

Regolamento di elaborazione dei dati del Gruppo Sanitas

1. Introduzione

La Sanitas Assicurazione Malattia (di seguito denominata Sanitas) elabora conformemente alla Legge federale sulla protezione dei dati (LPD) dati personali nel quadro della Legge federale sull'assicurazione malattie (LAMal) e della Legge federale sull'assicurazione infortuni (LAINF) in qualità di organo federale e di persona giuridica privata ai sensi della Legge federale sul contratto d'assicurazione (LCA).

In virtù dell'art. 12 della Legge federale sulla protezione dei dati (LPD) e degli artt. 5 e 6 dell'Ordinanza sulla protezione dei dati (OPDa), Sanitas è tenuta, tra l'altro, a redigere un regolamento di elaborazione.

1.1 Scopo e ambito di applicazione

Il regolamento di elaborazione dei dati garantisce la necessaria trasparenza nell'ambito dell'elaborazione dei dati.

Il regolamento rende l'elaborazione dei dati comprensibile e valutabile anche ai «non addetti ai lavori».

Il presente regolamento di elaborazione dei dati stabilisce i principi dell'elaborazione dei dati ai sensi della LPD. Sanitas osserva in particolare i seguenti principi.

- L'elaborazione dei dati da parte di Sanitas si basa su basi legali o sul consenso esplicito della persona interessata. Il consenso esplicito deve essere fornito, ad esempio, se un privato effettua una profilazione ad alto rischio o se un organo federale effettua la profilazione.
- I dati personali possono essere elaborati soltanto per lo scopo indicato all'atto della loro raccolta, risultante dalle circostanze o previsto da una legge. Lo scopo dell'elaborazione dei dati personali e la loro acquisizione devono essere espressamente dichiarati, riconoscibili dalla persona interessata o evidenti dalle circostanze.
- La portata dell'elaborazione deve essere proporzionata allo scopo e limitata a quanto necessario per raggiungere l'obiettivo.
- I dati personali devono essere distrutti o anonimizzati non appena non sono più necessari ai fini dell'elaborazione.
- I dati devono essere protetti da misure di sicurezza tecniche e organizzative. I dati errati vengono rettificati.
- I diritti della persona interessata devono essere rispettati. La persona interessata riceve informazioni sui propri dati registrati e può richiederne la cancellazione o la rettifica.

1.2 Attualità

Il detentore della collezione di dati dovrà rivedere annualmente il regolamento e le descrizioni delle collezioni di dati per assicurarsi che siano aggiornati e notificare all'IPD eventuali modifiche o confermarne l'attualità.

1.3 Definizioni e abbreviazioni

Nel presente regolamento di elaborazione dei dati vengono utilizzate le seguenti abbreviazioni.

- IPD Incaricato alla protezione dei dati del Gruppo Sanitas

- LPD Legge federale del 20 settembre 2020 sulla protezione dei dati, RS 235.1
- IFPDT Incaricato federale della protezione dei dati e della trasparenza
- OPDa Ordinanza sulla protezione dei dati del 31 agosto 2022, RS 235.11
- LAMal Legge federale del 18 marzo 1994 sull'assicurazione malattie, RS 832.10
- MF Medico di fiducia
- SMF Servizio medico-fiduciario

2. Notifica della collezione di dati all'IFPDT

La Sanitas adempie all'obbligo di presentazione nei confronti dell'IFPDT ai sensi dell'art. 84b LAMal.

3. Protezione e sicurezza dei dati

3.1 Protezione dei dati

Il Consiglio d'Amministrazione del Gruppo Sanitas è responsabile del rispetto della protezione dei dati. Ne delega l'attuazione al Comitato direttivo delle società del Gruppo.

Il Comitato direttivo è responsabile dell'attuazione, della comunicazione, del controllo e del monitoraggio della politica di protezione dei dati prescritta in tutto il Gruppo Sanitas. Garantisce che Sanitas abbia un'organizzazione efficiente che sostiene il rispetto della protezione dei dati. Sanitas dispone di un consulente per la protezione dei dati, che a sua volta garantisce l'attuazione delle direttive di protezione dei dati e dispone delle necessarie risorse umane e finanziarie.

L'Incaricato alla protezione dei dati del Gruppo Sanitas (IPD) definisce i comportamenti più importanti in materia di protezione dei dati e garantisce il rispetto delle disposizioni sulla protezione dei dati applicabili alle imprese del Gruppo Sanitas.

L'IDP, in collaborazione con gli uffici interni competenti, emette direttive appropriate per il rispetto di leggi e standard il cui scopo principale è creare una trasparenza ottimale nell'elaborazione dei dati personali al fine di consentire l'adeguata identificazione e valutazione di eventuali rischi per la protezione dei dati.

All'interno della propria sfera di competenza, collaboratrici e collaboratori sono responsabili del rispetto di tutte le disposizioni in materia di protezione dei dati, in particolare dell'obbligo d'informazione e di riservatezza. Questa responsabilità non può essere delegata né da collaboratrici e collaboratori, né da superiori. Al momento dell'assunzione, ogni collaboratore e ogni collaboratrice Sanitas deve firmare una dichiarazione di protezione dei dati. Collaboratrici e collaboratori di Sanitas devono inoltre mantenere la riservatezza nei confronti di terzi sulle informazioni di cui vengono a conoscenza nell'ambito della loro attività professionale, in particolare sui dati medici, durante e dopo la cessazione del rapporto di lavoro. I superiori devono garantire che collaboratrici e collaboratori siano costantemente informati sulle disposizioni legali e interne applicabili.

Il presente regolamento di elaborazione disciplina anche i criteri di accesso ai dati e l'acquisizione dei diritti di accesso ai dati, nonché la gestione delle informazioni ottenute dalla collezione dei dati. Le persone autorizzate hanno accesso soltanto ai dati personali di cui hanno bisogno per svolgere i loro compiti.

L'accesso ai locali in cui vengono elaborati dati personali degni di particolare protezione è protetto mediante limitazioni di accesso. L'accesso ai locali è consentito solo a collaboratrici e collaboratori Sanitas o a terzi che hanno un rapporto di consulenza con Sanitas e che hanno sottoscritto una dichiarazione di protezione dei dati e di riservatezza. L'accesso ai locali del servizio medico-fiduciario è soggetto a ulteriori restrizioni.

Per quanto riguarda l'utilizzo di hardware e software, Internet e posta elettronica, si applicano in aggiunta le direttive sull'utilizzo sicuro di tali strumenti.

3.2 Sicurezza dei dati

Per proteggere i sistemi, l'accesso ai dati è generalmente possibile solo se la persona che accede può legittimarsi attraverso un nome utente e una password. I client e le applicazioni informatiche che hanno accesso a dati personali degni di particolare protezione sono inoltre provvisti di ulteriori limitazioni.

3.2.1 Misure generali

I sistemi operativi di Sanitas sono regolarmente controllati e protetti contro gli attacchi di malware. Per proteggere le collezioni di dati dalla distruzione non autorizzata o accidentale, dalla perdita accidentale, da errori tecnici, dalla falsificazione, dal furto o dall'uso illegale e dall'elaborazione non autorizzata, vengono adottate le seguenti misure:

- backup, salvataggio dei dati
- verbalizzazione
- protezione d'accesso
- reti sicure
- comunicazione all'esterno (e-mail, Internet) di dati personali degni di particolare protezione solo con una sufficiente codificazione
- limitazione dell'accesso al centro dati, alle reti e ad altre strutture tecniche per la conservazione e l'elaborazione di dati

3.2.2 Misure speciali

Controllo d'accesso

L'accesso agli edifici Sanitas è protetto da un sistema di badge. I visitatori devono registrarsi alla reception. I locali / edifici con attrezzature tecniche per la trasmissione e la conservazione di dati, come server, router, switch ecc. sono protetti da sistemi di chiusura e/o accesso e sono accessibili solo a un gruppo ristretto di persone. Le stanze e gli edifici con client che consentono l'accesso alle collezioni di dati sono protetti da sistemi di accesso.

Controllo dei supporti di dati personali

Le misure di limitazione dell'accesso ai locali e ai dati permettono di controllare anche i supporti di dati personali. Grazie a precauzioni tecniche, l'elaborazione dei dati su supporti elettronici è consentita solo alle persone autorizzate.

Controllo del trasporto

È necessario impedire alle persone non autorizzate di leggere, copiare (su altri drive o supporti di dati), stampare, modificare o rimuovere i supporti di dati.

Non è consentito inviare informazioni sensibili in forma non codificata tramite posta elettronica (e-mail). Ove possibile, il necessario trasporto di dati sensibili deve avvenire per via elettronica ed essere codificato mediante una procedura riconosciuta.

Il trasporto fisico di dati avviene tramite un sistema di trasporto sicuro, i dati vengono codificati per il trasporto con una procedura riconosciuta e la chiave viene trasportata separatamente.

Controllo di comunicazione e descrizione delle interfacce

I destinatari dei dati a cui vengono comunicati dati personali tramite impianti di trasmissione dei dati vengono identificati ed è garantito il rispetto dei requisiti legali per la comunicazione (base giuridica, dichiarazione di consenso). Le trasmissioni di dati vengono verbalizzate e l'identità dei dati viene controllata prima della loro trasmissione.

Controllo di memoria

Gli inserimenti, le modifiche o le cancellazioni non autorizzate nella memoria sono impediti da controlli dell'accesso ai locali e agli impianti e da controlli delle autorizzazioni (p. es. nome utente / password) e dalle applicazioni informatiche. Quando si sostituiscono le memorie dei dati (dischi rigidi) o i computer (PC e server), è necessario assicurarsi che tutti i dati vengano cancellati in modo irrevocabile.

Controllo degli utenti

L'accesso ai sistemi di elaborazione dei dati è di principio protetto da misure tecniche e deve essere approvato per ogni singolo collaboratore e collaboratrice. Il sistema d'informazione concede a collaboratrici e collaboratori diritti di accesso differenziati. L'accesso da parte delle persone autorizzate è limitato ai dati di cui le persone autorizzate hanno effettivamente bisogno per svolgere i loro compiti.

Diritto d'accesso ai dati / autorizzazioni

L'accesso ai dati dell'elaborazione automatizzata è consentito a collaboratrici e collaboratori solo mediante applicazioni informatiche. È necessario richiedere le autorizzazioni necessarie. Collaboratrici e collaboratori hanno diritti d'uso solo per le applicazioni informatiche di cui hanno bisogno per svolgere i loro compiti e, all'interno delle applicazioni informatiche, solo per le aree funzionali che corrispondono ai loro compiti. Le richieste di autorizzazione devono essere approvate dai rispettivi superiori e dal titolare dell'autorizzazione. Le autorizzazioni devono essere ritirate a collaboratrici e collaboratori quando non sono più necessarie per i compiti assegnati.

L'organizzazione interna definisce i diritti di accesso per ogni collaboratrice e collaboratore attraverso un concetto di accesso ai dati. Quanto più sensibili sono i dati elaborati, tanto più elevati sono i requisiti per l'autorizzazione all'accesso ai dati. Viene conservato un elenco (file di log di audit) delle autorizzazioni concesse.

L'accesso remoto ai sistemi di elaborazione dei dati è possibile solo per persone appositamente autorizzate tramite un accesso codificato.

Controllo dell'introduzione

Vengono verbalizzati i dati introdotti e le mutazioni. Quando i dati vengono introdotti o modificati automaticamente - il che avviene principalmente durante lo scambio elettronico di dati o l'elaborazione automatica successiva, come ad esempio l'esecuzione di pagamenti ecc. - di principio si verbalizza l'origine dei dati e il tempo di elaborazione.

4. Procedura di elaborazione dei dati

4.1 Diritto d'informazione

Il Consulente per la protezione dei dati di Sanitas è responsabile di concedere agli assicurati il diritto di accesso ai propri dati. Il Consulente per la protezione dei dati ottiene i dati, fornisce le informazioni e, se necessario, garantisce la rettifica dei dati secondo un processo definito internamente.

Le richieste possono essere inviate per iscritto al seguente indirizzo:

Sanitas Assicurazione Malattia

Consulente per la protezione dei dati

Jägergasse 3

8021 Zurigo

4.2 Procedura di rettifica

Una volta identificate, le persone interessate possono richiedere che i dati registrati su di loro che sono sproporzionati o non necessari per l'esecuzione del contratto siano rettificati o distrutti. Il Consulente per la protezione dei dati di Sanitas decide in merito a tali richieste.

4.3 Blocco dei dati

Tutte le persone inserite in una collezione di dati possono, previa identificazione, richiedere il blocco dell'elaborazione dei dati e in particolare della comunicazione dei loro dati a terzi. Il Consulente per la protezione dei dati di Sanitas decide in merito a tali richieste e decide le conseguenze della loro attuazione.

4.4 Anonimizzazione

I test e i progetti sono realizzati con dati anonimizzati. I dati statistici sono anonimizzati in conformità ai requisiti di legge. Non è possibile risalire a persone specifiche.

4.5 Archiviazione

I dati vengono conservati in conformità ai requisiti di legge e alle direttive aziendali interne.

4.6 Backup / Ripristino

Vengono eseguiti backup regolari di tutti i dati rilevanti definiti come tali nei contratti. Le banche dati vengono regolarmente copiate in un registro separato e sottoposte a backup. Il ripristino dei dati è garantito dal sistema di backup.

4.7 Verbalizzazione

Vengono verbalizzate importazioni definite (v. punto «Interfacce») nonché i login degli utenti nei sistemi che consentono la verbalizzazione. Sanitas può analizzare le verbalizzazioni in forma anonima per controllare il rispetto del regolamento di utilizzo. Se viene rilevato o sospettato un uso improprio, Sanitas può effettuare un'analisi completa dell'utilizzo. I dati verbalizzati devono essere conservati per un anno in conformità con i requisiti in materia di revisione.

4.8 Definizione delle collezioni di dati

Le collezioni di dati di Sanitas si basano sui processi aziendali. Ne risultano le seguenti collezioni di dati:

dati anagrafici / contrattuali

- dati sulle prestazioni
- dati finanziari
- dati dell'offerta e della proposta
- casi di regresso
- dossier d'esecuzione
- dati telefonici
- garanzie di copertura dei costi
- dati dell'intermediario

4.8.1 Interfacce

Le descrizioni delle interfacce esterne rilevanti per l'azienda contengono l'origine dei dati, il destinatario, lo scopo, il tipo di dati e le informazioni sulla periodicità e sul tipo di trasmissione dei dati.

Nella descrizione dell'interfaccia sono riportate le seguenti informazioni sulla trasmissione dei dati (comunicazione).

- Da dove provengono i dati?
- Chi riceve i dati?
- A quale scopo vengono trasmessi i dati?
- Quali dati vengono trasmessi?
- Con quale periodicità vengono trasmessi i dati?
- Chi ha avviato la trasmissione dei dati?
- In quale forma vengono trasmessi i dati?

4.8.2 Processi

La raccolta, l'elaborazione e la trasmissione dei dati da parte di Sanitas avvengono secondo processi definiti. I singoli processi sono documentati in descrizioni di processo destinate all'uso interno.

4.8.3 Responsabilità

- Protezione dei dati in generale e richieste di accesso: Consulente per la protezione dei dati Sanitas
- Sicurezza tecnica dei dati: settore aziendale IT
- Distruzione di dati elettronici: settore aziendale IT
- Documenti per il medico di fiducia: medico di fiducia
- Controlli di accesso: Incaricato della sicurezza Sanitas

5. Disposizioni finali

5.1 Entrata in vigore

Il presente regolamento sostituisce tutti i regolamenti pubblicati in precedenza. Il presente documento entra in vigore il 1° settembre 2023*.

5.2 Documenti complementari

- Regolamenti di elaborazione
- Elenco delle attività di elaborazione
- Concetti di accesso alle collezioni di dati

* Decisione del Comitato direttivo