen der GKK. Sollten sich Probleme bei der Speicherung derselben ergeben, sind diese stets mit andern Symptomen in den elektronischen Arbeitsmitteln von KMU Stadt Bern 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 Sicherungsmass-nahmen“ oben Dargelegten verzichtet werden.

Jede Bearbeitung der elektronisch erhobenen, gespeicherten, bearbeiteten, archivierten und weitergereichten Daten der GKK wird in der GKK-Applikation, Sage Sesam 50 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 andern Symptomen in den elektronischen Arbeitsmitteln von KMU Stadt Bern verbunden. Solche behindern die tägliche Arbeit, was stets umgehend wahrgenommen und bereinigt wird. Sicherheitskopien werden vom Server 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.