Regolamento per il trattamento dei dati della EGK-Cassa della Salute

La EGK-Cassa della salute comprende la Fondazione EGK-Cassa della salute con le società anonime ad essa affiliate EGK Assicurazioni di base SA (assicuratore nell'ambito dell'assicurazione obbligatoria delle cure medico-sanitarie secondo LAMal) ed EGK Assicurazioni private SA (assicuratore nell'ambito delle assicurazioni complementari secondo LCA).

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

Sommario

Abbreviazioni

Sigla	Descrizione
LPGA	Legge federale del 6 ottobre 2000 sulla parte generale del diritto delle assicurazioni sociali (RS 830.1)
UFSP	Ufficio federale della sanità pubblica
Cent	Cent Systems AG
Centris	Centris AG
SRD	Servizio di ricezione dei dati
DRG	Diagnosis Related Groups (raggruppamenti omogenei di diagnosi)
LPD	Legge federale del 1° settembre 2023 sulla protezione dei dati (RS 235.1)
OPDa	Ordinanza del 1° settembre 2023 sulla protezione dei dati (RS 235.11)
IFPDT	Incaricato federale della protezione dei dati e della trasparenza
FINMA	Autorità federale di vigilanza sui mercati finanziari
IaaS	Infrastructure as a Service
LAMal	Legge federale del 18 marzo 1994 sull'assicurazione malattie (RS 832.10)
LVAMal	Legge federale del 26 settembre 2014 concernente la vigilanza sull'assicurazione sociale contro le malattie (RS 832.12)
MCD	Minimal Clinical Dataset
SaaS	Software as a Service
SFTP	Secure File Transfer Protocol
SHP	Swiss Health Platform
SPS	Swiss Post Solutions AG
SMF	Servizio del medico di fiducia
LCA	Legge federale del 2 aprile 1908 sul contratto d'assicurazione (RS 221.229.1)

1 Aspetti generali

1.1 Ambito di applicazione

Il presente regolamento sul trattamento dei dati (di seguito denominato «regolamento») della EGK-Cassa della Salute (di seguito denominata «EGK») si applica a tutti i soggetti giuridici che aderiscono al Gruppo EGK. Da un lato, la EGK Assicurazioni di base SA tratta i dati personali nell'ambito dell'assicurazione sociale malattia (assicurazione obbligatoria delle cure medico-sanitarie e assicurazione facoltativa d'indennità giornaliera) e, dall'altro, la EGK Assicurazioni private SA tratta i dati personali nell'ambito dell'assicurazione malattia complementare privata.

Il presente documento cerca di usare formulazioni neutre rispetto al genere. Ove ciò non fosse possibile, viene usato solo un genere per una migliore leggibilità. Le relative denominazioni si applicano a tutti i generi.

1.2 Base giuridica

La EGK tratta i dati personali in conformità alle disposizioni della LPD. Nella sua funzione di organo federale e di assicurazione malattia autorizzata ai sensi della LVAMal, è legittimata per legge al trattamento dei dati personali nell'ambito della LAMal. In qualità di fornitore di assicurazioni malattia complementari ai sensi della LCA, tratta i dati personali anche come persona giuridica privata sulla base dei contratti di assicurazione stipulati con la clientela.

Sulla base dell'art. 6 della OPDa in combinato disposto con l'art. 84b della LAMal, la EGK ha elaborato il presente regolamento per il trattamento automatizzato dei dati che contengono informazioni degne di particolare protezione o dati di profilazione. Il trattamento dei dati viene eseguito dalla EGK per adempiere ai propri compiti di assicurazione malattia sociale e privata. Ai sensi dell'art. 12 cpv. 1 e 4 LPD in combinato disposto con l'art. 56 LPD, la EGK in qualità di organo federale, è tenuta a comunicare il trattamento dei dati personali all'IFPDT, il quale pubblica tale comunicazione in un registro accessibile al pubblico (https://datareg.edoeb.admin.ch/search).

1.3 Scopo del regolamento

Il regolamento descrive le procedure di trattamento e di controllo e la gestione del trattamento elettronico dei dati della EGK. Contiene indicazioni sui settori e sulle persone responsabili della protezione e della sicurezza dei dati, sulla provenienza dei dati e sugli scopi e descrive la procedura di assegnazione dei diritti di accesso ai singoli moduli dei sistemi informatici elettronici.

1.4 Titolare del trattamento

La Direzione EGK è responsabile delle decisioni in termini di finalità e mezzi di trattamento dei dati.

1.5 Outsourcing

Il trattamento dei dati personali può essere trasferito a terzi per legge o previo accordo (outsourcing). I principali servizi di outsourcing fanno parte delle voci con obbligo di approvazione da parte delle autorità di vigilanza (UFSP per l'assicurazione sociale malattia secondo LAMal e FINMA per l'assicurazione malattia complementare secondo LCA) da inserire nel piano d'esercizio.

I fornitori di servizi sono tenuti a trattare i dati loro forniti esclusivamente nell'ambito del quadro definito per contratto, così come li può trattare anche la EGK in conformità alle rispettive norme giuridiche applicabili e qualora nessun obbligo di riservatezza legale o contrattuale lo vieti.

1.6 Obbligo del segreto ai sensi dell'art. 33 LPGA

Tutti i collaboratori sono tenuti all'obbligo del segreto ai sensi dell'art. 33 LPGA. Inoltre, congiuntamente al contratto di lavoro sottoscrivono anche una dichiarazione con cui si impegnano a mantenere il segreto e la riservatezza. Si applicano peraltro le disposizioni in materia di segretezza e riservatezza del Codice di comportamento della EGK.

1.7 Servizio di ricezione dei dati certificato (SRD)

Il SRD della EGK, obbligatorio per legge, è gestito dalla società Centris di Soletta che offre questo servizio agli assicuratori malattie. L'area di certificazione del SRD (campo d'attività) non coinvolge quindi soltanto Centris e il suo SRD, ma anche alcuni reparti della EGK, SPS e Cent (ved. anche il capitolo 2 Modello operativo e interfacce IT).

2 Modello operativo e interfacce IT

2.1 Modello operativo

Per lo svolgimento delle proprie attività nell'ambito dell'assicurazione sociale malattia e dell'assicurazione malattia complementare privata, la EGK, oltre ad avere i propri servizi IT Business, acquista anche servizi aziendali da fornitori informatici selezionati sotto forma di IaaS e SaaS. Il sistema cardine dell'assicurazione malattia è costituito dalla SHP di Centris.

2.2 Interfacce

La EGK riceve dati dai propri clienti e fornitori di servizi. Le fatture elettroniche vengono trasmesse nel relativo formato dai fornitori di servizi direttamente a Centris o al SRD gestito da Centris. I giustificativi cartacei delle fatture vengono scansionati da SPS e trasmessi a Cent per l'acquisizione delle fatture (capturing), che fornisce poi i dati nel formato adeguato per la successiva elaborazione in Centris. Le lettere di corrispondenza e i moduli vengono importati nel sistema centrale di assicurazione malattia SHP di Centris dopo la scansione presso SPS.

La EGK e i suoi fornitori di servizi applicano tecniche moderne di cifratura simmetrica e asimmetrica per lo scambio dei dati. Le interfacce sicure consentono il contatto e lo scambio elettronico di dati con clienti, fornitori di prestazioni, autorità e altri fornitori di servizi.

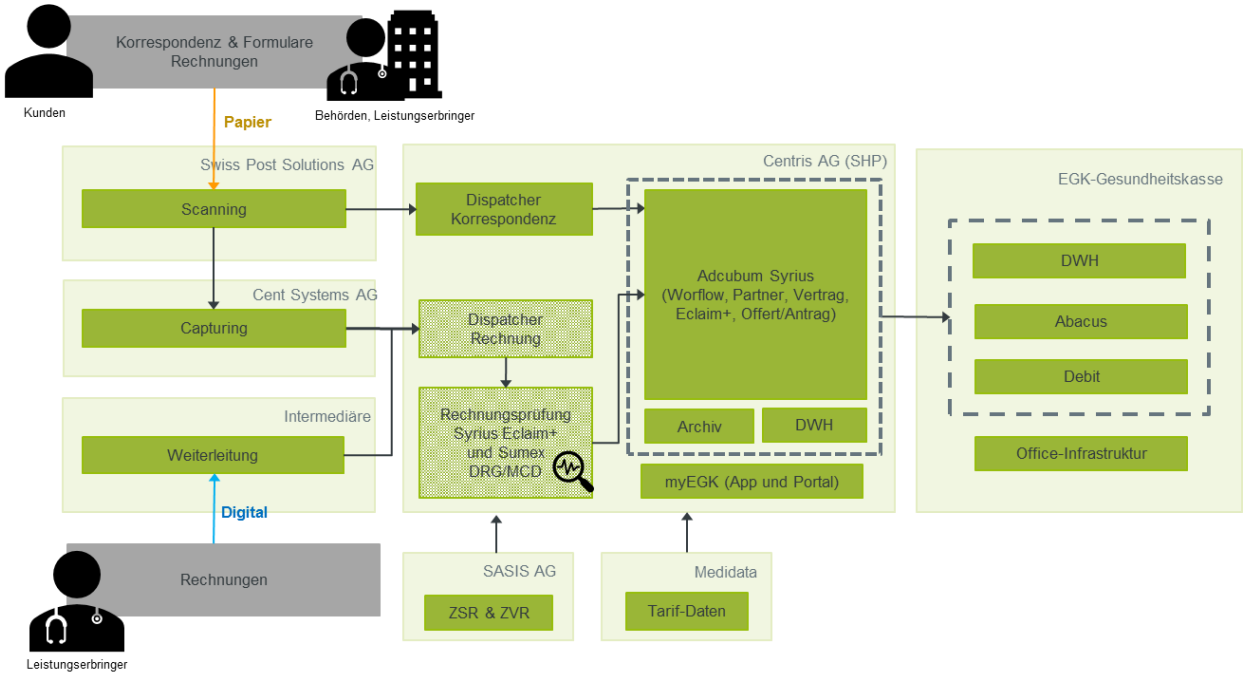

Figura 1 Schema delle interfacce

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)

Figura 2: Descrizione delle interfacce

2.3 Responsabili dei processi

I responsabili dei processi e gli utenti finali garantiscono il rispetto delle disposizioni e delle istruzioni legali e contrattuali così come dei regolamenti interni sul trattamento dei dati, in particolare per quanto riguarda la sicurezza e la protezione dei dati.

Sono tenuti a mettere a disposizione i dati applicativi solo ai sensi dei principi giuridici o conformemente a ulteriori limitazioni stabilite dai regolamenti presenti e dalla policy per la sicurezza dei sistemi d'informazione della EGK e da istruzioni interne.

La EGK definisce anche le responsabilità corrispondenti per ogni trattamento di dati personali (ved. capitolo 4.5 Registro delle attività di trattamento).

3 Persone coinvolte nel trattamento dei dati

3.1 Tipi di utenti con i relativi diritti di accesso

- Collaboratori della EGK, qualora ciò sia richiesto per lo svolgimento delle loro mansioni
- Collaboratori di aziende di servizi esterne, qualora ciò sia richiesto per lo svolgimento delle loro mansioni e in conformità ai requisiti contrattuali e legali (ved. anche capitolo 1.5 Outsourcing)

Dispongono di autorizzazioni supplementari per gli MCD:

- specialisti DRG / specialisti delle codifiche (2 persone)

Autorizzazioni aggiuntive ai documenti del SMF:

- collaboratori SMF

3.2 Amministrazione utenti

I diritti di accesso degli utenti sono strutturati e organizzati in base ai ruoli. La definizione dei singoli ruoli spetta al reparto specialistico di competenza. Il consulente per la protezione dei dati controlla i requisiti di protezione dei dati e il principio della separazione dei poteri.

La gestione dei diritti degli utenti si basa su un processo standard definito (entrata, mutazione, uscita). I collaboratori sono autorizzati ad accedere solo ai dati necessari per il proprio lavoro (principio «need to know»/«necessità di sapere»). In caso di mutazioni (es. cambio di reparto), le autorizzazioni vengono modificate di conseguenza. I collaboratori che lasciano la EGK vedranno bloccato il loro accesso ai dati al più tardi a partire dal loro ultimo giorno di lavoro.

I collaboratori sono istruiti in merito alla protezione dei dati sia durante la formazione di base della EGK sia durante lo svolgimento delle loro mansioni nei rispettivi reparti. Il tema della protezione dei dati è, inoltre, parte integrante della formazione annuale sulla compliance ed esiste un programma di awareness per sensibilizzare regolarmente i collaboratori. I collaboratori possono inoltre frequentare gli appositi corsi sulla protezione dei dati offerti dall'associazione di categoria, che sono obbligatori per gli specialisti DRG e per i collaboratori del SMF.

4 Procedura di trattamento dei dati

4.1 Scopo del trattamento dei dati

Nell'ambito dell'assicurazione obbligatoria delle cure medico-sanitarie e dell'assicurazione facoltativa d'indennità giornaliera ai sensi della LAMal, la EGK tratta i dati in adempimento dei diritti e degli obblighi previsti dalla legge per l'esercizio dell'attività assicurativa. Nell'ambito delle assicurazioni complementari delle cure medico-sanitarie ai sensi della LCA, il trattamento dei dati avviene per l'adempimento dei diritti e degli obblighi contrattuali per l'esercizio dell'attività assicurativa. Il trattamento dei dati è documentato in particolare dal contratto d'assicurazione nell'ambito della conclusione del contratto, della gestione del pagamento nonché della verifica e della gestione dei diritti alle prestazioni degli assicurati.

4.2 Origine dei dati e relative categorie

I dati provengono da un lato dalle persone assicurate e dall'altro da persone fisiche e giuridiche come fornitori di servizi, assicurazioni e autorità che sono state legittimate dalla legge o dal consenso delle persone assicurate alla trasmissione dei dati.

I seguenti dati personali trattati vengono classificati nelle rispettive applicazioni ai sensi dell'art. 12 cpv. 2 lett. c LPD e protetti dall'accesso non autorizzato.

- Cognome, nome, indirizzo, numeri di telefono, (e-mail)
- Data di nascita
- Numero di assicurazione
- Numero di assicurazione sociale
- Lingua e nazionalità
- Situazione familiare e rappresentanza legale
- Informazioni sulla salute
- Misure di assistenza sociale
- Dati relativi alle prestazioni
- Dati relativi ai premi
- Coordinate di pagamento
- Dati di sollecito e incasso

4.3 Comunicazione dei dati

Nell'ambito dell'assicurazione di base, i dati vengono comunicati nell'ambito delle disposizioni di legge ai sensi dell'art. 84a LAMal. Nel settore delle assicurazioni complementari, i dati vengono comunicati in base al contratto di assicurazione stipulato. In tutti gli altri casi, i dati vengono comunicati a terzi previo consenso scritto della persona interessata.

4.4 Durata di conservazione e cancellazione dei dati

Il periodo minimo di conservazione si basa sullo specifico obbligo legale di conservazione in conformità alle disposizioni pertinenti del diritto svizzero. I dati sono protetti da modifiche e accessi non autorizzati e vengono cancellati dal sistema informatico EGK alla scadenza del periodo di conservazione.

4.5 Registro delle attività di trattamento

La EGK tiene un registro delle attività di trattamento per tutte le operazioni di trattamento di dati personali. Tale registro fornisce in particolare informazioni su responsabilità, finalità e periodo di conservazione dei dati personali corrispondenti.

4.6 Procedura per l'anonimizzazione dei dati

I test dovrebbero essere eseguiti possibilmente con record dati anonimi. Inoltre, ove richiesto dalla legge, i dati vengono sempre utilizzati in forma anonima per fini statistici.

5 Sicurezza dei dati

La EGK protegge i propri sistemi con diritti di accesso autorizzati tramite nome utente, password ed eventuali altri fattori. Inoltre, l'accesso alle applicazioni che consentono l'accesso ai dati personali è soggetto a un limite temporale. Se l'applicazione non viene utilizzata per un certo tempo, è necessario effettuare nuovamente il login e inserire la password.

5.1 Provvedimenti tecnici e organizzativi

In base all'art. 3 OPDa, la EGK protegge i propri sistemi contro distruzione non autorizzata o accidentale, perdita accidentale, errori tecnici, falsificazione, furto o uso illegale e trattamento non autorizzato. A questo scopo, la EGK ha adottato le seguenti misure generali:

- I dati si trovano in centri di calcolo protetti con i più moderni mezzi tecnici e misure organizzative. I locali speciali in cui si trovano impianti tecnici informatici sono ulteriormente protetti.
- Per la trasmissione di dati personali degni di particolare protezione (specificamente dati sanitari) tramite messaggi di posta elettronica individuale si deve fare ricorso alla cifratura.
- I destinatari di dati personali inviati mediante dispositivi per la trasmissione di dati sono identificati tramite le interfacce. Le trasmissioni periodiche di dati personali avvengono sempre in maniera standardizzata attraverso un canale cifrato (es. SFTP).
- È consentito collegare alla rete interna unicamente terminali della EGK. Le interfacce per l'eventuale scambio dei dati sono bloccate e abilitate solo per una determinata cerchia di persone.
- L'esportazione dei dati su supporti di memoria esterni (es. chiavetta USB) è tecnicamente soppressa.
- Le memorie dati locali dei terminali mobili sono cifrate con una valida procedura crittografica e protette da password.

Di seguito sono spiegati brevemente nel dettaglio i provvedimenti tecnici e organizzativi.

5.1.1 Controllo degli accessi

Solo alle persone autorizzate è consentito l'accesso a SHP e ai relativi sistemi periferici, nonché ai sistemi informatici EGK

(principio «need to know»/«necessità di sapere»). L'accesso ai sistemi informatici EGK è protetto da un User ID abbinato a una password personale con validità temporale limitata (secondo la direttiva EGK sulle password). La direttiva sulle password viene applicata tramite standard tecnici specifici. Determinati sistemi periferici sono protetti con l'uso di una password ulteriore.

5.1.2 Controllo dell'accesso

L'accesso ai locali della EGK è protetto tramite sistema a badge per impedire l'accesso di persone non autorizzate. Zone di consulenza appositamente allestite e misure concernenti i locali impediscono a terzi non autorizzati di prendere visione o accedere a locali e zone in cui vengono trattati dati personali.

Persone terze possono accedere ai luoghi di lavoro solo previo consenso della EGK e con un badge per visitatori o accompagnate da collaboratori. I visitatori devono annunciarsi presso la reception, dove riceveranno un badge per visitatori, che deve essere indossato in modo visibile.

L'accesso a locali in cui sono presenti o vengono trattati dati degni di particolare protezione (SMF, locali tecnici ecc.) è inoltre limitato alla cerchia dei collaboratori strettamente necessari.

5.1.3 Controllo dell'utente

La concessione dei diritti di utente e le eventuali modifiche alle autorizzazioni esistenti seguono un processo di approvazione chiaramente definito. Le autorizzazioni esistenti vengono controllate regolarmente e, se necessario, modificate. In caso di mutazioni (es. cambio di reparto), le autorizzazioni vengono modificate di conseguenza. In caso di uscita, l'accesso ai dati viene bloccato al più tardi a partire dall'ultimo giorno lavorativo.

5.1.4 Controllo dei supporti di dati

I dati sono trattati solo «da remoto». Inoltre, la concessione delle autorizzazioni di accesso garantisce che i collaboratori ricevano l'accesso solo ai dati necessari per il proprio lavoro (principio «need to know»/«necessità di sapere»), rendendo così impossibile leggere, copiare, modificare o cancellare i dati da parte di persone non autorizzate.

5.1.5 Controllo della memoria

Misure tecniche di sicurezza garantiscono la possibilità di richiamare, trattare o salvare dati nel sistema informatico EGK esclusivamente alle persone autorizzate. In questo modo si rende impossibile l'inserimento non autorizzato in memoria, nonché la visione, la modifica o la cancellazione non autorizzata dei dati personali memorizzati.

5.1.6 Controllo del trasporto dei dati

Se i dati vengono scambiati o trasmessi a terzi, il trasferimento avviene sempre tramite canali criptati (ved. anche capitolo 2).

5.1.7 Ripristino

Insieme ai suoi partner di outsourcing nel settore dei servizi IT, la EGK assicura il ripristino più rapido possibile dei processi aziendali lungo l'intera catena sulla base delle misure BCM definite.

5.1.8 Disponibilità, affidabilità, integrità dei dati

Si garantiscono in ogni momento la disponibilità, l'integrità e il trattamento confidenziale e conforme alle norme sulla protezione dei dati per quanto riguarda i dati di assicurati, collaboratori e partner.

5.1.9 Sicurezza del sistema

La EGK assicura con opportune misure che i sistemi operativi e il software applicativo eseguano sempre gli ultimi aggiornamenti di sicurezza e che le criticità note siano risolte.

5.1.10 Controllo degli inserimenti (verbalizzazione)

Viene eseguito un controllo di inserimenti e modifiche. Ciò consente di verificare a posteriori quali dati personali sono stati inseriti, quando e da chi.

5.1.11 Controllo della comunicazione dei dati

La EGK si assicura che i destinatari di dati personali inviati mediante dispositivi per la trasmissione di dati possano essere identificati tramite interfacce.

5.1.12 Rilevamento ed eliminazione

La EGK assicura con opportune misure che le violazioni della sicurezza dei dati siano rilevate tempestivamente e che siano presi provvedimenti per attenuare o evitare le conseguenze.

6 Diritti delle persone interessate

6.1 Diritto d'accesso

Ogni persona può chiedere alla EGK se sono trattati dati personali che la riguardano. Il diritto d'accesso si basa sugli artt. 25 e 26 LPD e sugli artt. da 16 a 19 OPDa. La richiesta di accesso deve essere inoltrata al consulente per la protezione dei dati con allegata la copia di un documento d'identità (datenschutz@egk.ch).

6.2 Portabilità dei dati

Ogni persona può esigere dalla EGK che i dati personali che la concernono e che le ha comunicato le siano consegnati in un formato elettronico usuale e che vengano trasmessi a un altro titolare del trattamento, se ciò non richiede un onere sproporzionato e se sussistono i requisiti dell'art. 28 cpv. 1 lett. a e b LPD.

6.3 Opposizione alla comunicazione di dati personali

La persona interessata che rende verosimile un interesse degno di protezione può opporsi alla comunicazione di determinati dati personali da parte dell'organo federale competente. Questo diritto legale è disciplinato all'art. 37 LPD. L'organo federale respinge l'opposizione se sussiste un obbligo legale alla comunicazione o l'adempimento del suo compito ne risultasse altrimenti pregiudicato.

6.4 Diritto di rettifica e diritto di cancellazione

Il diritto di rettifica e il diritto di cancellazione delle persone interessate sono disciplinati dagli artt. 32 e 41 LPD, nel rispetto degli obblighi legali e/o contrattuali di conservazione dei dati. Una richiesta in tal senso deve essere indirizzata alla EGK all'attenzione del consulente per la protezione dei dati (datenschutz@egk.ch).

7 Disposizioni conclusive

7.1 Garanzia della protezione dei dati da parte degli assicuratori

Il presente regolamento è stato redatto ai sensi dell'art. 84b LAMal e serve a informare le persone interessate sui loro diritti

e a documentare i provvedimenti tecnici e organizzativi per garantire la sicurezza e la protezione dei dati. Esso sarà pubblicato sul sito web della EGK.

7.2 Ulteriore documentazione

Per motivi di sicurezza di sistemi, processi e dati, di tutela della riservatezza delle persone assicurate e di protezione dei segreti aziendali della EGK e dei suoi partner commerciali, gli ulteriori documenti menzionati in questo regolamento non saranno resi accessibili al pubblico.

7.3 Competenza / Revisione

Il presente regolamento viene aggiornato periodicamente dalla EGK secondo gli artt. 5 e 6 OPDa. In collaborazione con gli uffici tecnici competenti, il consulente per la protezione dei dati lo sottopone a revisione e aggiornamento almeno annualmente e lo trasmette alla Direzione per l'approvazione. All'occorrenza può essere modificato in qualsiasi momento.

7.4 Entrata in vigore

Il presente regolamento entra in vigore il 1° settembre 2023 e sostituisce la versione precedente.