

Dichiarazione sulla protezione dei dati e Regolamento per il trattamento concernenti le assicurazioni infortuni di Helsana

Versione 2.0 del 03.09.2019

1. Breve panoramica

In conformità alla Legge federale sull'assicurazione contro gli infortuni (**LAINF**), i lavoratori devono essere obbligatoriamente assicurati contro gli infortuni attraverso il proprio datore di lavoro. I lavoratori indipendenti possono assicurarsi facoltativamente contro gli infortuni secondo la LAINF. L'assicurazione obbligatoria contro gli infortuni corrisponde prestazioni assicurative in caso di infortuni professionali e, a partire da un orario di lavoro settimanale superiore alle otto ore, anche in caso di infortuni non professionali e di malattie professionali. Tale assicurazione copre le spese di cura, indennità giornaliera, rendite, indennità per menomazione dell'integrità e assegni per grandi invalidi.

Le prestazioni temporanee e permanenti dell'assicurazione obbligatoria contro gli infortuni possono essere integrate con un'assicurazione complementare contro gli infortuni. È possibile quindi assicurare, ad esempio, salari più alti rispetto all'importo massimo obbligatorio del salario assicurato, come anche aumentare il comfort in ospedale passando dal reparto comune a quello semiprivato o privato.

Alla stregua di altri assicuratori infortuni privati, delle casse pubbliche d'assicurazione contro gli infortuni e della SUVA, Helsana Infortuni SA è autorizzata a gestire l'assicurazione obbligatoria contro gli infortuni conformemente a quanto previsto dalla LAINF. Helsana Infortuni SA offre, inoltre, un'assicurazione integrativa infortuni conformemente alla Legge federale sul contratto d'assicurazione (**LCA**). Le assicurazioni infortuni secondo la LAINF e la LCA possono essere integrate da un'assicurazione di capitale di Solida Assicurazioni SA (entrambe collettivamente **Helsana**) in caso di decesso e invalidità in seguito a infortunio.

Helsana tratta dati personali nell'ambito della gestione dell'assicurazione infortuni, segnatamente del calcolo dei premi, della valutazione delle prestazioni o del regresso nei confronti di terzi responsabili. Per «dati personali» si intendono tutte le informazioni che si riferiscono a una persona (fisica) determinata o determinabile. Da un lato, Helsana tratta dati di clienti privati assicurati presso Helsana e che comunicano da sé a quest'ultima i propri dati personali. Dall'altro, Helsana tratta anche i dati dei lavoratori di clienti aziendali che trasmettono i dati da sé o attraverso il loro datore di lavoro nell'ambito della notifica e del disbrigo di un infortunio. Tali dati personali comprendono, ad esempio, informazioni di contatto, come nome, indirizzo o numero di telefono. Per adempiere il proprio mandato previsto per legge o contrattuale, Helsana necessita anche di ulteriori dati personali, come data di nascita, numero AVS o di assicurato, nonché informazioni sullo stato di salute delle persone.

Dato che per Helsana è molto importante tutelare questi dati particolarmente degni di protezione, la presente Dichiarazione sulla protezione dei dati fornisce informazioni su:

- chi è responsabile del trattamento dei dati;
- quali dati di quali persone vengono raccolti e trattati;
- come e da chi sono raccolti e trattati i dati;
- per quale scopo e su quale base legale vengono trattati i dati;
- a chi vengono comunicati i dati;
- per quanto tempo vengono conservati i dati;
- quali sono i diritti delle persone interessate.

2. Applicabilità della Dichiarazione sulla protezione dei dati

La presente Dichiarazione sulla protezione dei dati spiega come sono raccolti e successivamente trattati i dati personali da parte di Helsana in relazione alle assicurazioni infortunio. Allo stesso tempo, essa funge da regolamento sul trattamento dei dati ai sensi degli artt. 11 e 21 dell'Ordinanza relativa alla legge federale sulla protezione dei dati (**OLPD**) in combinato disposto con gli artt. da 96 a 98 LAINF.

Resta riservato il diritto di raccogliere e trattare successivamente i dati personali contemplati da altre dichiarazioni sulla protezione dei dati o condizioni di utilizzo, derivanti dalle circostanze o disciplinati a norma di legge.

3. Titolare del trattamento, responsabile della protezione dei dati

Per la raccolta e il successivo trattamento di dati personali in relazione alla gestione delle assicurazioni infortuni, la società di Helsana interessata è il titolare del trattamento (in particolare ai sensi dell'art. 4 cpv. 7 del Regolamento generale sulla protezione dei dati dell'Unione europea [**RGPD**] e della legge federale sulla protezione dei dati, come pure di eventuali altre disposizioni applicabili nel caso concreto).

Eventuali richieste, pretese o informazioni nell'ambito della legislazione sulla protezione dei dati concernenti Helsana possono essere indirizzate, allegando la copia di un documento di identità, al responsabile di Helsana della protezione dei dati all'indirizzo seguente:

Helsana Infortuni SA
Responsabile della protezione dei dati
Casella postale
8081 Zurigo

4. Raccolta, trattamento e utilizzo di dati personali

4.1 Interessati

Helsana raccoglie e tratta i dati personali di

- persone che sono o erano assicurate – nel caso dei lavoratori attraverso il loro datore di lavoro – presso Helsana o un altro assicuratore malattia del gruppo Helsana;
- persone i cui datori di lavoro vengono assegnati a Helsana dalla cassa suppletiva al fine di assolvere l'obbligo di assicurazione (cfr. art. 73 cpv. 2 LAINF);
- partecipanti ai concorsi, alle ricerche di mercato, ai sondaggi di opinione o sul grado di soddisfazione condotti da Helsana;
- persone potenzialmente o effettivamente interessate ai prodotti e servizi di Helsana.

(Detti collettivamente **clienti**).

Inoltre, Helsana raccoglie e tratta i dati di fornitori di prestazioni, medici consulenti, prestatori di servizi, partner di vendita e altri partner di affari di Helsana come pure dei loro collaboratori e contatti (**partner**).

Helsana tratta segnatamente le categorie di dati personali dei clienti riportate di seguito.

- **Dati personali e informazioni di contatto:** rientrano in questa categoria in particolare, ma non esclusivamente, nome e cognome, sesso, data di nascita, età, stato civile, numero AVS e numero di assicurato, lingue, nazionalità, attinenza cantonale e comunale, indirizzo (e-mail), numero di telefono, dati concernenti la salute (ad es. dichiarazione sullo stato di salute), familiari, ecc.
- **Dati in relazione alla comunicazione:** rientrano in questa categoria informazioni come canale di comunicazione preferito, corrispondenza e comunicazione con Helsana per lettera, e-mail, telefono o altre modalità (comprese le registrazioni della comunicazione), soddisfazione del cliente, ecc.
- **Dati contrattuali:** tipo di assicurazione e copertura, tipo ed estensione delle prestazioni, data di entrata e di uscita.
- **Dati in relazione al disbrigo delle prestazioni:** rientrano in questa categoria, fra l'altro, fornitori di prestazioni, diagnosi, rapporti medici, informazioni dei medici consulenti, costi delle prestazioni, relazioni bancarie e postali, pagamenti, dati di assicuratori terzi, informazioni in relazione a richieste di chiarimenti, fatture del fornitore di prestazioni.
- **Dati in relazione al calcolo e alla riscossione dei premi:** rientrano in questa categoria segnatamente i premi assicurativi, la fatturazione dei premi, i dati relativi a procedure di incasso, le informazioni sulla solvibilità, ecc.
- **Dati in relazione a controversie legali:** rientrano in questa categoria in particolare i dati concernenti ricorsi e divergenze sulle prestazioni o sui relativi contratti, come per esempio regressi e controversie, nonché i dati relativi agli atti di procedure giudiziarie e amministrative, ecc.
- **Dati in relazione al marketing di prodotti e servizi:** rientrano in questa categoria informazioni come documentazioni ricevute, attività speciali, newsletter, preferenze e interessi personali, ecc.

- **Dati in relazione al case management:** informazioni su salute, datore e rapporto di lavoro, circostanze mediche, sociali e specifiche del posto di lavoro e relativo bisogno di sostegno, ecc.

(Detti collettivamente **dati del cliente**).

Inoltre, Helsana tratta segnatamente le seguenti categorie di dati personali dei partner:

- **Dati di fornitori di prestazioni, prestatori di servizi e altri partner di affari nonché informazioni sui loro collaboratori e contatti**, in particolare dati di contatto, informazioni sulla funzione, sui rapporti avuti con tali persone, informazioni su attività di marketing (ad es. ricevimento di newsletter), informazioni su operazioni commerciali, richieste, offerte, proposte, condizioni e contratti (in particolare in relazione a convenzioni tariffali), informazioni su formazioni e attività professionale, ecc. (**dati dei partner**).

Nel quadro della loro relazione di affari i clienti dovranno mettere a disposizione i dati necessari o prescritti a norma di legge per allacciare e gestire il rapporto contrattuale e per adempiere i relativi obblighi contrattuali. In linea di principio, senza tali dati Helsana non sarà in grado di stipulare né eseguire il contratto con il cliente in questione. Questo vale per analogia anche per i dati dei partner, nella misura in cui si tratti di rapporti di affari con prestatori di servizi, fornitori e partner di affari di Helsana; in linea di principio, tali rapporti non possono essere allacciati né gestiti senza informazioni sui loro collaboratori e altri contatti.

4.2 Fonti dei dati

I dati personali vengono raccolti in primo luogo mediante la comunicazione diretta con i clienti (lettere, formulari di contatto e di proposta, e-mail, telefono, utilizzo di pagine Internet o in altro modo).

Tuttavia, i dati personali possono essere raccolti anche indirettamente, in particolare tramite

- persone e uffici autorizzati dai clienti (segnatamente il datore di lavoro);
- altri assicuratori conformemente all'art. 68 cpv. 1 LAINF al di fuori del gruppo Helsana (ad es. società assicurative private, casse pubbliche d'assicurazione contro gli infortuni e casse malati), le casse suppletive e la SUVA (art. 97 LAINF);
- medici consulenti;
- lo scambio di informazioni nel quadro dell'assistenza giudiziaria e amministrativa (art. 32 della legge federale sulla parte generale del diritto delle assicurazioni sociali [LPGA] e art. 98 LAINF);
- fonti di pubblico dominio (ad es. Internet, stampa, media, registri);

e nell'ambito dei clienti aziendali attraverso

- l'acquisto di informazioni complementari da fonti di dati di terzi (ad es. commercianti di indirizzi).

4.3 Responsabile del trattamento dei dati e uffici coinvolti

L'assicurazione infortuni è gestita in primo luogo dai collaboratori dei servizi clienti regionali e delle agenzie generali/dei punti vendita di Helsana. Per adempiere a tale compito, essi trattano i dati personali, compresi quelli degni di particolare protezione contenuti nella raccolta di dati di Helsana (cfr. punto 9).

Per la gestione dell'assicurazione infortuni, nel quadro delle attività di trattamento dei dati (le **attività dati**) descritte qui di seguito i collaboratori hanno accesso ai dati necessari per svolgere il proprio compito specifico:

- gestione dei canali di vendita e sostegno alle vendite;
- sviluppo dell'offerta;
- attività con nuovi clienti;
- servizio clienti;
- amministrazione contratti;
- management delle prestazioni;
- acquisto prestazioni;
- assicurazione del personale;
- medici consulenti;
- scienze della salute;
- incasso, finanze, attuariato;
- audit, risk, legal e compliance;
- management IT e gestione sicurezza dati;
- Fondazione per la previdenza del personale (segnatamente in caso di situazioni di sovrinden-
- acquisti.

A garantire il rispetto delle disposizioni delle direttive e dei regolamenti per il trattamento dei dati in relazione alle attività dati presso Helsana sono i cosiddetti process owner. Questi devono garantire che tutti i dati della loro applicazione vengano messi a disposizione solo nell'ambito definito dalla legge.

4.4 Decisioni singole automatizzate

Nel quadro della liquidazione delle prestazioni vengono prese da Helsana decisioni singole automatizzate. Se clienti o fornitori di prestazioni presentano a Helsana una fattura, la verifica se la prestazione ricevuta viene considerata infortunio (art. 10 e segg. LAINF e art. 9 e segg. OAINF) e quindi anche la decisione se sussista il diritto alla prestazione avvengono in modo automatizzato. In tal caso non viene effettuata alcuna profilazione, dato che solo le fatture vengono controllate in base ai dati di contratti e alle tariffe. Se in relazione a una procedura di incasso è stato avviato un procedimento d'esecuzione, gli ulteriori passi (domanda di continuazione dell'esecuzione, domanda di fallimento, domanda di realizzazione, ecc.) sono automatizzati, in quanto questi vengono attivati allo spirare del termine corrispondente qualora il debito non sia ancora stato pagato. Tali decisioni singole automatizzate vengono prese perché sono necessarie ai fini dell'adempimento del contratto di assicurazione fra il cliente ed Helsana ed esistono misure adeguate per tutelare i diritti e i legittimi interessi delle persone interessate (cfr. punto 11).

5. Scopo e basi legali del trattamento dei dati

5.1 Dati dei clienti

I dati dei clienti vengono raccolti innanzitutto ai fini dell'ordinaria esecuzione dell'assicurazione infortuni conformemente ai seguenti scopi di legge (art. 96 LAINF):

- sorvegliare l'osservanza dell'obbligo di assicurarsi;
- calcolare e riscuotere i premi;
- stabilire il diritto alle prestazioni, nonché calcolare, versare e coordinare le prestazioni con quelle di altre assicurazioni sociali;
- far valere una pretesa di regresso nei confronti di terzi responsabili;
- allestire statistiche;
- assegnare o verificare il numero di assicurato dell'assicurazione vecchiaia e superstiti;
- effettuare comunicazioni dei dati a terzi ai sensi degli artt. 97 e 98 LAINF.

Inoltre, i trattamenti dei dati servono in particolare e nella misura ammessa dalla legge (anche) agli scopi seguenti:

- tutela di clienti, collaboratori e altre persone specialmente in caso di minacce concernenti i collaboratori, protezione dei dati, dei segreti e dei valori patrimoniali affidati a Helsana, nonché sicurezza dei sistemi e degli edifici di Helsana;
- in relazione ai servizi offerti, alla stipulazione e all'esecuzione di contratti, alla cura e allo sviluppo delle relazioni con i clienti, alla comunicazione, al servizio e al supporto clienti, a promozioni, pubblicità e marketing (compresi la newsletter e l'invio di materiale pubblicitario);
- amministrazione, esercizio e perfezionamento del sito Internet (compresa la messa a disposizione di funzionalità che presuppongono identificatori o altri dati personali) e di ulteriori sistemi IT, controlli di identità.
- rispetto dei criteri legali e normativi nonché delle regole interne di Helsana, esercizio e messa in atto di vari diritti, difesa da pretese legali, processi civili, ricorsi, lotta agli abusi, per scopi concernenti inchieste o procedimenti legali e per rispondere alle richieste di informazioni da parte delle autorità;
- vendita o acquisto di settori aziendali, società o parti di società e altre operazioni di diritto societario con il relativo trasferimento di dati dei clienti;
- per altri scopi, se un obbligo legale richiede il trattamento o al momento della raccolta dei dati tali scopi erano riconoscibili od opportuni in considerazione delle circostanze;

e nell'ambito dei clienti aziendali anche per

- controllo di qualità, ricerca di mercato, perfezionamento di prodotti e servizi, allestimento di statistiche, preventivi, registrazioni e informazioni per il management e altri rapporti su clienti, operazioni, attività, offerte e qualsiasi altro aspetto commerciale di Helsana ai fini della gestione e dello sviluppo dell'azienda, della sua offerta e delle sue attività, project management;

(Detti collettivamente **scopo di elaborazione dei clienti**).

Helsana utilizza i dati dei clienti a scopo di trattamento dei medesimi in virtù delle basi legali seguenti:

- adempimento del contratto;
- adempimento di un obbligo legale di Helsana;
- autorizzazione del cliente (in particolare nella misura in cui il trattamento avviene a motivo di una richiesta concreta, che può essere revocata in qualsiasi momento, ad esempio per ricevere una newsletter a cui il cliente si è iscritto);
- legittimi interessi di Helsana, in particolare
 - protezione efficiente ed efficace di clienti, collaboratori e altre persone nonché protezione di dati, segreti e valori patrimoniali di Helsana e di quelli che le sono stati affidati, sicurezza dei sistemi e degli edifici di Helsana;
 - rispetto dei criteri legali e normativi e delle regole interne di Helsana;
 - assistenza efficiente ed efficace dei clienti, cura dei contatti e altre comunicazioni con i clienti anche al di fuori dell'esecuzione del contratto;
 - mantenimento e organizzazione sicura, efficiente ed efficace dell'esercizio dell'azienda, compreso un esercizio sicuro, efficiente ed efficace e il buon esito di un ulteriore sviluppo del sito Internet e di altri sistemi informatici;
 - vendita e fornitura di prodotti e servizi anche in relazione a persone che non sono direttamente partner contrattuali (come ad es. beneficiari);
 - conduzione e sviluppo razionale dell'azienda;
 - comprensione di comportamenti, attività, preferenze ed esigenze dei clienti, studi di mercato;
 - miglioramento efficiente ed efficace dei prodotti e servizi esistenti e sviluppo di nuovi prodotti e servizi;
 - realizzazione di pubblicità e marketing;
 - funzionamento di sistemi informatici di Helsana;
 - buon esito della vendita o dell'acquisto di settori aziendali, società o parti di società e altre operazioni di diritto societario;
 - interesse a impedire truffe, crimini e reati nonché alle indagini in relazione a tali reati e altri comportamenti inopportuni, trattamento di azioni legali e procedimenti nei confronti di Helsana, partecipazione a procedimenti legali e collaborazione con autorità nonché qualsiasi rivendicazione, esercizio o difesa di diritti legali.

5.2 Dati dei partner

Nella misura consentita dalle disposizioni applicabili in materia di protezione dei dati Helsana può trattare i dati dei partner in particolare per gli scopi seguenti: stipulazione ed esecuzione di contratti e altri rapporti di affari con i partner, promozioni, pubblicità e marketing, comunicazione, invito a eventi e partecipazione ad azioni per i partner, svolgimento di attività congiunte, rispetto dei criteri legali e normativi nonché delle regole interne di Helsana, esercizio e messa in atto di vari diritti, difesa da pretese legali, processi civili, ricorsi, lotta alle frodi e agli abusi, per scopi concernenti inchieste o procedimenti legali e per rispondere alle richieste di informazioni da parte delle autorità, per la vendita o l'acquisto di settori aziendali, società o parti di società e altre operazioni di diritto societario con il relativo trasferimento di dati dei partner. Tutto questo sulla medesima base come spiegato più sopra per i dati dei clienti.

6. Comunicazione dei dati a terzi

6.1 Obbligo del segreto

Tutti i collaboratori di Helsana sottostanno all'obbligo del segreto (art. 33 LPGA). I collaboratori sono informati sulle sanzioni e inoltre quando entrano in servizio presso Helsana firmano una dichiarazione di segretezza e sull'obbligo del segreto.

6.2 Eccezioni all'obbligo del segreto

Le eccezioni all'obbligo del segreto sono definite dalla legge (art. 32 LPGA e artt. 97 e 98 LAINF) e sono applicabili – purché non vi siano interessi privati preponderanti che vi si oppongono – in particolare al trattamento di dati personali da parte di

- terzi su mandato di Helsana;
- altri terzi, se nel caso concreto la persona interessata ha dato il suo consenso scritto oppure non è possibile chiedere il consenso o in base alle circostanze il consenso si può presumere, in quanto nell'interesse della persona assicurata;
- altri organi dell'assicurazione sociale, se necessario per adempiere i propri compiti legali o se sussiste un obbligo legale di rendere noti i dati;
- altre autorità, tribunali e pubblici uffici (ad es. in relazione all'imposta alla fonte, alle statistiche della Confederazione, a una denuncia penale, per impedire un reato o per l'incasso dei premi).

I dati non personali possono essere resi noti se ciò corrisponde a un interesse preponderante. Purché sia garantito l'anonimato delle persone interessate, è consentito pubblicare i dati di interesse generale.

6.3 Categorie di terzi

Nella misura in cui le disposizioni legali applicabili (anche concernenti la protezione dei dati) lo consentono, Helsana può trasmettere i dati dei clienti e dei partner alle seguenti categorie di terzi che trattano i dati personali per il rispettivo scopo specifico su mandato di Helsana o per propri scopi:

- interessati (in particolare assicurati) e terzi da questi delegati;
- altre società del gruppo Helsana;
- altri assicuratori (malattia) al di fuori del gruppo Helsana;
- organizzazioni di categoria, federazioni, organizzazioni e altri organismi;
- fornitori di prestazioni, medici consulenti, ufficio dell'ombudsman;
- prestatori di servizi (all'interno e all'esterno del gruppo Helsana), ivi compresi i responsabili del trattamento su mandato;
- fornitori e altri partner di affari;
- acquirenti o interessati all'acquisto di settori aziendali, società o altre parti di Helsana;
- media;
- pubblico;
- autorità e pubblici uffici locali, nazionali o esteri (in particolare organi della Confederazione e dei Cantoni, uffici AI, ecc.);

- altre parti in procedimenti legali possibili o reali.

7. Trasmissione di dati all'estero

Helsana può trasmettere i dati dei clienti e dei partner all'interno di Helsana, come pure a terzi in qualsiasi Paese del mondo, in particolare in tutti i Paesi, in cui i prestatori di servizi di Helsana trattano i suoi dati (segnatamente nei Paesi Bassi, in Irlanda, in Germania). Se i dati sono trasmessi in un Paese senza un'adeguata protezione dei dati, Helsana garantisce una protezione adeguata ricorrendo a sufficienti garanzie contrattuali, segnatamente sulla base di clausole contrattuali tipo dell'UE, Binding Corporate Rules o basandosi sulle eccezioni del consenso, dell'esecuzione del contratto, dell'accertamento, dell'esercizio o della rivendicazione di pretese legali, dell'interesse pubblico preponderante, dei dati pubblicati da clienti o partner o perché necessario per tutelare l'incolumità delle persone in questione. Inviando la copia di un documento ufficiale di identità all'indirizzo di contatto sopra indicato (cfr. 3), il cliente o il partner può chiedere una copia delle garanzie contrattuali o sapere dove si può ritirare una tale copia. Helsana si riserva il diritto di annerire alcune parti di tali copie per motivi di protezione dei dati o di segretezza.

Le trasmissioni di dati all'estero avvengono in particolare nei confronti di fornitori di prestazioni stranieri in relazione alle garanzie d'assunzione dei costi, ai formulari elettronici e ai rimpatri.

8. Conservazione dei dati

In linea di principio Helsana archivia i dati dei clienti relativi ai contratti e i dati dei partner per la durata del rapporto contrattuale, che può durare in parte fino all'età di pensionamento e, per le rendite d'invalidità LAINF fino al decesso, e per dieci anni oltre la fine del rapporto contrattuale, se nel caso concreto non vige l'obbligo legale di un'archiviazione più lunga o più breve, se è necessario a titolo di prova (segnatamente in caso di accertamenti ai fini di una revisione) o se in base a un altro diritto applicabile sussiste un motivo valido per un'eccezione o è indicata una cancellazione anticipata (segnatamente perché i dati non servono più o Helsana è obbligata a cancellarli).

Per i dati aziendali contenenti dati di clienti o di partner (ad es. protocolli, log) si applicano in linea di principio termini di archiviazione più brevi, di 13 mesi al massimo.

I documenti aziendali, comunicazioni comprese, vengono conservati per tutto il tempo in cui Helsana è interessata agli stessi (per esempio, in particolar modo, se interessano come prova in caso di pretese, documentazione del rispetto di determinate prescrizioni legali e altre prescrizioni o se vi è un interesse a un'analisi impersonale) o è obbligata a farlo (per contratto, per legge o in virtù di altre prescrizioni). Restano riservati gli obblighi per esempio riguardo all'anonimizzazione o alla pseudonimizzazione dei dati.

9. Raccolta di dati di Helsana

9.1 Struttura

La raccolta di dati di Helsana è strutturata in base alle attività dati e comprende le categorie seguenti:

- gestione dei canali di vendita e sostegno alle vendite;
- sviluppo dell'offerta;
- attività con nuovi clienti;
- servizio clienti;

- amministrazione contratti;
- management delle prestazioni;
- acquisto prestazioni;
- assicurazione del personale;
- scienze della salute;
- incasso, finanze, attuariato;
- audit, risk, legal e compliance;
- management IT e gestione sicurezza dati;
- Fondazione di previdenza per il personale;
- acquisti.

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

9.2 Utilizzo e accesso ai dati

9.2.1 Persone autorizzate all'accesso

Alla raccolta di dati di Helsana hanno diritto ad accedere:

- collaboratori di Helsana, se ciò è necessario per svolgere il proprio incarico «Gestione dell'assicurazione infortuni»;
- sistemisti di Helsana;
- prestatori di servizi cui sia stato conferito un mandato contrattuale

(detti collettivamente **persone autorizzate all'accesso**).

9.2.2 Gestione delle persone autorizzate all'accesso

Della gestione delle persone autorizzate all'accesso si occupa in modo centralizzato l'IT di Helsana. I collaboratori interni vengono registrati attraverso l'interfaccia HR e quelli esterni attraverso il rispettivo sourcing. 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.

9.2.3 Autorizzazione personale di accesso

Con l'entrata in servizio presso Helsana, ogni collaboratore riceve le sue autorizzazioni di accesso alle informazioni in base al modello dei ruoli, secondo la funzione assegnatagli. 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, dall'approvatore del ruolo.

9.2.4 Revoca dell'autorizzazione di accesso

L'autorizzazione di accesso alla raccolta di dati di Helsana è valida soltanto finché il collaboratore in questione necessita dei dati per svolgere la propria funzione lavorativa. Se 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.

9.2.5 Formazione delle persone autorizzate all'accesso

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

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

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

Le unità organizzative competenti creano, mediante istruzioni specifiche, un livello di valutazione delle prestazioni secondo la LAINF uniforme per tutto il territorio assicurativo della Svizzera.

9.2.7 Prestatori di servizi informatici

Se l'esercizio della raccolta di dati di Helsana è stato esternalizzato a prestatori esterni di servizi informatici, questi si attengono nel proprio settore a regole analoghe.

10. Misure tecniche e organizzative

10.1 Controllo di accesso

Tutti i locali di Helsana in cui vengono trattati dati personali degni di particolare protezione sono protetti mediante un sistema elettronico o manuale dall'accesso di persone non autorizzate. I responsabili tengono un verbale sull'amministrazione delle chiavi e sul controllo elettronico di accesso. 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 supporti elettronici di dati 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 supporti elettronici di dati nei server e nei computer decentralizzati non gestiti dall'IT di Helsana sono protetti con misure di sicurezza paragonabili a quelle dei server e dei computer da essa gestiti.

10.2 Controlli dei supporti di dati personali

Le misure a livello informatico consentono di trattare i dati sui supporti elettronici esclusivamente alle persone autorizzate. Solo le persone autorizzate possono accedere alla raccolta di dati di Helsana.

10.3 Autenticazione delle persone autorizzate all'accesso

L'accesso ai sottosistemi della raccolta di dati di Helsana viene protetto dall'ID utente combinato a una password personale, la cui validità è limitata nel tempo.

10.4 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).

10.5 Trasmissione di dati

La trasmissione di dati tra i dispositivi terminali e il computer host è protetta dal protocollo di trasmissione.

10.6 Controllo dell'archiviazione

Le persone autorizzate all'accesso ricevono autorizzazioni specifiche per le modifiche dei campi dati di cui hanno bisogno per svolgere i loro compiti secondo la LAINF.

10.7 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.

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

I terminali sono collocati in zone protette. I dispositivi mobili contengono memorie di dati protette da un'efficace procedura di cifratura con password.

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.

10.9 Verbalizzazione

Oltre al controllo degli accessi alla raccolta di dati di Helsana mediante la procedura di autorizzazione e la protezione attraverso il riconoscimento dell'ID utente e la password, i singoli sottosistemi dispongono di una verbalizzazione del trattamento automatizzato, in modo da poter verificare a posteriori se il trattamento dei dati è avvenuto in conformità agli scopi per cui tali dati sono stati raccolti o comunicati. La verbalizzazione viene effettuata in applicazione dell'art. 10 OLPD: i verbali vengono conservati per 13 mesi in una forma che sia adeguata a un'eventuale revisione. Sono accessibili esclusivamente agli organi incaricati di verificare l'applicazione delle disposizioni per la protezione e la sicurezza dei dati e possono essere utilizzati soltanto a questo scopo. Nel caso dei prestatori esterni di servizi informatici, per la verbalizzazione vigono regole in parte simili a quelle menzionate, ma proprie.

10.10 Sviluppo

Le richieste per un ulteriore sviluppo del sistema vengono raggruppate nonché definite, preventivate e realizzate come intervento di manutenzione, piccolo progetto o progetto. La procedura è disciplinata nell'ambito della «procedura progettuale Helsana».

10.11 Assistenza per le persone autorizzate all'accesso e obbligo di comunicazione

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

Le persone autorizzate all'accesso sono a conoscenza della classificazione dei livelli di sicurezza della raccolta dei dati di Helsana e delle disposizioni concernenti l'uso del sistema e dei relativi dati. Le disposizioni sono descritte nei manuali di istruzioni nella sezione dedicata alla 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.

Tutte le persone autorizzate all'accesso sono tenute a segnalare le seguenti constatazioni al process owner o al rappresentante delle persone autorizzate all'accesso:

- punti deboli e vizi osservati o presunti riguardo alla sicurezza del sistema;
- misure di sicurezza non attuate o non rispettate;
- eventi imprevisti che possono ripercuotersi sulla sicurezza dell'informazione.

10.12 Vigilanza e responsabilità

I process owner dei sottosistemi controllano che le persone autorizzate all'accesso si attengano alle direttive e al presente regolamento sul trattamento dei dati e i prestatori esterni di servizi informatici alle loro disposizioni contrattuali.

11. Diritti dei clienti e dei partner

Ogni interessato, cliente e partner ha nei confronti di Helsana il diritto di ottenere informazioni sui dati personali che lo concernono. Inoltre, ha il diritto di esigere da Helsana la rettifica, la cancellazione e la limitazione dei dati personali che lo concernono come pure di opporsi a un tale trattamento dei dati personali. Se il trattamento dei dati personali si basa su un consenso, tale consenso può essere revocato in qualsiasi momento dalla persona interessata. Negli Stati dell'UE e del SEE in determinati casi la persona assicurata ha il diritto di ricevere i dati generati dall'uso dei servizi online in una forma strutturata, usuale e leggibile da computer, così da poter essere ulteriormente utilizzati e trasmessi. Le richieste relative a tali diritti devono essere inviate per iscritto, allegando la copia di un documento di identità ufficiale, all'indirizzo di contatto (cfr. punto 3). Helsana si riserva di limitare i diritti della persona interessata entro i limiti delle norme legali applicabili, ad es. non fornendo tutte le informazioni richieste o rifiutandosi di cancellarle.

Se Helsana prende automaticamente nei confronti di una singola persona una decisione che produce effetti giuridici che la riguardano o la danneggia notevolmente in modo analogo, la persona in questione può parlare con un collaboratore competente di Helsana e chiedergli un riesame della decisione o esigere fin dal principio la valutazione da parte di una persona, se il diritto applicabile lo prevede. In tal

caso, eventualmente, la persona interessata non può più utilizzare determinati servizi automatizzati. Tale persona viene informata di dette decisioni successivamente o in anticipo in separata sede.

Ogni persona interessata ha il diritto di interporre ricorso presso l'autorità competente per la protezione dei dati. In Svizzera tale autorità è l'Incaricato fed. della protezione dei dati e della trasparenza (<http://www.edoeb.admin.ch/edoeb/it/home.html>).

12. Modifica della Dichiarazione sulla protezione dei dati

Helsana può modificare la presente Dichiarazione sulla protezione dei dati in qualsiasi momento senza preavviso né comunicazione. Si applica sempre la versione attuale pubblicata nel sito Internet.

Se la Dichiarazione sulla protezione dei dati fa parte di un accordo con clienti e partner, in caso di aggiornamento Helsana può informarli della modifica mediante e-mail o in altro modo idoneo. In assenza di contestazione entro 30 giorni si ritiene che la nuova Dichiarazione sulla protezione dei dati sia stata accettata. In caso di contestazione, Helsana ha facoltà di disdire l'accordo in via straordinaria e senza preavviso.

* * * * *