Helsana

Regolamento per il trattamento dei dati del gruppo Helsana

1. Scopo del regolamento per il trattamento dei dati

Il regolamento per il trattamento dei dati assicura la necessaria trasparenza sia per lo sviluppo dei sistemi sia per il trattamento dei dati. Viene redatto nella forma più concisa e comprensibile possibile, così da permettere anche ai «non esperti» di comprendere e giudicare lo sviluppo del sistema e il trattamento dei dati. Il principio «quanto serve e il meno possibile» deve essere assunto nel regolamento.

Il presente regolamento per il trattamento stabilisce i principi di trattamento dei dati per tutte le attività di raccolta di dati delle società d'assicurazione del gruppo Helsana (di seguito anche «**Helsana**», «**noi**» o «**ci**»). Fanno parte delle società d'assicurazione del gruppo Helsana: Helsana Assicurazioni SA, Helsana Assicurazioni integrative SA e Helsana Infortuni SA.

2. Trattamenti dei dati e procedimenti

2.1 Struttura

Il trattamento dei dati di Helsana è strutturato nelle seguenti attività:

- Sviluppo dell'offerta per Clienti privati (IG)
- Audit, Risk, Legal & Compliance
- Management della sicurezza dei dati
- Facility management
- Scienze della sanità pubblica
- Management HR
- Incasso ed esborso, finanze, attuariato
- Management IT
- Servizio clienti IG
- Servizio clienti affari con i clienti aziendali (UG)
- Acquisto di prestazioni IG
- Management delle prestazioni IG
- Management delle prestazioni UG
- Nuovi affari IG e UG
- Assicurazione del personale IG e UG
- Fondazione per la previdenza del personale
- Servizio medico fiduciario (SMF)
- Gestione dei contratti IG
- Management dei canali di vendita IG
- Management dei canali di vendita UG
- Supporto alla vendita IG

Diverse interfacce consentono il contatto diretto con prestatori di servizi e fornitori di prestazioni esterni, ad es. per il conteggio diretto del fornitore di prestazioni con Helsana. Esiste inoltre un'interfaccia con la quale determinati fornitori di prestazioni possono verificare online la copertura assicurativa della persona assicurata. La protezione dei dati e la relativa sicurezza vengono garantite attraverso un'efficace procedura di autenticazione nonché con moderne tecnologie di cifratura e trasmissione.

2.2 Procedure di trattamento dei dati

Helsana stabilisce in regolamenti interni le modalità di inventario e di controllo della legalità nel trattamento dei dati (compliance check). Le procedure per la memorizzazione, la comunicazione a terzi, la conservazione, l'archiviazione, la pseudonimizzazione, l'anonimizzazione, la cancellazione o la distruzione dei dati sono definite nei rispettivi piani di protezione dei dati per ogni trattamento dei dati.

2.3 Utilizzo e accesso ai dati

2.3.1 Persone autorizzate all'accesso

Hanno diritto di accesso ai sistemi IT di Helsana:

- il personale di Helsana, se ciò è necessario per svolgere il proprio incarico «Gestione dell'assicurazione malattia»;
- gli amministratori di sistema di Helsana;
- i prestatori di servizi cui sia stato conferito un mandato contrattuale

(denominati collettivamente persone autorizzate all'accesso).

2.3.2 Gestione delle persone autorizzate all'accesso

La gestione delle persone autorizzate all'accesso si svolge in modo centralizzato tramite l'Identity & Access Management di Helsana. Le collaboratrici e i collaboratori interni ed esterni vengono registrati attraverso l'interfaccia HR. Nuove identità, account compresi, vengono registrate soltanto se esiste un contratto di lavoro o di servizio valido e i relativi diritti sono stati autorizzati dal superiore gerarchico.

2.3.3 Autorizzazione personale di accesso

Al momento dell'ingresso in Helsana, tutte le persone autorizzate all'accesso ricevono i diritti di accesso alle informazioni secondo il modello dei ruoli, in base alla rispettiva funzione e alla loro appartenenza organizzativa. Tutti gli altri diritti devono essere richiesti personalmente mediante il portale delle autorizzazioni. A tal fine è necessario che ogni richiesta venga confermata dal superiore diretto e anche, secondo il ruolo di autorizzazione, dalla persona che approva il ruolo.

2.3.4 Revoca dell'autorizzazione di accesso

L'autorizzazione di accesso ai sistemi IT di Helsana è valida soltanto finché la collaboratrice o il collaboratore in questione necessita dei dati per svolgere la propria funzione lavorativa. Se la collaboratrice o il collaboratore lascia l'azienda o assume nuove mansioni all'interno di Helsana, l'autorizzazione di accesso viene revocata e le autorizzazioni di accesso necessarie per lo svolgimento delle nuove mansioni vengono assegnate mediante il modello dei ruoli.

2.3.5 Formazione delle persone autorizzate all'accesso

Le persone autorizzate all'accesso seguono corsi di formazione per i diversi sottosistemi e applicazioni.

2.3.6 Manuali e direttive sul trattamento dei dati per le persone autorizzate all'accesso

Per i sottosistemi sono disponibili apposite documentazioni. Il trattamento dei dati viene definito inoltre nelle direttive, nei regolamenti e nei manuali sulle prestazioni nonché nelle liste. Questi documenti vengono aggiornati regolarmente dalle unità organizzative competenti.

Le unità organizzative competenti creano, mediante istruzioni specifiche, un livello di valutazione delle prestazioni secondo la legge federale sull'assicurazione malattie (LAMal) uniforme per tutto il territorio assicurativo della Svizzera.

2.3.7 Prestatori di servizi informatici

Se la gestione dei sistemi IT di Helsana viene esternalizzata a prestatori esterni di servizi informatici, questi si attengono a regole analoghe nel proprio ambito.

3. Diritto all'informazione, alla rettifica e alla divulgazione dei dati

Ai sensi dell'art. 25 della legge federale sulla protezione dei dati (LPD), le persone interessate possono chiedere al titolare informazioni sull'eventuale trattamento di dati personali che le riguardano e possono richiedere la consegna di tali dati. Hanno inoltre il diritto di far correggere i propri dati da Helsana.

4. Misure tecniche e organizzative a garanzia della sicurezza dei dati

4.1 Controllo dell'accesso

Tutti i locali di Helsana in cui vengono trattati dati personali che meritano una protezione specifica sono protetti mediante un sistema elettronico o manuale dall'accesso di persone non autorizzate. I responsabili redigono un verbale sulla gestione delle chiavi e sul controllo elettronico degli accessi. L'incaricato della sicurezza fisica può richiederne la visione o le valutazioni in qualsiasi momento. Le zone protette determinano le misure di sicurezza da attuare: le postazioni di lavoro sono protette dall'accesso di terzi non autorizzati. I locali speciali e quelli sensibili, come le sale impianti e i centri di calcolo, sono protetti nel modo seguente:

- i sistemi IT nei centri di calcolo e i server decentralizzati gestiti dall'IT di Helsana sono protetti applicando maggiori requisiti di sicurezza fisica, affinché l'accesso venga consentito esclusivamente a persone appositamente autorizzate;
- i sistemi IT nei server decentralizzati non gestiti dall'IT di Helsana sono protetti con misure di sicurezza paragonabili a quelle dei server e dei computer da essa gestiti.

Le precauzioni informatiche garantiscono che solo le persone autorizzate possano elaborare i dati. Solo le persone autorizzate hanno accesso ai sistemi IT di Helsana.

4.2 Autenticazione delle persone autorizzate all'accesso

L'accesso ai sistemi IT di Helsana viene protetto dall'ID utente combinato con una funzione di autorizzazione individuale limitata nel tempo.

4.3 Controllo della comunicazione dei dati

I destinatari a cui vengono comunicati dati personali attraverso dispositivi di trasmissione vengono identificati mediante le interfacce (ad es. consultazioni online della copertura effettuate dai fornitori di prestazioni attraverso l'uso della tessera di assicurato).

4.4 Trasmissione dei dati

La trasmissione dei dati è protetta da procedure di crittografia.

4.5 Controllo dell'archiviazione

Le persone autorizzate all'accesso ricevono autorizzazioni specifiche per le modifiche dei campi di dati di cui hanno bisogno per svolgere i loro compiti (ad es. in conformità alla LAMal o alla legge federale sull'assicurazione contro gli infortuni [LAINF]).

4.6 Requisiti tecnici dei terminali

L'accesso alla rete interna di Helsana è limitato, protetto e monitorato mediante misure di controllo specifiche. Le reti dei prestatori esterni di servizi informatici sono protette in modo analogo.

4.7 Misure per la protezione dei dati (riservatezza) concernenti i terminali

Tutti i dispositivi terminali di dati (client) sono protetti da attacchi con molteplici misure tecniche di sicurezza.

I dati stampati vengono conservati in modo che terze persone (ad es. gli addetti alle pulizie) non possano prenderne visione né copiarli. In applicazione di una direttiva interna, questi dati vengono conservati in contenitori chiusi a chiave o smaltiti tramite un distruggidocumenti o Datarec. Vale il principio del clean desk e del clear screen.

4.8 Verbalizzazione

Oltre al controllo degli accessi ai sistemi IT di Helsana mediante la procedura di autorizzazione e la protezione attraverso l'ID utente personale e l'autorizzazione, i singoli sistemi IT dispongono di una verbalizzazione del trattamento automatizzato, in modo da poter verificare a posteriori se il trattamento dei dati sia avvenuto in conformità alle finalità per cui tali dati sono stati raccolti o comunicati. La verbalizzazione avviene in applicazione dell'art. 4 dell'ordinanza sulla protezione dei dati (OPDa): i verbali vengono conservati per 13 mesi in una forma che sia adeguata a un'eventuale revisione. Sono accessibili solo agli organi e alle persone incaricati di verificare l'applicazione delle disposizioni per la protezione dei dati o di mantenere o ripristinare la riservatezza, l'integrità, la disponibilità e la tracciabilità dei dati e possono essere utilizzati soltanto a tale scopo. Nel caso dei prestatori esterni di servizi informatici, per la verbalizzazione vigono regole in parte simili a quelle menzionate, ma proprie.

4.9 Sviluppo

Le richieste di ulteriore sviluppo del sistema vengono raggruppate e definite, preventivate e realizzate come intervento di manutenzione o progetto. Il procedimento e la governance sono disciplinati nell'ambito della «procedura progettuale Helsana».

4.10 Assistenza per le persone autorizzate all'accesso e obbligo di notifica

Per quanto concerne gli aspetti specialistici, le persone autorizzate all'accesso ricevono supporto dalle gestioni specialistiche dei rispettivi settori. Il supporto tecnico per i sistemi IT e la rete viene prestato dall'IT di Helsana o commissionato.

Le persone autorizzate all'accesso sono informate sulla necessità di proteggere il sistema IT di Helsana e sulle disposizioni concernenti l'uso del sistema IT e dei suoi dati. Le disposizioni sono descritte in direttive e promemoria per la sensibilizzazione sulla sicurezza dell'informazione. Le persone autorizzate all'accesso sono a conoscenza delle possibili sanzioni in caso di violazioni della sicurezza dell'informazione commesse intenzionalmente o per negligenza.

Ogni violazione deve essere notificata immediatamente al superiore secondo la procedura degli incidenti concernenti la sicurezza o all'Ufficio denunce in conformità al codice di condotta.

4.11 Vigilanza e responsabilità

Le persone responsabili dei sistemi IT e delle applicazioni controllano che le persone autorizzate all'accesso si attengano alle direttive e al presente regolamento per il trattamento dei dati e i prestatori esterni di servizi informatici alle loro disposizioni contrattuali.

5. Versione

Il presente regolamento per il trattamento dei dati non fa parte di un contratto con gli assicurati o con altri terzi. Pertanto, possiamo modificarlo in qualsiasi momento. La versione pubblicata su questo sito web è sempre la versione aggiornata.

Ultimo aggiornamento: **settembre 2023**