Informationssicherheitspolitik der EGK-Gesundheitskasse

EGK-Gesundheitskasse
Brislachstrasse 2, 4242 Laufen
T 061 765 51 11
info@egk.ch, www.egk.ch

Verteiler: - Geschäftsleitung der EGK-Gesundheitskasse
- alle Mitarbeitenden der EGK-Gesundheitskasse (Intranet)

Veröffentlichung: http://www.egk.ch/egk/

Wichtige Informationen zum Dokument	
Verantwortlicher Autor:	Kilian Schmidlin
Dateiname:	Informationssicherheitspolitik der EGK-Gesundheitskasse
Versionsnummer:	1.4
Dokumentnummer:	1.3.02-d
Seitenzahl:	7
Vertraulichkeitsstufe:	V1 - öffentlich
Erstellung begonnen am:	25. September 2014
Freigabe am:	20. Oktober 2014
Letzte Bearbeitung am:	24. Oktober 2019
Bearbeitungsstatus:	Freigegeben
Letzte Freigabe am:	28. Oktober 2019
Freigegeben durch:	Geschäftsleitung

Ergänzende Dokumente/Mitgeltende Unterlagen			
Titel des Dokuments	*Version*	*Datum*	*Verantwortlicher Autor*
Bearbeitungsreglement für die Datensammlung	3.1	28.10.2019	Kilian Schmidlin
Datenschutzerklärung für die Online-Dienste	1.0	01.06.2019	Stefanie Omlin
Reglement zu Informatikmitteln	2.0	19.08.2019	Andrea Grolimund
BCM-Konzept	2.6	20.08.2018	Patrick Tanner Alice Grolimund Kilian Schmidlin
Datensicherungskonzept	1.4	25.10.2019	Patrick Tanner
Richtlinie zur Klassifizierung von Daten / Informationen / Dokumenten	1.1	28.10.2019	Kilian Schmidlin

EGK-Gesundheitskasse
Brislachstrasse 2, 4242 Laufen
T 061 765 51 11
info@egk.ch, www.egk.ch

I. Inhaltsverzeichnis

II. Abkürzungsverzeichnis

BCM	Business Continuity Management (deutsch: Betriebliches Kontinuitätsmanagement)
CENT	Cent Systems AG
DAS	Datenannahme-Stelle
DRG	Diagnosis Related Groups (deutsch: diagnosebezogene Fallgruppen für stationäre Spitalrechnungen)
DSG	Datenschutz-Gesetz
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
FINMA	Eidgenössische Finanzmarktaufsicht
ICT	Information and communications technology (deutsch: Informations- und Kommunikations-Technologie)
KVG	Krankenversicherungs-Gesetz
MCD	Minimal clinical dataset (deutsch: Medizinischer Datensatz)
OCR	Optical character recognition (deutsch: optische Zeichenerkennung)
SHP	Swiss Health Platform (Kernapplikation der EGK/Centris AG)
SPS	Swiss Post Solutions, Tochtergesellschaft der Swiss Post
TARPSY	Tarif für stationäre Psychiatrie (diagnosebezogene Tagesfallgruppe)
VVG	Versicherungsvertrags-Gesetz

1 Geltungsbereich

Die Firmenbezeichnung EGK-Gesundheitskasse, nachfolgend EGK genannt, umfasst die Stiftung EGK-Gesundheitskasse mit den ihr angegliederten Aktiengesellschaften: EGK Grundversicherungen AG (Versicherungsträger der obligatorischen Krankenpflegeversicherung nach KVG), EGK Privatversicherungen AG (Versicherungsträger der Zusatzversicherungen nach VVG) sowie EGK Services AG. Die Informationssicherheitspolitik der EGK gilt für alle Firmen der EGK-Gruppe.

2 Zweck

Entsprechend dem Leitbild der EGK-Gesundheitskasse schützen und respektieren wir die Privatsphäre unserer Kunden. Dies bedeutet, dass wir sorgfältig mit den uns zur Verfügung gestellten und von uns bearbeiteten Daten umgehen. So ist es auch im Verhaltenskodex und in mehreren Reglementen festgehalten. Diese Grundsätze geben den Rahmen für die Informationssicherheitspolitik der EGK vor.

Informationen und Daten, insbesondere Personen- und Gesundheitsdaten der Versicherten, sind für die Erfüllung unseres gesetzlichen Auftrags gemäss KVG in der Obligatorischen Krankenpflegeversicherung (Grundversicherung) sowie für die vertragskonforme Abwicklung der Zusatzversicherungen nach VVG von zentraler Bedeutung. Unsere Datenschutz- und Sicherheitsmassnahmen dienen dazu, schädigende Ereignisse möglichst zu verhindern, respektive deren Häufigkeit und Auswirkungen zu reduzieren sowie in einem tragbaren und verhältnismässigen Rahmen zu halten.

3 Sicherheitsziele der EGK

- Aufrechterhaltung der zentralen Geschäftsprozesse.

- Hohes Sicherheitsniveau, Stabilität, Kontinuität und Qualität bei der Bearbeitung von Daten und Informationen sowie der Erbringung von Dienstleistungen unter Berücksichtigung der gesetzlichen Vorgaben, des Prinzips der Verhältnismässigkeit und vertretbaren ökonomischen Aspekten.
- Verhinderung von Reputations- oder finanziellen Schäden für die EGK durch Verlust von Daten oder Informationen, beziehungsweise durch Kenntnisnahme von Daten und Informationen durch unberechtigte Dritte.
- Hohes Sicherheits- und Datenschutzbewusstsein der Mitarbeitenden auf allen Stufen und in allen Geschäftsbereichen.

4 IT Sourcing Strategie

Die EGK setzt mittels zielgerichteter Auslagerung und Delegation von Engineering- und Betriebs-Leistungen auf eine Teil-Outsourcing Strategie von IT-Dienstleistungen. Dabei ist die Versicherungskernapplikation an die Centris AG in Solothurn ausgelagert. Diese ist ein professioneller, zertifizierter Branchendienstleister, der für mehrere Krankenversicherer die „Swiss Health Platform“ SHP betreibt. Die Centris AG nimmt auch im elektronischen Prozess bei Rechnungen vom Typus DRG / TARPSY die Funktion als zertifizierte Datenannahmestelle (DAS) der EGK wahr. Sie ist dafür beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) als solche registriert und anerkannt. Zur SHP-Umgebung gehören insbesondere die Systeme Syrius ASE, CBPM, SUMEX II, DWH, OA, das Archivsystem FileNet, Massenprinting und die Digital Insurance Platform (DIP).

Weiter bezieht die EGK IT-Dienstleistungen hinsichtlich RZ Infrastruktur und RZ Basisbetrieb als Managed Service von der Econis AG. Als Managed Service ist der Betrieb der Hardware im Bereich Server Storage und Remote Access zu verstehen.

Die EGK ICT hält die Hoheit ab der Ebene der Betriebssysteme der im Einsatz stehenden Datenbankinfrastruktur (Server HW und OS) für die EGK Umsysteme.

Die Netzwerkinfrastruktur sowie die Telefonie Dienstleistungen werden von der Swisscom bezogen.

Weitere wichtige Outsourcing-Partner der EGK bei der Datenbearbeitung sind die Swiss Post Solutions (SPS) als Scanning Dienstleister sowie die Cent Systems AG (Cent) für die Capturingservices.

5 Grundsätze

5.1 Vorschriften, Gesetzte und Verträge

- Bei der Bearbeitung von Daten und Informationen sind die gesetzlichen, vertraglichen und internen Bestimmungen jederzeit einzuhalten.
- Bei sensiblen Daten und Informationen von Versicherten sind insbesondere die spezialrechtlichen Grundsätze des Bundesgesetzes über den Datenschutz (DSG) sowie des Bundesgesetzes über die Krankenversicherung (KVG) zu beachten.
- Es ist ein Datenbearbeitungsreglement gemäss Art. 84b KVG zu erstellen, das öffentlich zugänglich ist.
- Die Kontinuität der Geschäftstätigkeit ist auch bei aussergewöhnlichen Ereignissen und Situationen sicherzustellen und die von der FINMA anerkannten Mindeststandards für Versicherungsunternehmen sind einzuhalten (BCM).
- Die Aufbewahrung von Daten, Informationen und Unterlagen richtet sich nach den gesetzlichen Vorgaben; im Zweifelsfalle gilt eine Aufbewahrungsfrist von mindestens 10 Jahren

5.2 IT-Schutzziele

- Es ist sicherzustellen, dass die Verfügbarkeit, die Integrität und die vertrauliche Behandlung von Daten und Informationen der EGK, von ihren Versicherten, Mitarbeitenden und Partnern jederzeit gewährleistet sind. Dazu gelten folgende Grundsätze:

5.2.1 Vertraulichkeit

- Werden Daten und Informationen an Dritte weitergegeben, so ist vertraglich zu vereinbaren, wie diese Informationen verwendet, bearbeitet und genutzt werden dürfen. Die Datenweitergabe erfolgt anonymisiert oder über verschlüsselte Datenträger und Kanäle.

- Im individuellen E-Mailverkehr muss bei der Übermittlung von personenbezogenen Daten das Verschlüsselungsverfahren angewandt werden. Das Mail-System der EGK bietet diese Möglichkeit an.

- Die Mitarbeitenden werden in Bezug auf Datenschutz und Informationssicherheit aus- und weitergebildet. Es wird sichergestellt, dass sie die für ihren Bereich geltenden Bearbeitungsreglemente kennen und anwenden.

- Daten und Informationen sind durch Klassifizierungen zu schützen. Die Klassifizierungsstufen sind unabhängig von der Applikation, auf welcher die Daten und Informationen zur Verfügung gestellt werden.

5.2.2 Verfügbarkeit

- Es ist ein Datensicherungskonzept zu erstellen, welches die Rahmenbedingungen für organisatorische und technische Massnahmen zur Datensicherheit festhält.

- Applikationsänderungen haben nach einem definierten Change-Management-Prozess zu erfolgen.

- Personenbezogenen Datensammlungen sind in einem Daten-Verarbeitungsverzeichnis zu führen aus welchem hervorgeht, wo die Daten gespeichert und wie die Löschfristen definiert sind.

5.2.3 Integrität

- Zum Schutz von Informationen müssen kryptographische Schlüssel mit einem absehbaren Enddatum von max. 3 Jahren versehen werden.

- Durch ein rollenbasiertes Berechtigungskonzept muss sichergestellt sein, dass die Mitarbeitenden nur auf jene Daten und Informationen Zugriff haben, die sie im Rahmen ihrer Tätigkeit benötigen.

- Mit Schutzmechanismen muss sichergestellt werden, dass ausschliesslich berechtigte Mitarbeitende ausführende Dateien selber installieren können.

6 Verantwortung

Die Verantwortung für die Daten- und Informations-Sicherheit sowie die Datenverfügbarkeit und -Integrität liegt beim Leiter ICT der EGK.

Die Bereichsleitenden sowie die Führungskräfte in den einzelnen Bereichen sind für die Umsetzung innerhalb ihres Zuständigkeitsbereichs verantwortlich.

Die Mitarbeitenden sind aufgefordert, entdeckte oder vermutete Datenschutz- oder Sicherheitsprobleme der Bereichsleitung oder dem Betrieblichen Datenschutzverantwortlichen zu melden.

7 Prozesse für den Umgang mit Abweichungen und Ausnahmen.

Ausnahmen und Abweichungen, welche im Widerspruch zur Informationssicherheitspolitik stehen sind mittels Antrag zur Prüfung und Genehmigung an die Geschäftsleitung zu stellen.

8 Inkrafttreten / Überprüfung

Dieses Dokument zur Informationssicherheitspolitik tritt am 20.10.2014 in Kraft. Es wird mindestens einmal jährlich auf seine Aktualität und notwendige Anpassungen überprüft. Änderungen treten mit deren Freigabe durch die Geschäftsleitung in Kraft.

9 Änderungsnachweis

Änderungsnachweis				
Versions-nummer	*Bearbeitungs-status*	*Datum*	*Bearbeiter*	*Änderung / Bemerkung*
0.1	Initialfassung	25.09.2014	K. Schmidlin	
1.0	Freigegeben	20.10.2014	K. Schmidlin	
1.1	Freigegeben	03.10.2016	K. Schmidlin	- Anpassungen an neue Systemumgebung SHP
1.2	Freigegeben	25.09.2017	K. Schmidlin	- Integration BCM - div. kleine Anpassungen.
1.3	Freigegeben	01.10.2018	P. Tanner	- Anpassungen bei Kapitel 4 - Neue Kapitel 5.1 und 5.2 und 7 - kleine red. Anpassungen
1.4	Freigegeben	28.10.2019	K. Schmidlin	- kleine red. Anpassungen und Aktualisierungen