Reglement der Datenbearbeitungen der EGK-Gesundheitskasse

Die EGK-Gesundheitskasse 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.

EGK-Gesundheitskasse
Birspark 1, 4242 Laufen
T 061 765 51 11
info@egk.ch, www.egk.ch

Inhaltsverzeichnis

Abkürzungsverzeichnis

Begriff	Beschreibung
ATSG	Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (SR 830.1)
BAG	Bundesamt für Gesundheit
Cent	Cent Systems AG
Centris	Centris AG
DAS	Datenannahmestelle
DRG	Diagnosis Related Groups (diagnosebezogene Fallgruppen)
DSG	Bundesgesetz vom 01. September 2023 über den Datenschutz (SR 235.1)
DSV	Verordnung vom 01.September 2023 über den Datenschutz (SR 235.11)
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
FINMA	Eidgenössischen Finanzmarktaufsicht
IaaS	Infrastructure as a Service
KVG	Bundesgesetz vom 18. März 1994 über die Krankenversicherung (SR 832.10)
KVAG	Bundesgesetz vom 26. September 2014 betreffend die Aufsicht über die soziale Kranken-versicherung (SR 832.12)
MCD	Minimal Clinical Dataset
SaaS	Software as a Service
SFTP	Secure File Transfer Protocol
SHP	Swiss Health Plattform
SPS	Swiss Post Solutions AG
VAD	Vertrauensärztlicher Dienst
VVG	Bundesgesetz vom 2. April 1908 über den Versicherungsvertrag (SR 221.229.1)

1 Allgemeines

1.1 Geltungsbereich

Das vorliegende Reglement der Datenbearbeitungen (nachfolgend Reglement) der EGK-Gesundheitskasse (nachfolgend EGK) gilt für alle der EGK-Gruppe angegliederten Rechtsträger. Einerseits bearbeitet die EGK Grundversicherungen AG Personendaten im Bereich der sozialen Krankenversicherung (obligatorische Krankenpflegeversicherung und der freiwilligen Taggeldversicherung) und andererseits die EGK Privatversicherungen AG im Bereich der privaten Krankenzusatzversicherung. Die EGK Services AG ihrerseits erbringt für alle Rechtsträger der EGK-Gruppe Administrations- und Service-Dienstleistungen.

In diesem Dokument wird auf eine geschlechtsneutrale Formulierung geachtet. Wo dies nicht möglich ist, wird zur besseren Lesbarkeit nur ein Geschlecht verwendet. Die entsprechenden Bezeichnungen gelten für alle Personen.

1.2 Rechtliche Grundlage

Die EGK bearbeitet die Personendaten gemäss den Bestimmungen des DSG. In ihrer Funktion als Bundesorgan und zugelassene Krankenversicherung nach KVAG ist sie per Gesetz legitimiert Personendaten im Bereich des KVG zu bearbeiten. Als Anbieterin von Krankenzusatzversicherungen gemäss VVG bearbeitet sie ebenfalls Personendaten als private juristische Person auf Basis der mit den Kunden abgeschlossenen Versicherungsverträge.

Gestützt auf Art. 6 DSV in Verbindung mit Art. 84b KVG hat die EGK für automatisierte Bearbeitungen von Daten, die besonders schützenswerte Daten oder ein Profiling beinhalten, das vorliegende Reglement erstellt. Die Bearbeitung der Daten erfolgt von der EGK zur Erfüllung ihrer Aufgaben als soziale und private Krankenversicherung. Im Sinne von Art. 12 Abs. 1 und 4 DSG i.V.m. Art. 56 DSG ist die EGK als Bundesorgan verpflichtet dem EDÖB die Bearbeitung von Personendaten zu melden, dieser veröffentlicht die Meldung in einem öffentlich zugänglichen Register (https://datareg.edoeb.admin.ch/search).

1.3 Ziel des Reglements

Das Reglement umschreibt die Datenbearbeitungs- und Kontrollverfahren und den Betrieb der elektronischen Datenbearbeitung der EGK. Es enthält Angaben über die für den Datenschutz und die Datensicherheit verantwortlichen Bereiche und Personen, die Herkunft der Daten, die Zwecke und beschreibt das Verfahren für die Erteilung der Zugriffsberechtigungen auf die einzelnen Module der elektronischen Informationssysteme.

1.4 Verantwortliche Stelle

Die Geschäftsleitung der EGK ist verantwortlich für die Entscheidungen im Sinne des Zweckes und der Mittel der Datenbearbeitung.

1.5 Outsourcing

Die Bearbeitung von Personendaten kann durch Gesetz oder Vereinbarung an Dritte übertragen werden (Outsourcing). Die wesentlichen Outsourcing-Dienstleistungen sind Teil der bewilligungspflichtigen Eingaben zum Geschäftsplan an die Aufsichtsbehörden (BAG für die soziale Krankenversicherung nach KVG und FINMA für die Krankenzusatzversicherungen nach VVG).

Die Dienstleister sind verpflichtet, die ihnen zur Verfügung gestellten Daten ausschliesslich im vertraglich definierten Rahmen zu bearbeiten, so wie sie die EGK gemäss den jeweils anwendbaren rechtlichen Normen auch bearbeiten dürfte und sofern keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

1.6 Schweigepflicht nach Art. 33 ATSG

Sämtliche Mitarbeitende der EGK unterstehen der Schweigepflicht nach Art. 33 ATSG. Zusätzlich unterzeichnen sie zusammen mit dem Arbeitsvertrag eine Geheimhaltungs- und Schweigepflichtserklärung. Ebenso gelten die Bestimmungen zur Schweigepflicht und Geheimhaltung des Verhaltenskodex der EGK.

1.7 Zertifizierte Datenannahmestelle

Die gesetzlich erforderliche DAS der EGK wird durch die Firma Centris in Solothurn betrieben, welche diese Dienstleistung für verschiedene Krankenversicherer anbietet. Der Zertifizierungsbereich der DAS (Scope) erstreckt sich nicht nur über die Centris und deren DAS, sondern es werden auch Teilbereiche der EGK, die SPS und die Cent miteinbezogen (siehe auch Kapitel 2 IT Betriebsmodell und Schnittstellen).

2 IT Betriebsmodell und Schnittstellen

2.1 Betriebsmodell

Für die Durchführung ihrer Tätigkeiten im Rahmen der sozialen Krankenversicherung sowie der privaten Krankenzusatzversicherung bezieht die EGK neben eignen IT Business Services auch Business Services von ausgewählten IT-Dienstleistern in Form von IaaS und SaaS. Das Krankenversicherungskernsystem besteht aus der SHP von Centris.

2.2 Schnittstellen

Die EGK empfängt von ihren Kunden und Dienstleistern Daten. Elektronische Rechnungen werden im entsprechenden Format von den Leistungserbringern direkt an die Centris respektive, an die von ihr betriebene DAS übermittelt. Rechnungsbelege in Papierform werden von der SPS eingescannt und für die Rechnungserfassung (Capturing) an die Cent übermittelt, welche anschliessend die Daten im entsprechenden Format für die Weiterverarbeitung bei Centris bereitstellt. Korrespondenzschreiben und Formulare werden nach dem Scanning bei SPS ins Krankenversicherungskernsystem SHP der Centris importiert.

Die EGK und ihre Dienstleister wenden beim Datenaustausch zeitgemässe symmetrische und asymmetrische Verschlüsselungsverfahren an. Sichere Schnittstellen ermöglichen den Kontakt und elektronischen Austausch von Daten mit Kunden, Leistungserbringern, Behörden und Dienstleistern.

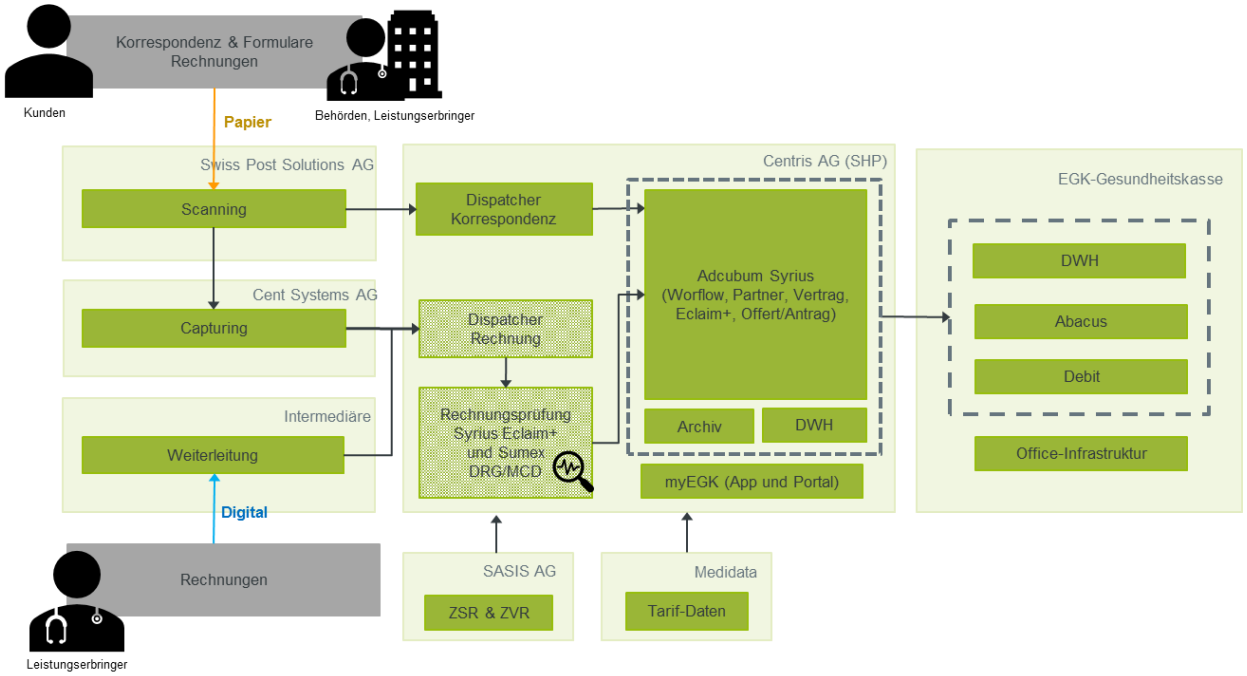

Abbildung 1 Grobübersicht Schnittstellen

Von	Nach	Zweck beim Empfänger	Daten
Versicherte Leistungserbringer Behörden	SPS	Digitalisieren von Papierdokumenten (Korrespondenz/Formulare, Rechnungen) und Zuweisen des Dokumenttyps	Dokumente in Papierform (Belege, Formulare)
SPS	CENT	Datenweiterleitung der Belege zur Erkennung und Erfassung (Capturing) des Dokumenteninhalts	TIFF mit Metainformationen
SPS	Centris	Datenweiterleitung der Korrespondenz/Formulare für die Verarbeitung über das Workflowsystem	PDF mit Metainformationen
CENT	Centris	Datenweiterleitung zur Rechnungsprüfung	Elektronische Rechnungen nach Standard Forum Datenaustausch (XML 4.x)
Intermediäre	Centris	Datenweiterleitung zur Rechnungsprüfung	Elektronische Rechnungen nach Standard Forum Datenaustausch (XML 4.x)
Centris	EGK	DWH: Reports und Datenanalysen für interne geschäftliche Zecke und Behörden	Personenstammdaten, Vertragsdaten, Leistungsdaten
Centris	EGK	Debit: Bearbeitung von Inkassofällen	Betreibungsinformationen
Centris	Ämter	Austausch an Betreibungsämter (eSchKG) für rechtliches Inkasso und DA 64 mit Kantonen (Leistungsaufschub, Quartalsabrechnungen Verlustscheine)	Partnerstammdaten (Schuldnerangaben) und offene Forderungen
SASIS AG	Centris	Zahlstellenregister und zentrales Vertragsregister der Leistungserbringer	Adressstammdaten und Tarifpreise der Leistungserbringer
Medidata	Centris	Tarifdaten	Tarifdaten des schweizerischen Gesundheitssystems (Taxpunkte)

Abbildung 2: Beschreibung der Schnittstellen

2.3 Prozessverantwortliche

Die Prozessverantwortlichen und Endanwender sorgen für die Einhaltung der gesetzlichen und vertraglichen Bestimmungen, Weisungen und internen Regularien zur Datenbearbeitung, insbesondere in den Bereichen Datensicherheit und Datenschutz.

Sie sind verantwortlich, dass die Applikationsdaten nur gemäss den Rechtsgrundlagen oder gemäss weitergehenden Einschränkungen aufgrund des vorliegenden Reglements, der Informationssicherheitspolitik der EGK und der internen Weisungen zur Verfügung gestellt werden.

Ebenfalls definiert die EGK für jede personenbezogene Datenbearbeitung die entsprechenden Verantwortlichkeiten (siehe Kapitel 4.5 Verzeichnis der Bearbeitungstätigkeiten).

3 An den Datenbearbeitungen beteiligte Personen

3.1 Benutzertypen mit entsprechenden Zugriffsrechten

- Mitarbeitende der EGK, soweit sie dies zur Ausübung ihres Auftrages benötigen
- Mitarbeitende von externen Dienstleistungsunternehmen, soweit sie dies zur Ausübung ihres Auftrages benötigen und gemäss den vertraglichen und rechtlichen Vorgaben (siehe auch Kapitel 1.5 Outsourcing)

Zusatzberechtigungen auf MCD haben:

- Fachspezialist/innen DRG / Codierspezialist/innen (2 Personen)

Zusatzberechtigungen auf Dokumente des VAD:

- Mitarbeitende VAD

3.2 Benutzerverwaltung

Die Benutzerrechte sind rollenbasiert konzipiert und ausgestaltet. Zuständig für die Definition der einzelnen Rollen ist die zuständige Fachabteilung. Die datenschutzberatende Person überwacht dabei die datenschutzrechtlichen Anforderungen und das Prinzip der Gewaltentrennung.

Die Verwaltung der Benutzerrechte basiert auf einem definierten Standardprozess (Eintritt, Mutation, Austritt). Die Mitarbeitenden erhalten lediglich die Berechtigung auf die für ihre Arbeit notwendigen Daten (Prinzip «need to know»). Bei Mutationen (z.B. Abteilungswechsel) werden die Berechtigungen entsprechend angepasst. Mitarbeitenden, die die EGK verlassen, wird der Zugriff auf die Daten spätestens ab dem letzten Arbeitstag gesperrt.

Die Mitarbeitenden werden im Rahmen der Basisschulung der EGK sowie bereichsintern aufgabenbezogen betreffend Datenschutz ausgebildet. Zudem ist das Thema Datenschutz fester Bestandteil der jährlichen Compliance-Schulungen und es besteht ein Awareness-Programm zur regelmässigen Sensibilisierung der Mitarbeitenden. Ferner stehen den Mitarbeitenden die speziellen Datenschutzkurse des Branchenverbandes offen. Für die Fachspezialist/innen DRG und die Mitarbeitenden des VAD sind diese Kurse zwingend.

4 Datenbearbeitungsverfahren

4.1 Zweck der Datenbearbeitung

Die EGK bearbeitet im Bereich der obligatorischen Krankenpflegeversicherung und der freiwilligen Taggeldversicherung nach KVG die Daten in Erfüllung der gesetzlichen Rechte und Pflichten zur Durchführung des Versicherungsgeschäfts. Im Bereich der Krankenpflegezusatzversicherungen nach VVG erfolgt die Bearbeitung der Daten zum Zwecke der Erfüllung der vertraglichen Rechte und Pflichten zur Durchführung des Versicherungsgeschäfts. Die Datenbearbeitung dokumentiert insbesondere das Versicherungsverhältnis im Rahmen des Vertragsabschlusses, der Zahlungsverarbeitung sowie der Prüfung und Abwicklung der Leistungsansprüche der versicherten Personen.

4.2 Herkunft der Daten und ihre Kategorien

Die Daten stammen einerseits von den versicherten Personen und andererseits von natürlichen und juristischen Personen wie Leistungserbringern, Versicherungen und Behörden, die von Gesetzes wegen oder per Einwilligung durch versicherte Personen, legitimiert wurden, Daten zu übermitteln.

Die folgenden Daten der bearbeiteten Personendaten werden in den jeweiligen Applikationen gemäss Art. 12 Abs. 2 Bst. c. DSG kategorisiert und vor unbefugter Einsicht geschützt:

- Name, Vorname, Adresse, Telefonnummern, (E-Mail)
- Geburtsdatum
- Versicherungsnummer
- Sozialversicherungsnummer
- Sprache und Nationalität
- Familiensituation und gesetzliche Vertretung
- Angaben zur Gesundheit
- Massnahmen der sozialen Hilfe
- Leistungsdaten
- Prämiendaten
- Zahlungsverbindung
- Mahn- und Inkassodaten

4.3 Datenbekanntgabe

Im Bereich der Grundversicherung werden die Daten im Rahmen der gesetzlichen Vorschriften gemäss Art. 84a KVG bekanntgegeben. Im Bereich der Zusatzversicherungen erfolgt die Datenbekanntgaben auf der Basis des abgeschlossenen Versicherungsvertrages. In allen anderen Fällen erfolgt die Datenbekanntgabe an Dritte mit schriftlicher Einwilligung der betroffenen Person.

4.4 Aufbewahrungsdauer und Löschung der Daten

Die minimale Aufbewahrungsdauer richtet sich nach der spezifischen gesetzlichen Aufbewahrungspflicht gemäss den massgebenden Bestimmungen des schweizerischen Rechts. Die Daten werden vor Veränderung und unerlaubtem Zugriff geschützt und nach Ablauf der Aufbewahrungspflicht aus dem EGK-Informationssystem gelöscht.

4.5 Verzeichnis der Bearbeitungstätigkeiten

Die EGK führt ein Verzeichnis der Bearbeitungstätigkeiten über alle personenbezogenen Datenbearbeitungen, welches insbesondere Auskunft über die Verantwortlichkeiten, Zwecke und Aufbewahrungsdauer der entsprechenden Personendaten gibt.

4.6 Verfahren zur Anonymisierung der Daten

Testungen sollen, wenn immer möglich mit anonymen Datensätzen erfolgen. Zudem werden Daten, wo es das Gesetz verlangt, stets anonymisiert für statistische Zwecke verwendet.

5 Datensicherheit

Die EGK schützt ihre Systeme mit autorisierten Zugriffsberechtigungen per Benutzername, Passwort und allenfalls weiteren Faktoren. Zudem ist der Zugang zu Anwendungen, welche Zugriff auf Personendaten ermöglichen, mit einer zeitlichen Limite versehen. Wird die Anwendung eine gewisse Zeit nicht benutzt, wird eine erneute Anmeldung mit Eingabe des Passwortes notwendig.

5.1 Technische und organisatorische Massnahmen

Gestützt auf Art. 3 DSV schützt die EGK ihre Systeme gegen unbefugte oder zufällige Vernichtung, zufälligen Verlust, technische Fehler, Fälschung, Diebstahl oder widerrechtliche Verwendung und unautorisierte Bearbeitung, wofür die EGK die folgenden generellen Massnahmen getroffen hat:

- Die Daten befinden sich in Rechenzentren, die mit den modernsten technischen Mitteln und organisatorischen Massnahmen gesichert sind. Spezialräume, wo sich IT-technische Anlagen befinden, sind zusätzlich gesichert.
- Im individuellen E-Mailverkehr muss bei der Übermittlung von besonders schützenswerten Personendaten (insbesondere bei Gesundheitsdaten) das Verschlüsselungsverfahren angewandt werden.
- Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, werden über die Schnittstellen identifiziert. Die regelmässigen Übermittlungen von Personendaten finden immer standardisiert über einen verschlüsselten Kanal statt (z.B. SFTP).
- Es dürfen nur EGK-eigene Endgeräte am internen Netzwerk angeschlossen werden. Die Schnittstellen für möglichen Datenaustausch sind gesperrt und nur einem eingeschränkten Personenkreis freigegeben.
- Datenexporte auf fremde Speichermedien (z.B. USB Stick) ist technisch unterdrückt.
- Die lokalen Datenspeicher in den mobilen Endgeräten werden durch ein starkes, kryptographisches Verfahren verschlüsselt und mit Passwort geschützt.

Nachfolgend werden die technischen und organisatorischen Massnahmen im Einzelnen kurz erläutert.

5.1.1 Zugriffskontrolle

Nur berechtigte Personen erhalten Zugriff auf die SHP und deren Umsysteme sowie die EGK-eigenen Systeme (Prinzip «need to know»). Der Zugriff auf die EGK-eigenen Informationssysteme ist durch eine User-ID kombiniert mit einem zeitlich limitierten, individuellen Passwort (gemäss Passwortrichtlinie EGK) geschützt. Die Passwortrichtlinie wird über entsprechende technische Vorgaben durchgesetzt. Gewisse Systeme sind zusätzlich mit der Verwendung eines weiteren Passwortes geschützt.

5.1.2 Zugangskontrolle

Der Zutritt zu den Räumlichkeiten der EGK ist mit einem Badgesystem vor dem Zugang unbefugter Personen gesichert. Durch speziell eingerichtete Beratungszonen und mit räumlichen Massnahmen wird verhindert, dass unbefugte Dritte Einsicht oder Zugang zu Räumen und Zonen haben, in denen Personendaten bearbeitet werden.

Dritte haben nur im Einverständnis mit der EGK und mit Besucher-Badge oder in Begleitung von Mitarbeitenden Zutritt zu den Arbeitsplätzen. Besucher müssen sich jeweils beim Empfang anmelden, wo ihnen der Besucher-

Badge übergeben wird, welcher gut sichtbar getragen werden muss.

Zu Räumen, in welchen besonders schützenswerte Daten vorhanden sind oder bearbeitet werden (VAD, Technikräume usw.) ist der Zutritt zusätzlich auf den notwendigen Kreis der Mitarbeitenden eingeschränkt.

5.1.3 Benutzerkontrolle

Die Erteilung von Benutzerrechten sowie allfällige Änderungen an den bestehenden Berechtigungen folgen einem klar definierten Bewilligungsprozess. Bestehende Berechtigungen werden regelmässig überprüft und bei Bedarf angepasst. Bei Mutationen (z.B. Abteilungswechsel) werden die Berechtigungen entsprechend angepasst. Bei einem Austritt wird der Zugriff auf die Daten spätestens ab dem letzten Arbeitstag gesperrt.

5.1.4 Datenträgerkontrolle

Die Daten werden ausschliesslich „remote“ bearbeitet. Ausserdem sorgt die Erteilung der Zugriffsberechtigungen dafür, dass Mitarbeitende lediglich die für ihre Arbeit notwendigen Zugriffe auf Daten erhalten (Prinzip «need to know») und somit das Lesen, Kopieren, Verändern oder Löschen von Daten für unbefugte Personen verunmöglicht wird.

5.1.5 Speicherkontrolle

Durch sicherheitstechnische Vorkehrungen ist es ausschliesslich berechtigten Personen möglich, Daten im EGK-Informationssystem abzufragen, zu bearbeiten oder zu speichern. Die unbefugte Eingabe in den Speicher sowie die unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten wird somit verunmöglicht.

5.1.6 Transportkontrolle

Werden Daten ausgetauscht respektive an Dritte übermittelt, erfolgt der Transfer immer über verschlüsselte Kanäle (siehe auch Kapitel 2).

5.1.7 Wiederherstellung

Zusammen mit ihren Outsourcing-Partnern im Bereich IT Dienstleistungen und Services stellt die EGK über die gesamte Prozesskette mit den definierten BCM-Massnahmen eine möglichst rasche Wiederaufnahme der Geschäftsprozesse sicher.

5.1.8 Verfügbarkeit, Zuverlässigkeit, Datenintegrität

Es wird sichergestellt, dass die Verfügbarkeit, die Integrität und die vertrauliche respektive datenschutzkonforme Behandlung der Daten von Versicherten, Mitarbeitenden und Partnern jederzeit gewährleistet sind.

5.1.9 Systemsicherheit

Die EGK stellt sicher, dass mittels geeigneter Massnahmen die Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden.

5.1.10 Eingabekontrolle (Protokollierung)

Es wird eine Eingabe- und Änderungskontrolle aller Mutationen geführt. So kann sichergestellt werden, dass nachträglich überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden.

5.1.11 Bekanntgabekontrolle

Die EGK stellt sicher, dass Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, über die Schnittstellen identifiziert werden können.

5.1.12 Erkennung und Beseitigung

Die EGK stellt sicher, dass mittels geeigneten Massnahmen Verletzungen der Datensicherheit rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden.

6 Rechte der Betroffenen

6.1 Auskunftsrecht

Jede Person kann von der EGK Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden. Das Auskunftsrecht richtet sich nach Art. 25 und 26 DSG sowie Art. 16 bis 19 DSV. Das Auskunftsgesuch ist unter Beilage einer Kopie eines amtlichen Ausweises an die datenschutzberatende Person zu richten (datenschutz@egk.ch).

6.2 Datenportabilität

Jede Person kann von der EGK die Herausgabe ihrer Personendaten, die sie ihm bekanntgegeben hat, in einem gängigen elektronischen Format und wenn es keinen unverhältnismässigen Aufwand erfordert die Übertragung ihrer Personendaten an einen anderen Verantwortlichen verlangen, wenn die Voraussetzungen von Art. 28 Abs. 1 Bst. a und b DSG erfüllt sind.

6.3 Widerspruch gegen die Bekanntgabe

Die betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, kann gegen die Bekanntgabe bestimmter Personendaten durch das verantwortliche Bundesorgan Widerspruch einlegen. Dieser Rechtsanspruch richtet sich nach Art. 37 DSG. Falls eine Rechtspflicht zur Bekanntgabe besteht oder die Erfüllung der Aufgaben des verantwortlichen Bundesorgans gefährdet wäre, wird das Begehren abgewiesen.

6.4 Berichtigungs- und Löschungsrecht

Das Berichtigungs- und Löschungsrecht betroffener Personen richtet sich nach Art. 32 und 41 DSG unter Wahrung der gesetzlichen und/oder vertraglichen Aufbewahrungspflichten. Ein entsprechendes Gesuch ist an die EGK zuhanden der datenschutzberatenden Person zu richten (datenschutz@egk.ch).

7 Abschliessende Bestimmungen

7.1 Sicherstellung des Datenschutzes durch die Versicherer

Das vorliegenden Reglement wurde gemäss Art. 84b KVG erstellt und dient der Information der betroffenen Personen über ihre Rechte sowie der Dokumentation der technischen und organisatorischen Massnahmen zur Sicherstellung der Datensicherheit und des Datenschutzes. Es wird auf der Website der EGK veröffentlicht.

7.2 Weiterführende Unterlagen

Aus Gründen der Sicherheit von Systemen, Prozessen und Daten, der Wahrung der Vertraulichkeit der Versicherten sowie des Schutzes von Geschäftsgeheimnissen der EGK und ihren Geschäftspartnern, werden die in

diesem Reglement erwähnten weiterführenden Unterlagen nicht öffentlich zugänglich gemacht.

7.3 Zuständigkeit / Überprüfung

Dieses Reglement wird von der EGK gemäss Art. 5 und 6 DSV regelmässig aktualisiert. In Zusammenarbeit mit den zuständigen Fachstellen überprüft es die datenschutzberatende Person mindestens jährlich auf seine Aktualität und lässt es von der Geschäftsleitung genehmigen. Bei Bedarf kann es jederzeit angepasst werden.

7.4 Inkrafttreten

Dieses Reglement tritt per 1. September 2023 in Kraft und ersetzt die vorhergehende Version.