1. Governance

Regolamento sulla protezione dei dati del Gruppo Assura

Indice

1. Scopo e campo di applicazione

1.1 Scopo

1.1.1 Il presente regolamento ha lo scopo di definire la politica generale di protezione e sicurezza dei dati del Gruppo Assura.

1.1.2 Esso stabilisce i principi e le norme applicabili che le società del Gruppo Assura, come definite dal Regolamento sull'organizzazione del Gruppo Assura («Règlement d'organisation du Groupe Assura»), e i loro collaboratori devono seguire nel trattamento dei dati di potenziali clienti, assicurati, candidati, collaboratori delle società del Gruppo Assura, terzi (come fornitori e intermediari assicurativi) e subappaltatori.

1.1.3 I principi e le norme di seguito riportati devono in particolare consentire l'attuazione dei requisiti di legge, in particolare quelli previsti dalla legge federale sulla protezione dei dati (LPD) in materia di trattamento dei dati personali, delle relative ordinanze di esecuzione (OPDa e OCPD) e dei requisiti regolamentari delle autorità di vigilanza.

1.2 Campo d'applicazione

1.2.1 Il presente regolamento si applica a tutte le società del Gruppo Assura come definite dal Regolamento sull'organizzazione del Gruppo Assura («Règlement d'organisation du Groupe Assura»).

1.2.2 Secondo la LPD, occorre distinguere tra i privati (persone fisiche e giuridiche) come Figeas SA, Assura SA o gli intermediari assicurativi, e gli organi federali come Assura-Basis SA, dato che ad essi si applicano alcune norme specifiche.

1.2.3 Sono interessati tutti i dati trattati nell'ambito dello svolgimento delle relative funzioni dei collaboratori, della Direzione generale e del Consiglio di amministrazione.

1.2.4 Il regolamento si applica anche ai dati trattati all'estero, a condizione che abbiano conseguenze in Svizzera.

1.2.5 L'emanazione del presente regolamento e delle sue successive modifiche è di competenza del Consiglio di amministrazione del Gruppo Assura.

1.2.6 L'uso di termini al genere maschile nel presente regolamento per riferirsi a persone è da considerarsi maschile generico comprende persone di entrambi i sessi.

2. Definizioni

Nel presente regolamento si applicano le seguenti definizioni:

2.1 Comunicazione

La trasmissione di dati personali o il fatto di renderli accessibili, anche all'estero (Stati o organismi internazionali).

2.2 Consenso

2.2.1 Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile con la quale l'interessato accetta, con una dichiarazione o con un atto concludente, che i dati personali che lo riguardano possono essere trattati.

2.2.2 Il consenso deve essere dato espressamente, ossia deve risultare da un'esplicita e chiara manifestazione di consenso nel caso di trattamento di dati sensibili o di profilazione da parte di un organo federale.

2.3 Decisione individuale automatizzata

Una decisione presa esclusivamente sulla base di un trattamento automatizzato dei dati personali, senza intervento umano, e che ha effetti giuridici per l'interessato o lo riguarda in modo significativo.

2.4 Dati

2.4.1 Tutte le informazioni che riguardano il Gruppo Assura e le sue società, gli assicurati, i potenziali clienti, i collaboratori del Gruppo Assura, i fornitori e i partner esterni (in particolare gli intermediari assicurativi).

2.4.2 Per «dati che riguardano il Gruppo Assura e le sue società» si intendono le informazioni relative alla loro organizzazione, alle loro procedure, ai loro processi e alle loro decisioni.

2.5 Dati personali

Qualsiasi informazione relativa a una persona fisica identificata o identificabile, in particolare un assicurato, un potenziale cliente, un collaboratore del Gruppo Assura, un fornitore o un partner esterno (in particolare gli intermediari assicurativi).

2.6 Dati personali sensibili

Tutti i dati personali relativi alla salute, alla sfera privata, all'origine etnica o razziale, alle opinioni o attività religiose, politiche, filosofiche o sindacali, nonché alle misure di assistenza sociale, i dati relativi a perseguimenti e sanzioni penali e amministrative, come pure i dati genetici e biometrici.

2.7 Organo federale

Autorità o servizio della Confederazione, oppure persona cui sono affidati compiti federali. Assura-Basis SA è un organo federale ai sensi della LPD.

2.8 Persona interessata

2.8.1 La persona fisica o giuridica i cui dati sono oggetto di trattamento.

2.8.2 Ai sensi della LPD, si tratta solo della persona fisica.

2.9 Privato

Il privato, la persona fisica o giuridica, che tratta i dati personali nell'ambito di un rapporto privato. Assura SA, allo stesso modo di Figeas SA, è un privato ai sensi della LPD.

2.10 Incaricato federale della protezione dei dati e della trasparenza (IFPDT)

La persona fisica incaricata di vigilare sulla corretta applicazione delle disposizioni federali sulla protezione dei dati. Si tratta dell'autorità di vigilanza in materia di protezione dei dati.

2.11 Profilazione

2.11.1 Trattamento automatizzato di dati personali consistente nell'utilizzazione degli stessi per valutare determinati aspetti personali di una persona fisica, in particolare per analizzare o prevedere aspetti concernenti il rendimento professionale, la situazione economica, la salute, le preferenze, gli interessi, l'affidabilità, il comportamento, i luoghi di permanenza e gli spostamenti di tale persona.

2.11.2 Se la profilazione comporta un collegamento tra dati che permette di valutare aspetti essenziali della personalità di una persona fisica, deve essere qualificata come profilazione a rischio elevato.

2.12 Titolare del trattamento

Il privato (fisico o giuridico) o l'organo federale che, singolarmente o insieme ad altri, determina lo scopo e i mezzi del trattamento dei dati, ossia l'obiettivo e il modo di realizzarlo.

2.13 Responsabile del trattamento

Il fornitore di servizi che tratta i dati personali per conto e secondo le istruzioni del titolare del trattamento.

2.14 Trattamento dei dati

Qualsiasi operazione relativa a dati personali, indipendentemente dai mezzi e dalle procedure impiegati, segnatamente la raccolta, la registrazione, la conservazione, l'utilizzazione, la modificazione, la comunicazione, l'archiviazione, la cancellazione o la distruzione di questo tipo di dati.

2.15 Violazione della sicurezza dei dati

Violazione della sicurezza in seguito alla quale, in modo accidentale o illecito, dati personali vengono persi, cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate.

3. Ruoli e responsabilità in materia di protezione dei dati

3.1 Direzione generale

3.1.1 La Direzione generale del Gruppo Assura è responsabile dell'applicazione di un'organizzazione interna conforme alle normative in materia di protezione dei dati.

3.1.2 È coadiuvata dal Consulente per la protezione dei dati.

3.2 Consulente per la protezione dei dati

Il Consulente per la protezione dei dati svolge in particolare le seguenti mansioni:

a) Definisce i requisiti minimi di protezione dei dati in base alla loro natura e alle finalità per cui vengono trattati.
b) Supporta i servizi operativi nell'attuazione delle misure relative alla protezione e alla sicurezza dei dati personali.
c) Si assicura che il trattamento dei dati sia conforme ai requisiti legali e normativi in materia di protezione dei dati, anche nei contratti e nei progetti aziendali.
d) Contribuisce alla gestione e alla risoluzione degli incidenti di sicurezza che coinvolgono dati personali.
e) Tiene un registro delle attività di trattamento di dati personali come definito dalla legge sulla protezione dei dati per Assura SA, Assura-Basis SA e Figeas SA. Per quanto riguarda Assura-Basis SA, lo notifica all'Incaricato federale della protezione dei dati.
f) Garantisce che le richieste relative al trattamento di dati personali (ad esempio, diritto di accesso, diritto all'oblio, diritto alla portabilità, ecc.) siano trattate correttamente e che sia data risposta entro i termini stabiliti dalla legge.
g) Partecipa alla formazione dei collaboratori in materia di protezione dei dati.
h) È l'interlocutore principale dell'Incaricato federale della protezione dei dati e degli interessati dal trattamento.

i) Riferisce regolarmente alla Direzione generale sullo stato di conformità delle società del Gruppo Assura e presenta il monitoraggio dei piani d'azione messi in atto in caso di non conformità.
j) Assicura che il presente regolamento sia periodicamente aggiornato e rispettato all'interno del Gruppo Assura.

3.3 Chief Information Security Officer (CISO)

3.3.1 Il CISO è l'interlocutore principale per la Direzione generale e dei collaboratori del Gruppo Assura, così come per i partner, per quanto concerne in particolare la definizione di politiche e standard volti a garantire la sicurezza dell'informazione e dei sistemi d'informazione.
3.3.2 I suoi compiti sono definiti in modo più dettagliato in una direttiva.

3.4 Collaboratori

Tutti i collaboratori sono responsabili di trattare i dati conformemente alle regole e i principi definiti nel presente regolamento.

3.5 Proprietario dei dati

All'interno del Gruppo Assura, qualsiasi dato, inclusi i dati personali, deve avere un proprietario. Il proprietario del dato è la persona responsabile del suo trattamento. È compito suo garantire il corretto livello di classificazione come definito nel capitolo 7 qui di seguito e di aggiornarlo se necessario.

3.6 Dipartimento Clienti e Mercato

Il dipartimento Clienti e Mercato è proprietario dei dati trattati nell'ambito dell'acquisizione di nuovi clienti in previsione della sottoscrizione di contratti di assicurazione, così come dei dati relativi agli intermediari assicurativi.

3.7 Dipartimento Prestazioni

3.7.1 Responsabilità generale

3.7.1.1 Il Dipartimento Prestazioni è proprietario dei dati trattati nell'ambito della sottoscrizione di contratti di assicurazione, del rapporto con gli assicurati e in relazione al rimborso di prestazioni (corrispondenza con i fornitori di cure, garanzie, elaborazione di fatture, conteggi di prestazioni, ecc.).
3.7.1.2 Per il trattamento dei dati dei collaboratori assicurati presso società assicurative del Gruppo Assura si applicano disposizioni particolari.

3.7.2 Servizio Clienti

Il Servizio Clienti è responsabile di assicurare la protezione dei dati degli assicurati che tratta al momento dell'affiliazione, durante il rapporto contrattuale e alla partenza dell'assicurato.

3.7.3 Servizio del medico di fiducia e medico di fiducia

3.7.3.1 Il Servizio del medico di fiducia è responsabile della protezione dei dati medici degli assicurati trattati nell'ambito dei servizi medici (in particolare questionari sulla salute, perizie di esperti e rapporti medici).
3.7.3.2 Il medico di fiducia assicura il rispetto delle ulteriori misure di protezione e di sicurezza adottate riguardo alla sensibilità di tali dati.

3.7.4 Responsabilità nell'ambito della SwissDRG

I collaboratori delle cellule DRG rientrano in un'entità particolare, soggetta a certificazione in materia di protezione dei dati. Sono responsabili dei «minimal clinical dataset» (MCD, diagnosi principali e secondarie, nonché le procedure) il cui trattamento è regolato da specifiche istruzioni.

3.8 Dipartimento Finanze

Il Dipartimento Finanze è proprietario di tutti i dati finanziari delle società del Gruppo Assura, così come dei dati finanziari degli assicurati trattati in particolare nell'ambito della riscossione dei premi, del rimborso delle prestazioni (conti cliente, pagamenti, corrispondenza e informazioni in particolare nell'ambito di procedure esecutive, atti di carenza beni) e dei dati relativi all'assegnazione di sussidi.

3.9 Dipartimento Sviluppo e Marketing

Il Dipartimento Sviluppo e Marketing è proprietario dei dati che tratta a fini statistici o di reporting, di campagne di marketing o sondaggi tra i clienti per tutto il Gruppo Assura.

3.10 Settore Risorse Umane

Il Settore Risorse Umane è proprietario dei dati personali dei collaboratori, ad eccezione dei dati relativi al loro statuto di assicurati presso le società assicurative del Gruppo Assura (ad esempio, elaborazione di polizze e prestazioni), che sono trattati da collaboratori dedicati del Dipartimento Prestazioni.

3.11 Dipartimento Informatica

Il Dipartimento Informatica è proprietario dei dati di configurazione, di codice sorgente e dei segreti che consentono l'accesso alle infrastrutture IT. È inoltre responsabile dell'attuazione delle misure tecniche e organizzative relative alla sicurezza dei dati elettronici trattati dai diversi sistemi d'informazione utilizzati dal Gruppo Assura, i suoi collaboratori e partner (accessi, internet, e-mail, ecc.).

3.12 Incaricato federale della protezione dei dati e della trasparenza (IFPDT)

3.12.1 Competenza dell'IFPDT

3.12.1.1 L'IFPDT apre, d'ufficio o su denuncia, un'inchiesta nei confronti di un organo federale o di un privato se indizi sufficienti lasciano presumere che un trattamento di dati potrebbe violare le disposizioni sulla protezione dei dati. L'IFPDT può rinunciare ad aprire un'inchiesta se la violazione delle disposizioni sulla protezione dei dati è di poca importanza o se il titolare del trattamento ha adottato le misure adeguate a ristabilire una situazione conforme alla legge.

3.12.1.2 Se si apre una procedura d'inchiesta, il titolare del trattamento deve collaborare con l'IFPDT fornendogli le informazioni necessarie per l'inchiesta.

3.12.1.3 Se il titolare del trattamento non adempie al suo obbligo di collaborare e l'IFPDT constata che sono state violate le disposizioni sulla protezione dei dati, quest'ultimo può ordinare diversi provvedimenti amministrativi nei confronti del titolare del trattamento, come adeguare, cessare o sospendere del tutto o in parte il trattamento nonché cancellare o distruggere del tutto o in parte i dati. Può inoltre esigere che siano prese misure in materia di sicurezza o che gli interessati siano informati.

3.12.1.4 L'IFPDT non ha tuttavia il potere di infliggere multe o sanzioni penali al titolare del trattamento.

3.12.2 Sanzioni

3.12.2.1 Per i privati

A querela di parte, le autorità possono infliggere una multa fino a CHF 250'000 nei confronti della persona fisica colpevole, per omissione o intenzionalmente, di violazione del dovere di informare, di concedere l'accesso, di collaborare, dell'obbligo di diligenza e del segreto, nonché in caso di inosservanza a un'ingiunzione dell'IFPDT.

3.12.2.2 Per gli organi federali

È passibile della stessa multa di cui al precedente articolo 3.12.2.1 qualsiasi persona fisica all'interno dell'organo federale che, nell'ambito delle sue attività e in violazione del suo obbligo del segreto, divulghi intenzionalmente dati personali di cui è a conoscenza. L'obbligo di serbare il segreto continua anche dopo la cessazione dei rapporti di lavoro.

3.12.2.3 Se la determinazione della persona punibile all'interno dell'azienda esige provvedimenti d'inchiesta sproporzionati, l'azienda stessa è condannata al pagamento di una multa fino a CHF 50'000.

4. Obblighi del titolare del trattamento

4.1 Principi generali

4.1.1 Legittimità / legalità

4.1.1.1 Per i privati

Qualsiasi trattamento di dati personali deve essere legittimo, ossia non contravvenire a una disposizione legale imperativa volta alla protezione della personalità della persona fisica. In caso contrario, occorre fornire una giustificazione (ad esempio, il consenso) per effettuare il trattamento.

4.1.1.2 Per gli organi federali

Qualsiasi trattamento di dati personali si deve fondare su una base legale. In mancanza di una legge che autorizzi tale trattamento, occorre una giustificazione (ad esempio, il consenso).

4.1.2 Proporzionalità

4.1.2.1 Possono essere trattati solamente dati personali atti e oggettivamente necessari a soddisfare gli scopi del trattamento.

4.1.2.2 Il trattamento deve essere effettuato nel rispetto di un rapporto ragionevole tra lo scopo previsto e i mezzi utilizzati, preservando allo stesso tempo il più possibile i diritti degli interessati. Occorre esaminare sistematicamente se esiste un mezzo meno intrusivo per raggiungere lo scopo previsto.

4.1.3 Conservazione dei dati personali

I dati personali devono essere distrutti o resi anonimi appena non sono più necessari per lo scopo del trattamento, a meno che una base legale non ne esiga la conservazione.

4.1.4 Buona fede e trasparenza

4.1.4.1 Qualsiasi trattamento di dati personali deve essere effettuato in buona fede, ossia in conformità con lo scopo comunicato agli interessati al momento della raccolta o che risulta dalla legge o dalle circostanze. Nessun dato può essere trattato all'insaputa o contro la volontà dell'interessato.

4.1.4.2 Sia la raccolta che gli scopi del trattamento devono essere riconoscibili dall'interessato.

4.1.5 Scopo

4.1.5.1 Qualsiasi trattamento di dati personali deve rispettare lo scopo comunicato al momento della raccolta.

4.1.5.2 Qualsiasi altro nuovo trattamento deve rimanere compatibile con gli scopi comunicati all'interessato.

4.1.6 Esattezza

I dati personali trattati devono essere esatti e aggiornati nella misura in cui le circostanze lo consentono. Fatti salvi eventuali obblighi legali contrari, il titolare del trattamento adotta le misure appropriate per rettificare, cancellare o distruggere i dati inesatti o incompleti. A tal fine, tutti i collaboratori segnalano le inesattezze constatate nell'ambito delle loro attività.

4.1.7 Sicurezza dei dati personali

I dati personali trattati dal Gruppo Assura devono essere protetti da misure organizzative e tecniche appropriate in funzione del rischio che comportano (livello di classificazione) contro qualsiasi violazione interna o esterna della sicurezza dei dati.

Tali misure devono garantire la riservatezza, la disponibilità, l'integrità e la tracciabilità dei dati trattati.

4.2 Obbligo d'informare

4.2.1 Al momento della raccolta dei dati personali presso l'interessato o terzi, il titolare del trattamento fornisce all'interessato le informazioni necessarie affinché questo possa far valere i propri diritti di cui al capitolo 6 qui di seguito e sia garantito un trattamento trasparente. Fornisce almeno le informazioni seguenti:

a) l'identità e i dati di contatto del titolare del trattamento;
b) lo scopo del trattamento;
c) all'occorrenza, i destinatari o le categorie di destinatari cui sono comunicati i dati personali;
d) all'occorrenza, il nome dello Stato terzo in cui i dati personali sono comunicati e le relative garanzie.

4.2.2 Quando i dati personali sono raccolti presso terzi, l'interessato viene informato entro un mese dal ricevimento dei dati, a meno che non abbia dato preventivamente il suo consenso alla raccolta o se quest'ultima è giustificata da una base legale. In caso di comunicazione a terzi entro questo periodo, l'interessato deve essere informato al più tardi al momento di tale comunicazione.

4.2.3 Il titolare del trattamento è esentato, può limitare o differire la comunicazione delle informazioni in alcune situazioni previste dalla LPD, ad esempio se l'interessato è già in possesso delle informazioni, se il trattamento è previsto dalla legge o se lo richiedono gli interessi preponderanti di terzi.

4.2.4 L'obbligo di informazione si attua in particolare con la pubblicazione dell'informativa sul trattamento dei dati sul sito internet del Gruppo Assura e con la pubblicazione del registro del trattamento da parte dell'organo federale.

4.3 Decisione individuale automatizzata

4.3.1 Una decisione individuale automatizzata è una decisione presa nei confronti di una persona tramite algoritmi applicati ai suoi dati personali, senza che alcun essere umano intervenga nel processo.

4.3.2 L'interessato che è oggetto di tale decisione deve essere informato in anticipo e deve poter esprimere il proprio punto di vista. All'occorrenza, può richiedere che la decisione individuale automatizzata sia rivista da una persona fisica.

4.3.3 Questo obbligo non si applica se la decisione è presa in relazione alla conclusione o all'esecuzione di un contratto e la richiesta dell'interessato è pienamente soddisfatta o se l'interessato ha espressamente acconsentito all'adozione di questo tipo di decisione.

4.4 Comunicazione di dati all'estero

4.4.1 Principio

I dati personali possono essere comunicati all'estero in un Paese la cui legislazione presenta un livello adeguato secondo l'elenco stabilito dal Consiglio federale, ad esempio in un Paese dell'Unione europea.

4.4.2 Garanzie complementari

Se la legislazione del Paese in questione non presenta un livello adeguato, il titolare del trattamento deve adottare misure supplementari per garantire un livello di protezione appropriato, ad esempio adottando clausole contrattuali standard approvate dall'IFPDT o se l'interessato ha dato espressamente il proprio consenso. In questi casi, è necessario consultare preventivamente il consulente per la protezione dei dati e ottenere il suo consenso prima di comunicare dati in un Paese che non offre un livello di protezione adeguato.

4.5 Registro delle attività di trattamento

4.5.1 Assura-Basis SA, Assura SA, Figeas SA, e i loro subappaltatori (per i dati trattati per loro conto) devono tenere un registro di tutte le attività di trattamento. Il registro deve contenere almeno le seguenti informazioni:

a) l'identità del titolare del trattamento;
b) lo scopo del trattamento;
c) una descrizione delle categorie di interessati e dei dati trattati;
d) le categorie di destinatari;
e) la durata di conservazione dei dati o i criteri utilizzati per determinare tale durata;
f) una descrizione generale delle misure di sicurezza dei dati
g) se i dati personali sono comunicati all'estero, il nome dello Stato in questione e, all'occorrenza, le garanzie previste.

4.5.2 Il registro del trattamento deve essere aggiornato almeno una volta all'anno, ogni volta che viene effettuato un nuovo trattamento o ogni volta che si rende necessaria una modifica.

4.5.3 In quanto organo federale, Assura-Basis SA lo deve dichiarare all'IFPDT, che lo pubblica sulla sua piattaforma. Su richiesta, Assura SA e Figeas SA devono metterlo a disposizione dell'IFPDT.

4.6 Valutazione d'impatto

4.6.1 Principio

4.6.1.1 Per qualsiasi nuovo trattamento di dati personali che comporta un rischio elevato per gli interessati in particolare per quanto riguarda la natura dei dati trattati, lo scopo del trattamento o l'utilizzo di nuove tecnologie, il titolare del trattamento deve effettuare una valutazione d'impatto. Tale valutazione d'impatto deve essere effettuata almeno quattro mesi prima dell'attuazione del trattamento previsto in considerazione del termine indicato all'articolo 4.6.1.4 qui di seguito.

4.6.1.2 Per qualsiasi nuovo trattamento, il consulente per la protezione dei dati deve preventivamente essere consultato in modo da determinare se una valutazione d'impatto sia necessaria.

4.6.1.3 La valutazione d'impatto deve essere conservata per almeno due anni dopo la fine del trattamento.

4.6.1.4 Per gli organi federali

Non appena è previsto un nuovo trattamento dei dati da parte di un organo federale, una valutazione d'impatto deve imperativamente essere effettuata se le condizioni riportate all'articolo 4.6.1.1 di cui sopra sono soddisfatte.

Se la valutazione d'impatto rivela che, malgrado le misure previste, sussiste un rischio elevato per la personalità o i diritti fondamentali dell'interessato, l'IFPDT deve essere consultato entro tre mesi per determinare le azioni da intraprendere.

4.6.1.5 Per i privati

I titolare privato tenuto a effettuare il trattamento in virtù di un obbligo legale è esentato dall'obbligo di procedere a una valutazione d'impatto. In alcuni casi può rinunciare a una valutazione d'impatto, in particolare se si avvale di un sistema, un prodotto o un servizio che dispone di una certificazione.

Se è necessaria una valutazione d'impatto, si può rinunciare a sottoporla all'IFPDT se viene consultato il consulente per la protezione dei dati.

4.6.2 Contenuto minimo

La valutazione d'impatto deve contenere almeno:

a) una descrizione del trattamento previsto;
b) una valutazione dei rischi per la personalità o i diritti fondamentali dall'interessato;
c) i provvedimenti previsti per proteggere la sua personalità e i suoi diritti fondamentali.

4.7 Privacy by design/by default

4.7.1 Protezione dei dati a partire dalla progettazione (privacy by design)

Per qualsiasi nuovo progetto di creazione di prodotti o servizi che implicano un trattamento di dati personali, il titolare del trattamento deve predisporre, dalla concezione del progetto, le misure tecniche e organizzative adeguate affinché il trattamento rispetti i principi elencati all'articolo 4.1 di cui sopra.

4.7.2 Protezione dei dati by default (privacy by default)

Se nell'ambito di un servizio, di un software o di un dispositivo sono offerte più opzioni per il trattamento dei dati personali e l'interessato stesso può configurare tali opzioni, il titolare del trattamento assicura che il trattamento deve limitarsi a quanto strettamente necessario allo scopo

perseguito tramite il trattamento dei dati, a meno che l'interessato non abbia dato il suo consenso per un trattamento più ampio. A tal fine, il titolare del trattamento deve prevedere appropriate impostazioni predefinite.

4.8 Formazioni

Il titolare del trattamento deve assicurarsi che i collaboratori del Gruppo Assura siano regolarmente formati in materia di protezione dei dati.

5. Trattamento di dati personali da parte di un responsabile

5.1 Principio

5.1.1 Il titolare del trattamento può affidare il trattamento dei dati a terzi (a un'altra società del Gruppo Assura o a un fornitore di servizi esterno) purché siano soddisfatte le seguenti condizioni:

a) Il trattamento di dati personali da parte di un responsabile è previsto da un contratto scritto o dalla legge.
b) Il responsabile del trattamento effettua soltanto i trattamenti che il titolare del trattamento avrebbe il diritto di effettuare.
c) Nessun obbligo legale o contrattuale di serbare il segreto lo vieta.

5.1.2 Il titolare del trattamento rimane in ogni caso responsabile della protezione e della sicurezza dei dati il cui trattamento è affidato a terzi.

5.2 Modalità

5.2.1 Obblighi del titolare del trattamento

5.2.1.1 Il titolare del trattamento sceglie il responsabile del trattamento che offre garanzie sufficienti in materia di protezione dei diritti degli interessati (ad esempio, sulla base di una certificazione).

5.2.1.2 Al fine di garantire la protezione e la sicurezza dei dati trattati nell'ambito della missione attribuita al responsabile del trattamento, il titolare del trattamento gli fornisce istruzioni ad hoc.

5.2.1.3 Il titolare del trattamento deve assicurarsi tramite regolari controlli, almeno una volta all'anno, che il responsabile del trattamento tratti i dati conformemente alle sue istruzioni e al contratto.

5.2.1.4 In caso di trattamento di dati personali di una funzione essenziale o importante da parte di un responsabile, sono previsti requisiti supplementari in una direttiva pertinente.

5.2.2 Obblighi del responsabile del trattamento

5.2.2.1 Il responsabile del trattamento scelto dal titolare del trattamento deve poter garantire in qualsiasi momento che il trattamento dei dati che gli è stato affidato sia conforme ai requisiti in materia di sicurezza della protezione dei dati.

5.2.2.2 Il responsabile del trattamento può trattare i dati unicamente sulla base delle istruzioni ricevute da parte del titolare del trattamento e per conto di quest'ultimo.

5.2.2.3 Il responsabile del trattamento deve creare un registro del trattamento dei dati personali che tratta per il titolare del trattamento, conformemente all'articolo 4.5.1 di cui sopra.

5.2.2.4 Il responsabile del trattamento può delegare il trattamento dei dati a terzi solo previa autorizzazione del titolare del trattamento.

6. Diritti degli interessati da un trattamento dei dati da parte del Gruppo Assura.

6.1 Diritto d'accesso

6.1.1 Chiunque può richiedere al titolare del trattamento, per iscritto o per via elettronica, l'accesso a tutti i dati che lo riguardano trattati dal Gruppo Assura. In linea di principio, l'informazione è comunicata per iscritto, anche se è possibile un incontro di persona, previo accordo, con il titolare del trattamento.

6.1.2 Tale diritto può essere esercitato in qualsiasi momento, senza necessità di particolari motivazioni e gratuitamente, a meno che la comunicazione dell'informazione non comporti sforzi sproporzionati, nel qual caso potrà essere richiesta un'adeguata partecipazione ai costi.

6.1.3 Il titolare del trattamento può rifiutare, limitare o differire la comunicazione dell'informazione in determinati casi previsti dalla legge, in particolare se lo esigono gli interessi preponderanti di terzi o se la richiesta di accesso è manifestamente infondata o querulosa.

6.1.4 L'informazione deve essere comunicata entro 30 giorni dal ricevimento della richiesta. Se tale termine non può essere rispettato, il titolare del trattamento ne informa l'interessato entro lo stesso periodo di tempo, precisando entro quale termine sarà fornita l'informazione. In caso di rifiuto, di limitazione o di differimento, lo comunica entro gli stessi termini precisandone i motivi.

6.2 Diritto in caso di decisione individuale automatizzata

L'interessato da una decisione automatizzata secondo l'articolo 4.3.1 di cui sopra può esercitare il diritto di far riesaminare la decisione da una persona fisica.

6.3 Diritto alla portabilità

6.3.1 Chiunque può esigere che i dati personali che lo concernono e che ha comunicato al titolare del trattamento gli siano consegnati in un formato elettronico usuale.

6.3.2 Tale diritto di applica solamente se:

a) i dati sono trattati in modo automatizzato;
b) non lede terzi;
c) i dati sono trattati su base consensuale.

6.3.3 Dopo che il consulente per la protezione dei dati ha verificato la legittimità della richiesta, il richiedente riceve le informazioni in un formato strutturato usuale e leggibile da un computer, nella misura in cui ciò sia possibile dal punto di vista tecnico.

6.3.4 L'esercizio del diritto alla portabilità può essere rifiutato per i motivi indicati all'articolo 6.1.3 di cui sopra.

6.4 Diritto di opposizione

6.4.1 Chiunque sia interessato da un trattamento dei dati può, sulla base di un interesse degno di protezione reso verosimile, opporsi espressamente al trattamento di specifici dati personali da parte del titolare del trattamento.

6.4.2 Questo diritto di opposizione può essere rifiutato se:

a) il trattamento dei dati si basa su una base legale;
b) lo esigono interessi privati o pubblici preponderanti superiori agli interessi dell'interessato.

6.5 Diritto all'oblio

Chiunque sia interessato da un trattamento dei dati può richiedere al titolare del trattamento che i suoi dati personali siano cancellati o resi anonimi non appena l'uso dei dati non è più necessario per lo scopo perseguito, se questi sono inesatti o se il trattamento si basa sul consenso dell'interessato e questi decide di revocarlo.
All'esercizio di questo diritto si applicano le stesse limitazioni di cui all'articolo 6.4.2 di cui sopra.

6.6 Diritto di rettifica

Chiunque sia interessato da un trattamento dei dati può chiedere al titolare del trattamento di correggere o aggiornare dati inesatti o incompleti, a meno che la modifica non sia vietata dalla legge.
Se l'inesattezza di un dato personale non può essere accertata, l'interessato può chiedere al titolare del trattamento che si aggiunga al dato in questione una menzione che ne indichi il carattere contestato.

7. Principi di sicurezza dei dati

In materia di sicurezza dei dati, il Gruppo Assura ha stabilito una classificazione basata sulle seguenti quattro dimensioni: riservatezza, integrità, disponibilità e tracciabilità. Per ogni dimensione sono stati stabiliti quattro livelli di criticità. Per ognuno di questi livelli sono state definite misure di sicurezza specifiche.

7.1 Riservatezza

Il proprietario di ogni dato deve classificare i dati che tratta in base a uno dei quattro livelli di riservatezza stabiliti dal Gruppo Assura, ossia: «Pubblico», «Interno», «Riservato» e «Segreto».

7.1.1 Dati pubblici (livello 1)

I dati e i documenti con la classificazione «Pubblico» non contengono alcun dato personale e sono destinati ad essere diffusi e consultati liberamente al di fuori del Gruppo Assura senza che ciò arrechi danno al Gruppo Assura (esempi: rapporti del Gruppo, opuscoli di marketing). A questo livello non è necessario alcun meccanismo di protezione.

7.1.2 Dati interni (livello 2)

7.1.2.1 I dati e i documenti con la classificazione «Interno» sono destinati ad essere utilizzati unicamente all'interno del Gruppo Assura, oppure all'esterno ma in modo limitato e mirato, all'occorrenza con l'accordo del proprietario dei dati o del documento (esempi: organigrammi, regolamenti, direttive). La loro diffusione al di fuori del Gruppo può arrecare danno al Gruppo Assura o alle persone i cui dati sono trattati. Sono necessari meccanismi organizzativi e tecnici per limitarne l'accesso.

7.1.2.2 I dati e i documenti interni non possono contenere dati personali sensibili.

7.1.3 Dati riservati (livello 3)

7.1.3.1 I documenti con la classificazione «Riservato» sono destinati ad essere comunicati in modo controllato all'interno del Gruppo Assura (esempi: dati personali degli assicurati o dei collaboratori, dati finanziari, progetti aziendali). La loro diffusione al di fuori del Gruppo può arrecare un danno effettivo al Gruppo Assura o alle persone i cui dati sono trattati. La

cerchia di persone che hanno accesso a questo tipo di dati è nota, limitata e conforme ai principi derivanti dal presente regolamento.

7.1.3.2 I dati e i documenti senza una specifica classificazione sono da trattare come riservati.

7.1.4 Dati segreti (livello 4)

I dati e i documenti con la classificazione «Segreto» sono destinati ad essere comunicati in modo molto limitato all'interno del Gruppo Assura (esempi: dati medici degli assicurati o dei collaboratori, redditività dei prodotti, progetti di partenariato o contratti strategici). La loro diffusione al di fuori del Gruppo può arrecare un danno importante all'azienda. Non possono essere diffusi senza l'accordo scritto del loro proprietario. La cerchia di persone che hanno accesso a questo tipo di dati è molto limitata, nota e può essere fornita in qualsiasi momento.

7.2 Integrità

L'integrità consente di assicurare l'esattezza dei dati, ossia che dati o documenti non siano stati modificati o distrutti in modo non autorizzato. Il proprietario di ogni dato deve classificare i dati che tratta in base a uno dei seguenti quattro livelli d'integrità stabiliti dal Gruppo Assura:

7.2.1 Nessun vincolo di integrità (livello 1)

I dati e i documenti possono essere modificati o cancellati senza che ciò arrechi danno al Gruppo Assura o alle persone i cui dati sono trattati. A questo livello non è necessario alcun meccanismo di correzione.

7.2.2 Integrità standard (livello 2)

Le modifiche o le cancellazioni di dati e di documenti a questo livello arreca un danno limitato al Gruppo Assura o alle persone i cui dati sono trattati (perdita di tempo nel trattamento, necessità di riprendere un lavoro già svolto). Sono necessari meccanismi organizzativi e tecnici per limitare l'impatto di tali modifiche o cancellazioni.

7.2.3 Integrità rafforzata (livello 3)

Le modifiche o le cancellazioni di dati e di documenti a questo livello arreca un danno effettivo al Gruppo Assura o alle persone i cui dati sono trattati (sforzi significativi per correggere gli errori, impatto sull'immagine, rapporti deteriorati con clienti e partner). Sono necessari meccanismi organizzativi e tecnici per limitare modifiche o cancellazioni.

7.2.4 Integrità inalterabile (livello 4)

Le modifiche o le cancellazioni di dati e di documenti a questo livello arrecano un danno molto grave al Gruppo Assura o alle persone i cui dati sono trattati (sforzi considerevoli per correggere gli errori, forte impatto sull'immagine, deteriorazione duratura dei rapporti con clienti e partner, inosservanza di obblighi legali). Sono indispensabili meccanismi organizzativi e tecnici per impedire modifiche o cancellazioni. Qualsiasi modifica deve essere soggetta ad audit dettagliati.

7.3 Disponibilità

Con «disponibilità» si intende un accesso in qualsiasi momento ai dati necessari per svolgere attività attraverso applicazioni dedicate. La strategia di continuità operativa descrive i processi chiave e le applicazioni che li supportano. Istruzioni ad hoc sulla gestione dei rischi definiscono cinque livelli di criticità in materia di impatto: severo, grave, moderato, secondario e insignificante. Per ognuno di questi livelli è descritta una durata massima ammissibile degli aspetti deficitari, così come le misure correttive.

7.4 Tracciabilità

La tracciabilità consente di identificare qualsiasi accesso non autorizzato e di determinare l'origine di un incidente sulla base di una registrazione. Quest'ultima permette di stabilire in particolare chi ha avuto accesso ai dati, se è stato effettuato un trattamento e quando è stata apportata un'eventuale modifica dei dati. Il proprietario di ogni dato deve classificare i dati che tratta in base a uno dei seguenti quattro livelli di tracciabilità stabiliti dal Gruppo Assura:

7.4.1 Nessuna tracciabilità (livello 1)

L'assenza di traccia relativa al dato o al trattamento non arreca alcun danno all'azienda o alle persone i cui dati sono trattati. A questo livello non è necessaria alcuna misura.

7.4.2 Tracciabilità standard (livello 2)

L'assenza di traccia a questo livello arreca un danno limitato all'attività e/o alla conformità dell'azienda. Le procedure interne dell'azienda e i vincoli normativi impongono la conservazione di una traccia minima dell'accesso al dato o dell'esecuzione del trattamento (chi ha avuto accesso al dato, a che ora e a quale sistema d'informazione).

7.4.3 Tracciabilità dettagliata (livello 3)

L'assenza di traccia a questo livello arreca un danno effettivo all'attività e/o alla conformità dell'azienda. Le procedure interne dell'azienda e i vincoli normativi impongono la conservazione di una traccia dettagliata dell'accesso al dato o dell'esecuzione del trattamento (chi ha avuto accesso al dato, a quale dato, a che ora, a quale sistema d'informazione e la natura del trattamento).

7.4.4 Tracciabilità completa (livello 4)

L'assenza di traccia a questo livello arreca un danno molto grave all'attività e/o alla conformità dell'azienda. Le procedure interne dell'azienda e i vincoli normativi impongono la conservazione di una traccia completa dell'accesso al dato o dell'esecuzione del trattamento (chi ha avuto accesso al dato, a quale dato, a che ora, a quale sistema d'informazione, la natura del trattamento e lo stato del dato prima e dopo l'accesso).

8. Misure generali atte a garantire la protezione dei dati

8.1 Misure inerenti ai dati fisici

Per garantire la sicurezza e la protezione dei dati fisici all'interno del Gruppo Assura, i collaboratori devono rispettare i seguenti principi:

a) *Accesso agli edifici:* solo i collaboratori che dispongono di un badge sono autorizzati ad accedere ai locali del Gruppo Assura. È vietato consegnare il badge a terzi.
b) *Clear desk policy*: i supporti fisici che contengono dati riservati devono essere conservati in luoghi chiusi a chiave (scrivanie, armadi).
c) *Posta interna:* le buste che contengono dati riservati o segreti devono essere chiuse e riportare l'indicazione «Riservato».
d) *Distruzione di documenti*: i documenti cartacei che contengono dati riservati o segreti, così come i documenti interni che contengono dati personali, devono essere eliminati con un distruggi documenti.
e) *Distribuzione di documenti*: la distribuzione dei documenti cartacei all'interno e al di fuori del Gruppo Assura deve essere mirata, limitata e basata sul principio di proporzionalità.
f) *Conservazione di documenti:* i documenti cartacei devono essere archiviati all'interno del Gruppo Assura e devono essere conservati e distrutti in conformità con la relativa direttiva interna.

8.2 Misure inerenti ai dati in formato elettronico

La protezione dei dati in formato elettronico all'interno del Gruppo Assura si basa sui seguenti principi:
a) L'accesso ai sistemi d'informazione del Gruppo Assura impone un'autenticazione e un'autorizzazione sistematica di ogni utente (nome utente e password necessari). Questi vengono aggiornati regolarmente nel tempo in base ad istruzioni ad hoc.
b) I diritti d'accesso ai sistemi d'informazione sono attribuiti sulla base di ruoli aziendali definiti dai diversi settori specialistici. Le eccezioni sono giustificate, valutate e controllate regolarmente dai manager e dal responsabile dell'applicazione aziendale. I diritti d'accesso sono riesaminati ogni anno.
c) I dati vengono crittografati a riposo e in transito.
d) Per gli accessi informatici più sensibili può essere necessaria un'autenticazione forte.
e) I dati elettronici devono essere archiviati ed eliminati in conformità con la relativa direttiva interna.
f) I dati e le informazioni sono cancellati dai dispositivi informatici prima che questi vengano riciclati.
g) Si attuano misure e soluzioni tecniche per lottare contro la perdita, il furto e la fuga di dati, nonché contro le minacce cibernetiche.

9 Disposizioni finali

Il presente regolamento è stato adottato dal Consiglio di amministrazione il 5 luglio 2023 ed entra in vigore il 1° settembre 2023. Sostituisce e annulla il «Regolamento inerente al trattamento dei dati» del 1° luglio 2016.