Regolamento per il trattamento della collezione di dati della fondazione Cassa d'indennità giornaliera per gli artisti ai sensi della LAMal

1. Disposizioni generali

1.1 Base giuridica

Ai sensi dell'art. 21 dell'Ordinanza relativa alla legge federale sulla protezione dei dati (OLPD) in relazione all'art. 84 della Legge federale sull'assicurazione contro le malattie (LAMal), la fondazione della Cassa d'indennità giornaliera per gli artisti ha allestito il presente regolamento per il trattamento della collezione automatizzata di dati.

1.2 Scopo del regolamento per il trattamento

Il regolamento per il trattamento descrive, in particolare, le procedure di trattamento e di controllo e la gestione del trattamento elettronico dei dati. Esso contiene indicazioni sull'organo responsabile della protezione e della sicurezza dei dati, sulla provenienza dei dati e sugli scopi per i quali essi vengono regolarmente comunicati e descrive l'iter dell'assegnazione del diritto d'accesso ai prodotti dei sistemi elettronici d'informazione.

1.3 Scopo del trattamento di dati

Lo scopo della collezione di dati è in primo luogo disciplinato dalla Legge federale sull'assicurazione contro le malattie (LAMal), art. 84:

> *Gli organi incaricati di applicare la presente legge o la LVAMal, o di controllarne o sorvegliarne l'esecuzione possono trattare o far trattare dati personali, compresi dati degni di particolare protezione e profili della personalità, di cui necessitano per adempiere i compiti conferiti loro dalla presente legge o dalla LVAMal, segnatamente per:*
>
> *a) sorvegliare l'osservanza dell'obbligo di assicurarsi;*
>
> *b) calcolare e riscuotere i premi;*
>
> *c) stabilire il diritto alle prestazioni, nonché calcolarle, versarle e coordinarle con quelle di altre assicurazioni sociali;*
>
> *d) stabilire il diritto a una riduzione dei premi ai sensi dell'art. 65, nonché calcolare le riduzioni e versarle;*
>
> *e) far valere una pretesa di regresso nei confronti di terzi responsabili;*

f) sorvegliare l'esecuzione della presente legge;

g) allestire statistiche;

h) assegnare o verificare il numero d'assicurata/o dell'AVS;

Lo scopo della fondazione è la gestione di un'assicurazione d'indennità giornaliera a favore di artisti di arti plastiche e figurative in ragione della Legge federale sull'assicurazione contro le malattie (LAMal). La fondazione non mira a conseguire utili. Eventuali utili vengono reinvestiti. Il patrimonio può essere utilizzato esclusivamente a scopo dell'assicurazione d'indennità giornaliera e, all'occorrenza, dell'assicurazione contro gli infortuni in ragione dei regolamenti.

Pertanto, la collezione di dati serve a questo scopo.

1.4 Responsabile

La fondazione della Cassa d'indennità giornaliera per gli artisti è una pura assicurazione d'indennità giornaliera ai sensi dell'art. 1a cifra 1 in relazione con l'art 67 segg. LAMal. La fondazione, risp. i suoi organi, sono responsabili del trattamento e della gestione di dati (osservanza della protezione e della sicurezza dei dati). Proprietaria della collezione dei dati e dei sistemi informatici è la fondazione. Adottando le misure descritte, la fondazione provvede all'osservanza delle prescrizioni rilevanti.

La fondazione, risp. i suoi organi, è anche responsabile per la protezione e la sicurezza dei dati.

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

Tutte le collaboratrici e tutti i collaboratori o terzi coinvolti sottostanno all'obbligo del segreto ai sensi dell'art. 33 LPGA.

In caso di violazione dell'obbligo del segreto, in virtù di una legge specifica essi soggiacciono alle disposizioni penali previste dall'art. 92 LAMal. Unitamente al contratto di lavoro le collaboratrici e i collaboratori firmano l'obbligo di mantenere il segreto.

1.6 Esternalizzazione di servizi

L'intera gestione e contabilità della fondazione viene svolta da Swiss Life, che per analogia è tenuta ad attenersi alle misure definite nel presente regolamento.

Il contratto di esternalizzazione con Swiss Life recita in modo inequivocabile che quest'ultima è tenuta a trattare i dati analogamente a come la fondazione avrebbe il diritto di fare. In tal modo lo scopo è garantito. L'osservanza delle regole della fondazione è, pertanto, fissata contrattualmente.

Mediante controlli adeguati, gli organi della fondazione verificano regolarmente l'osservanza delle condizioni legate alla protezione dei dati.

È disciplinata la trasmissione dei dati tra fondazione e Swiss Life.

2. Collezione di dati

2.1 Struttura della collezione di dati

La collezione di dati della fondazione comprende i seguenti sistemi e contenuti:

- KUBIK, sistema di rilevamento della fondazione Cassa d'indennità giornaliera. Il sistema, impiegato unicamente per la fondazione Cassa d'indennità giornaliera, registra i seguenti dati per gli assicurati:

- nome, indirizzo, numero d'assicurata/o, data di nascita, sesso, data d'entrata, età di pensionamento (donna / uomo), sezione associazione artistica, luogo di pagamento e verifica se sussiste una riserva per l'ammissione

- sinistro, data di rilevamento, grado di malattia e durata, diritto alle prestazioni e data del versamento

- informazione di contabilizzazione per il sistema di contabilità SAP (informazioni sull'imputazione)

2.2 Interfacce

La fondazione riceve l'insieme dei dati personali esclusivamente dal contraente, risp. dal medico di fiducia di quest'ultimo. La verifica se il contraente è membro dell'associazione artistica "visarte", "SSAA" o "SSBA" avviene esclusivamente tra la fondazione Cassa d'indennità giornaliera e le associazioni artistiche.

Identificazione e autenticazione, tecnologie di criptaggio e di trasmissione all'avanguardia garantiscono la protezione dei dati e la rispettiva sicurezza dei dati.

3. Parti coinvolte

3.1 Fondazione

La fondazione Cassa d'indennità giornaliera per gli artisti è proprietaria della collezione di dati e dei dati.

3.2 Swiss Life

L'intera gestione e contabilità della fondazione viene svolta da Swiss Life, che, pertanto, tratta i dati della fondazione conformemente allo scopo e in modo confidenziale.

3.3 Ulteriori parti coinvolte

Non vi sono ulteriori persone coinvolte.

3.4 Application owner

Gli Information Owner e gli Application Owner Business e IT si occupano delle collezioni di dati presso la fondazione e Swiss Life nonché dell'osservanza delle disposizioni delle istruzioni rilevanti in materia di protezione e sicurezza dei dati.

4. Utenti e accesso ai dati

4.1 Utenti

Hanno accesso alla collezione di dati e ai dati della fondazione solo le persone indicate per nome che utilizzano i dati in questione nell'ambito del lavoro quotidiano (per il versamento o la verifica delle indennità giornaliere).

Inoltre, i system administrator o i responsabili dell'applicazione hanno accesso ai dati in base allo scopo.

Le collaboratrici e i collaboratori di società di servizi esterne non hanno accesso.

4.2 Gestione utenti

Per l'insieme di prodotti, applicazioni e collezioni di dati sussistono processi e iter documentati a livello di gestione degli utenti, autorizzazioni e ruoli, nonché dei rispettivi diritti d'accesso. Il responsabile del profilo d'autorizzazione competente si occupa del disbrigo della procedura d'autorizzazione, d'intesa con i responsabili della fondazione. La domanda relativa alla richiesta d'accesso viene esaminata dalle persone in questione e concretizzata da Service Help Desk.

La procedura relativa al diritto d'accesso viene, pertanto, monitorata dai responsabili della fondazione. Le persone autorizzate hanno accesso solo fintantoché ciò è indispensabile per il loro lavoro quotidiano. In caso di uscita o di cambio d'impiego esse perdono automaticamente il diritto d'accesso.

4.3 Formazione degli utenti

In materia di protezione e sicurezza dei dati gli utenti seguono regolarmente corsi di formazione e perfezionamento. Ciò concerne anche il settore specifico del trattamento dei dati della fondazione.

5. Trattamento dei dati; categorie di dati

5.1 Raccolta di dati

I dati provengono in prevalenza dai contraenti della stessa Cassa d'indennità giornaliera nonché dalle sue rappresentanze.

5.2 Categorie di dati

Nell'allegato 1 sono riportate le categorie di dati della fondazione.

5.3 Classificazione dei dati

I dati sono classificati come confidenziali. Tutte le misure sono adeguate al maggiore livello di protezione. Le regole di trattamento sono disciplinate da istruzioni; le collaboratrici e i collaboratori seguono regolarmente corsi.

5.4 Inoltro di dati

In merito alla comunicazione di dati, ai sensi dell'art. 84a LAMal vale quanto segue:

Purché nessun interesse privato preponderante vi si opponga, gli organi incaricati di applicare la presente legge o la LVAMal, nonché di controllarne o sorvegliarne l'esecuzione possono comunicare i dati, in deroga all'articolo 33 LPGA:

a) ad altri organi incaricati di applicare la presente legge o la LVAMal, nonché di controllarne o sorvegliarne l'esecuzione, qualora ne necessitino per adempiere i compiti conferiti loro dalla presente legge o dalla LVAMal;

b) agli organi di altre assicurazioni sociali, qualora, in deroga all'articolo 32 capoverso 2 LPGA, l'obbligo di comunicazione sia sancito da una legge federale;

bbis) agli organi di un'altra assicurazione sociale per assegnare o verificare il numero d'assicurato dell'AVS;

c) alle autorità competenti per l'imposta alla fonte, conformemente agli articoli 88 e 100 della legge federale del 14 dicembre 1990 sull'imposta federale diretta (LIFD), nonché alle rispettive disposizioni cantonali;

d) agli organi della statistica federale, conformemente alla legge federale del 9 ottobre 1992 sulla statistica federale;

e) agli organi incaricati di allestire statistiche per l'esecuzione della presente legge, qualora i dati siano necessari all'adempimento di tale obbligo e l'anonimato degli assicurati sia garantito;

f) alle competenti autorità cantonali, qualora i dati rientrino nel campo d'applicazione dell'articolo 22a e siano necessari per la pianificazione degli ospedali e delle case di cura e per l'esame delle tariffe;

g) alle autorità istruttorie penali, qualora ne necessitino per denunciare o impedire un crimine;

…

5 Negli altri casi, in deroga all'articolo 33 LPGA, i dati possono essere comunicati a terzi alle condizioni seguenti:

a) per i dati non personali: se la comunicazione è giustificata da un interesse preponderante;

b) per i dati personali: se, nel caso specifico, la persona interessata ha dato il suo consenso scritto o, qualora non sia possibile ottenerlo, le circostanze permettono di presumere che la comunicazione dei dati sia nell'interesse della persona assicurata.

I dati vengono comunicati per:

- l'esame dei diritti alle prestazioni
- la gestione del rapporto contrattuale
- la contabilità
- il coordinamento con le altre assicurazioni sociali in base all'esame delle richieste

Rientrano tra i destinatari dei dati:

- gli assicurati e le persone da loro autorizzate

- le autorità (p.es. ufficio AI)
- Swiss Life
- i medici di fiducia

L'ulteriore inoltro di dati è disciplinato nella LAMal.

6. Durata della conservazione dei dati e cancellazione

Sia la fondazione che Swiss Life soddisfano le prescrizioni legali in materia di archiviazione. La durata dell'archiviazione dopo la conclusione dell'affare si basa, pertanto, anch'essa sulle prescrizioni legali. Successivamente, i dati vengono cancellati ed eliminati.

7. Misure tecniche e organizzative

7.1 Controllo dell'accesso

L'accesso è protetto e regolamentato: l'insieme dei locali della fondazione e di terzi interessati, in cui vengono trattati dati personali, sono protetti elettronicamente o manualmente dall'accesso di persone non autorizzate (l'ufficio principale è chiuso a chiave durante l'orario non lavorativo). All'esterno il controllo è garantito da un badge e dal monitoraggio dell'accesso. Gli accessi vengono protocollati.

Hanno accesso ai locali in cui vengono trattati dati della fondazione unicamente le persone incaricate specificamente di questo compito (need to know / least privilege).

Zone protette determinano le misure di sicurezza: i posti di lavoro sono protetti dall'accesso di terzi non autorizzati e un sistema d'allarme è installato in tutti i locali.

Locali speciali – centro di calcolo e data warehouse – sono protetti come segue:

- Il centro di calcolo e tutti i data warehouse / data center / data server sono tutelati da elevati requisiti di sicurezza conformemente alla loro classe di sicurezza e danno accesso unicamente alle persone autorizzate specificamente per la gestione.
- L'accesso viene protocollato.
- Un sistema d'allarme è impostato sulla classe di sicurezza più elevata.
- I server si trovano in cantine a loro volta ubicate in specifici locali protetti.

7.2 Controllo di supporti di dati personali

Provvedimenti tecnico-informatici consentono l'accesso esclusivamente alle persone autorizzate a trattare dati sui supporti di dati elettronici. Solo le persone autorizzate possono accedere alle collezioni di dati e ai sistemi informatici della fondazione o di Swiss Life. Inoltre, tutti i dati vanno messi al sicuro ed eliminati secondo la procedura prevista. In tal modo si evita che i dati personali della fondazione vengano letti, copiati, modificati o rimossi da persone non autorizzate.

L'organizzazione interna della fondazione o di terzi coinvolti allestisce i rispettivi profili di accesso e i diritti per le collaboratrici e i collaboratori e li controlla regolarmente.

All'avvio del sistema / notebook, la collaboratrice / il collaboratore deve identificarsi e autenticarsi. L'operazione viene protocollata.

7.3 Controllo degli utenti; identificazione e autenticazione

Diritti di accesso che dipendono dai ruoli, l'autenticazione e l'identificazione, firewall e un accesso a distanza ben definito garantiscono che abbiano accesso ai dati della fondazione unicamente le persone autorizzate.

L'identificazione di una persona e la rispettiva autenticazione vengono garantite dalle seguenti misure:

- L'accesso ai sistemi della fondazione o di Swiss Life è protetto dall'ID utente in combinazione con una password adeguatamente solida, individuale e limitata nel tempo. L'accesso ad alcuni sistemi è possibile unicamente tramite utilizzo di una password supplementare.

- La gestione di password è inoltre disciplinata da istruzioni specifiche a parte ed è oggetto di controlli regolari.

- Tutti gli account di utenti che permettono un'autenticazione sono individuali. Un account utente corrisponde a un'unica persona.

- Tutti i dischi rigidi delle collaboratrici e dei collaboratori sono inoltre tutelati da password.

- Le password devono essere solide e vanno cambiate regolarmente (ogni tre mesi).

7.4 Controllo della comunicazione

I destinatari di dati ai quali vengono comunicati dati personali mediante sistemi per l'inoltro di dati vengono identificati attraverso l'interfaccia e autenticati adeguatamente. Inoltre, i dati vengono, di regola, inviati generalmente per lettera, agli uffici definiti alla cifra 5.4.

7.5 Controllo della conservazione

Mediante diritti d'accesso basati su ruoli nonché la separazione di test, sviluppo e produzione è garantita la protezione dalla consultazione, la modifica o la cancellazione non autorizzata di dati memorizzati. La protezione da malware e dall'accesso non autorizzato dall'esterno è garantita da antivirus e firewall.

I dati vengono archiviati in forma adeguata alle esigenze della revisione.

7.6 Requisiti tecnici dei terminali

Non vengono impiegati terminali che trattano dati degli utenti.

7.7 Controllo dell'accesso

È garantito che abbiano accesso ai dati della fondazione solo le persone che necessitano dei dati nell'espletamento del lavoro quotidiano e nell'esercizio dello scopo della fondazione.

7.8 Controllo delle immissioni; messa a verbale

Tutti i sistemi dispongono di un trattamento protocollato, incl. l'accesso ai dati. Ciò serve sia alla tutela dell'integrità che alla verifica dello scopo dei dati. La messa a verbale viene, pertanto, effettuata in applicazione dell'art 10 OLPD. I verbali vengono custoditi durante un determinato lasso di tempo secondo la procedura prevista e sono accessibili unicamente per le persone a cui compete il monitoraggio e il controllo delle prescrizioni in materia di protezione dei dati e sono anch'essi conformi allo scopo.

7.9 Sviluppo del programma

Viene osservata la separazione tra sviluppo, test e produzione.

7.10 Vigilanza e responsabilità

Gli Information Owner, insieme ai responsabili dell'applicazione, vegliano affinché le persone si attengano alle istruzioni, al presente regolamento per il trattamento e alle prescrizioni.

7.11 Visitatori nell'edificio della fondazione o di terzi coinvolti

In caso di visitatori, l'accesso è regolamentato dimodoché essi non possano trattenersi nell'edifico da soli, bensì solo in compagnia e previo annuncio. Al momento di annunciarsi i dati personali vengono controllati mediante un certificato d'identità che viene trattenuto in deposito durante la visita.

7.12 Sicurezza del posto di lavoro

La sicurezza della postazione di lavoro delle collaboratrici e dei collaboratori è tutelata dalle seguenti misure:

- Le postazioni di lavoro sono impostate in modo tale che gli schermi non siano visibili dalla porta.
- Le collaboratrici e i collaboratori seguono regolarmente corsi di formazione e sono chiamati a non lasciare documenti incustoditi nella stampante.
- Per tutte le postazioni di lavoro vige la Clear Desk Policy (Istruzioni Clear Desk / Posto di lavoro ordinato), in base alla quale occorre tenere sotto chiave tutti i documenti.
- In tutte postazioni di lavoro i notebook sono protetti da accesso non autorizzato.
- I notebook sono protetti con firewall e programmi antivirus all'avanguardia, regolarmente aggiornati.

7.13 Accesso all'esterno dell'organizzazione

I dati della fondazione sono accessibili unicamente all'interno dell'organizzazione o da parte di terzi interessati. Nel trattamento dei dati della fondazione non vengono inoltre impiegati supporti dati esterni.

7.14 Protezione a lungo termine dei dati

Le misure di sicurezza definite devono essere garantite per l'intera durata del ciclo vitale. A tale scopo subentrano le seguenti misure:

- I dati vengono registrati esclusivamente da persone autorizzate, istruite in merito.
- Ove possibile, nel corso di un test vengono utilizzati solo dati fittizi o anonimizzati.
- La registrazione, modifica, cancellazione e l'accesso ai dati vengono protocollati. Si tratta di una procedura specificata con esclusivi scopi di sicurezza definiti che segue criteri chiari. I diritti d'accesso ai verbali sono chiaramente definiti (need to know) e conformi allo scopo. I verbali sono dotati dei medesimi meccanismi di protezione analogamente ai dati (protezione dall'accesso di terzi non autorizzati e da cambiamenti).
- Contenuto e durata della conservazione dei rispettivi logfile sono rapportati ai dati e alle misure di trattamento.
- L'archiviazione a lungo termine dei dati corrisponde alle prescrizioni del Codice delle obbligazioni e dell'Olc. Cancellazione ed eliminazione dei dati sono disciplinate da istruzioni specifiche.

7.15 Controllo del trasporto; trasmissione di dati

La trasmissione di dati avviene mediante TLS o connessione VPN. Di regola, i dati non vengono inviati per e-mail bensì per lettera alle persone interessate.

8. Diritti delle persone interessate

8.1 Diritto d'accesso

Ogni persona ha il diritto di richiedere informazioni dalla fondazione o da Swiss Life per sapere se dati che la concernono sono trattati. Pertanto, il diritto d'accesso si basa sulle prescrizioni della LPD. Le richieste vanno indirizzate alla fondazione o a Swiss Life allegando copia di un documento d'identità ufficiale.

La procedura è descritta nelle istruzioni Protezione dei dati SLCH 8.13.

8.2 Obbligo di informare nel caso di dati personali degni di particolare protezione

Ai sensi della LPD, se vengono raccolti dati personali degni di particolare protezione o profili della personalità, occorre informarne le persone interessate.

In linea di principio, i dati personali degni di particolare protezione vengono raccolti unicamente previo consenso delle persone interessate. In tutti gli altri casi, ai sensi dell'art. 12 cpv. 2 lettera c in relazione con l'art. 13 LPD, deve sussistere una causa di giustificazione per un interesse preponderante privato o pubblico o per legge. **Diritti di rettifica e di cancellazione**

I diritti di rettifica e di cancellazione delle persone interessate poggiano sull'art. 5 cpv. 2 LPD; le richieste vanno indirizzate alla fondazione.

9. Disposizioni conclusive

9.1 Allegati

Gli allegati menzionati nel presente regolamento per il trattamento sono parte integrante del regolamento. Il regolamento per il trattamento viene gestito e custodito presso il responsabile della protezione dei dati di Swiss Life.

9.2 Modifiche del presente regolamento

Il regolamento viene sottoposto a verifiche regolari concernenti l'attualità e, all'occorrenza, adeguato. Le modifiche necessitano della forma scritta e dell'approvazione della fondazione. L'aggiornamento compete alla fondazione.

9.3 Entrata in vigore

Il presente regolamento, revisionato l'ultima volta al 1° agosto 2016, entra in vigore fin da subito unitamente a tutti i suoi allegati.

Zurigo, 1° agosto 2016

Fondazione Cassa d'indennità giornaliera per gli artisti

Presidente

Dr. Stephan P. Thaler

Tesoriere

Adrian Steinmann

Allegato 1: Categorie di dati

Categorie dei dati personali trattati nella collezione di dati:

Appellativo
Nome
Cognome
Ditta
Numero d'assicurata/o (AVS)
Indirizzo 1
Indirizzo 2
NPA
Località
Paese
Telefono
Telefax
E-mail
Sesso
Lingua
Numero di partner (numero d'assicurata/o)
Data di nascita
Data d'entrata
Data d'uscita
Età di pensionamento (calcolata)
Deceduta/o (sì / no)
Sezione
Genere artistico
Recapito per i pagamenti: istituto finanziario, numero di conto
Riserva all'ammissione (sì / no)
Numero di sinistro (generato dal sistema)
Data di notifica
Periodo da - a
Descrizione
Tipo (malattia / infortunio / maternità)
Caso concluso (sì / no)
Caso di prestazione in corso di pagamento da (data) a (data)
Termine di carenza
Grado (percentuale)
Tasso d'indennità giornaliera (a titolo informativo)
Indennità giornaliera CHF (a titolo informativo)
Importo totale in CHF
Indennità giornaliera versata in data
Conto dare (informazione sull'imputazione per contabilità SAP)
Conto avere (informazione sull'imputazione per contabilità SAP)