MANUALE
SISTEMA DI GESTIONE DELLA PROTEZIONE DEI DATI PERSONALI

Rev.	Data	Descrizione	Redazione	Verifica ed Approvazione
00	01.09.2023	Prima emissione	Referente Privacy	Direzione

REVISIONI

REV.	DATA	DESCRIZIONE
00	**01.09.2023**	Prima emissione
01	31.08.2024	Seconda emissione

INDICE

1 INTRODUZIONE

1.1 Scopo

Il presente documento rappresenta il quadro di riferimento delle politiche, regole e linee guida di Unitas Associazione ciechi e ipovedenti della Svizzera italiana (di seguito anche Organizzazione), per l'attuazione e mantenimento del proprio sistema di gestione della privacy e della sicurezza dei dati personali trattati, in conformità con la Legge cantonale sulla Protezione dei Dati Personali (LPDP) e ai requisiti della Legge federale sulla Protezione dei Dati (LPD) che siano applicabili all'Organizzazione.

1.2 Campo di applicazione

Le indicazioni qui riportate si applicano a tutte le risorse e processi dell'Organizzazione interessati dal trattamento di dati personali e devono essere rispettate da tutti i dipendenti, consulenti, aziende esterne e fornitori, coinvolti nel trattamento di dati personali.

1.3 Riferimenti normativi

Le indicazioni qui riportate fanno riferimento alle seguenti normative.

Normative
Legge cantonale sulla Protezione dei Dati Personali (LPDP)
Legge federale sulla Protezione dei Dati (LPD)

1.4 Gestione documento

Questo documento è stato redatto da Referente Privacy ed approvato dalla Direzione (come indicato nella tabella in fondo alla prima pagina).

La Direzione è responsabile dell'aggiornamento del documento ogni volta che le circostanze lo richiedono e, in ogni caso, ne verifica l'adeguatezza periodicamente, con il supporto del Referente Privacy.

La distribuzione interna di questo documento è a cura del Referente Privacy.

1.5 Definizioni e abbreviazioni

Per "*titolare*" del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Per "*responsabile*" del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Per "*interessato*": la persona fisica identificata o identificabile, direttamente o indirettamente.

Per "*terzo*": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Per "*destinatario*": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazioni di dati personali, che si tratti o meno di terzi.

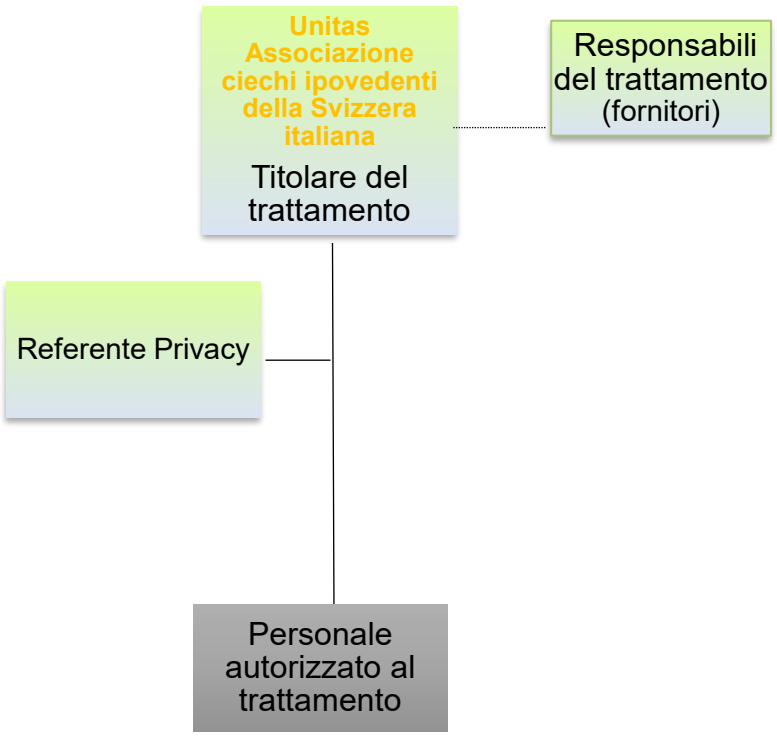
Per "*trattamento*" dei dati s'intende qualunque operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione la cancellazione o la distruzione.

Per "*dato personale*" s'intende qualunque informazione relativa a persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo, come il nome, un numero di identificazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Per "*Dati particolari*": i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona.

2 ORGANIGRAMMA PRIVACY

Di seguito i principali ruoli coinvolti nella gestione della privacy e della protezione dei dati personali.



2.1 Titolare del trattamento di dati

Il Titolare del trattamento (ossia la persona giuridica XYZ, rappresentata dalla Direzione) determina le finalità e i mezzi del trattamento dei dati personali.

UNITAS - Associazione ciechi e ipovedenti della Svizzera italiana

in qualità di Titolare del trattamento:

- decide sulle finalità del trattamento, sui mezzi e sul profilo delle misure di sicurezza;
- garantisce l'analisi dei rischi di sicurezza dei dati personali, identificando le principali criticità a livello organizzativo, di processo e tecnologico, la definizione e realizzazione del "Piano delle misure di sicurezza dei dati personali" (vedere cap. 3.3.)
- programma le misure di sicurezza tecniche ed organizzative adeguate, per garantire che il trattamento effettuato sia conforme alle normative;
- garantisce adeguata formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo (vedere cap. 5.3)
- nel caso di violazione dei dati pone in essere misure effettive e tempestive e procede, se necessario, alla notifica all'Autorità competente e alla comunicazione all'interessato;
- sorveglia sull'osservanza della normativa applicabile, delle regole e altre disposizioni interne relative alla protezione dei dati
- garantisce adeguata predisposizione, aggiornamento e verifica del corpo documentale del sistema di gestione della privacy e della protezione di dati.

Il Titolare del trattamento designa:

- il Referente Privacy
- (eventualmente) il "Consulente per la protezione dei dati personali" (così come definito dalla normativa)
- i Responsabili/Mandatari del trattamento (fornitori) a cui affida operazioni di trattamento in outsourcing;
- tra il personale dipendente e collaboratori, le persone incaricate delle operazioni di trattamento ("Autorizzati al trattamento").

2.2 Referente Privacy

Il Referente Privacy:

- informa, indirizza e fornisce consulenza all'interno dell'Organizzazione, sugli obblighi derivanti dal presente Manuale, sulle novità normative in materia di protezione dei dati personali e altre disposizioni

- supporta l'analisi dei rischi di sicurezza dei dati personali, la definizione ed il coordinamento della realizzazione del "Piano delle misure di sicurezza dei dati personali"
- coordina e supporta le attività di predisposizione, aggiornamento e verifica del corpo documentale del sistema di gestione della privacy e della protezione di dati
- verifica prima di ogni nuovo trattamento se necessario eseguire la Valutazione d'impatto sulla protezione dei dati (VIPD) e, ove necessario, ne supporta lo svolgimento (vedere cap. 3.10)
- supporta la gestione delle richieste degli interessati al trattamento (vedere cap. 3.9);
- supporta la gestione delle notifiche all'Incaricato cantonale della protezione dei dati e agli interessati nel caso di violazione dei dati personali (vedere cap. 3.11).
- si avvale della collaborazione dei responsabili dell'Organizzazione, ognuno in base alla propria area di competenza per:
    - verificare se i trattamenti sono svolti in conformità ai requisiti applicabili
    - valutare la conformità di ogni nuova finalità di trattamento dei dati personali, ovvero di ogni variazione delle finalità e delle modalità dei trattamenti esistenti;
    - analizzare l'evoluzione degli scenari di rischio in materia di protezione dei dati personali.

2.3 Personale autorizzato al trattamento di dati

Ogni dipendente e collaboratore dell'Organizzazione, preposto ad un determinato servizio che implichi il trattamento di dati personali, deve essere autorizzato ed istruito all'applicazione delle normative, regolamenti, procedure e misure che garantiscono il rispetto della privacy e la protezione dei dati personali.

Tali normative, procedure e misure garantiscono, in particolare, che i dati personali siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime;
- adeguati, pertinenti e limitati a quanto necessari rispetto alle finalità per i quali sono trattati;
- esatti, e se necessario aggiornati;
- conservati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- trattati nella massima sicurezza, al fine di evitare trattamenti non autorizzati o illeciti, perdita dei dati, danni accidentali.

2.4 Responsabili esterni del trattamento di dati

I Responsabili esterni del trattamento sono coloro che trattano i dati personali per conto dell'Organizzazione (es. fornitori di servizi informatici, società di servizi, ecc.).

Qualora Unitas Associazione ciechi e ipovedenti della Svizzera italiana dovessero affidare a enti/società terze processi/servizi che comportino il trattamento di dati personali, tale ente/società assume il ruolo di "Responsabile del trattamento" (come indicato dalle normative).

Unitas Associazioni ciechi e ipovedenti della Svizzera italiana garantisce la scelta di tali fornitori, che devono presentare garanzie sufficienti di conoscenza specialistica, affidabilità e risorse; inoltre, sottoscrive con essi un accordo/mandato formale per specificare le responsabilità della messa in atto delle misure tecniche ed organizzative necessarie al rispetto dei requisiti normativi e alla sicurezza dei dati.

2.5 Consulente per la protezione dei dati (se nominato)

Il Titolare del trattamento può avvalersi di un "Consulente per la protezione dei dati", interno o esterno all'Organizzazione.
Il Consulente, qualora nominato, viene individuato sulla base delle competenze professionali e personali, e opera secondo le indicazioni normative e le buone pratiche previste per il suo ruolo.

In particolare, tra i compiti del Consulente per la protezione dei dati, vi sono:

- rilevare le novità normative in materia di protezione dei dati personali e informarne l'Organizzazione
- fornire consulenza all'Organizzazione, in materia di privacy e protezione dei dati
- favorire la sensibilizzazione alla sicurezza dei dati e la formazione del personale
- sorvegliare sull'osservanza delle normative applicabili e altre disposizioni relative alla protezione dei dati
- collaborare con il Referente Privacy per garantire l'adeguato governo del Sistema di gestione della privacy e protezione dei dati
- se richiesto
  - supportare l'analisi dei rischi di sicurezza dei dati personali
  - supportare lo svolgimento della Valutazione d'impatto sulla protezione dei dati (VIPD)
  - supportare la gestione delle richieste degli interessati
  - supportare la notifica all'Incaricato cantonale della protezione dei dati in caso di violazione dei dati
  - fornire supporto di competenza in materia di privacy e sicurezza dei dati in caso di progetti di cambiamento e sviluppo dei processi e/o sistemi informatici dell'Organizzazione che interessano i dati personali (per l'applicazione dei principi Privacy by design e Privacy by default, previsti dalle normative).

3 PRINCIPI, DIRITTI E REQUISITI

3.1 Principi e base giuridica del trattamento

Unitas Associazione ciechi e ipovedenti della Svizzera italiana definisce ed implementa un adeguato sistema di gestione della privacy e protezione dei dati personali, nel rispetto dei principi e requisiti normativi e dei diritti e della personalità degli interessati.

Il Referente Privacy supporta il Titolare nel rispetto di tali principi e requisiti.

Tra questi si evidenzia in particolare che i dati personali devono essere (così come previsto dalle normative in materia):

- trattati in modo lecito, corretto e trasparente;
- acquisiti e trattati su idonea e pertinente base giuridica per scopi determinati, espliciti e legittimi;
- trattati solo per le finalità proprie dell'Organizzazione e in maniera non eccedente le predette finalità;
- trattati nel rispetto dei diritti e della personalità degli interessati;
- protetti dal rischio, anche solo potenziale, di distruzione, perdita, modificazione, rivelazione non autorizzata, accesso non autorizzato, non esattezza e non adeguatezza rispetto alle finalità per cui sono trattati.

3.2 Diritti dell'Interessato

Unitas Associazione ciechi e ipovedenti della Svizzera italiana garantisce l'effettivo esercizio dei diritti da parte dell'interessato relativamente ai trattamenti di dati di cui è Titolare.

Ai sensi della normativa, il soggetto interessato, a cui si riferiscono i dati, ha il diritto di ottenere l'accesso ai dati personali ed informazioni in relazione a:

- le finalità per cui i dati sono trattati;
- le categorie dei dati trattati;
- il periodo di conservazione dei dati;
- i destinatari dei dati personali;
- la logica cui risponde qualsiasi trattamento automatizzato di dati.

Inoltre, l'interessato ha il diritto di chiedere:

- rettifica;
- cancellazione ("diritto all'oblio");
- limitazione al trattamento;
- portabilità dei dati;
- opposizione;
- proporre reclamo ad un'Autorità di controllo.

La procedura "Gestione richieste degli interessati" riporta le fasi per rispondere alle richieste provenienti dagli interessati (vedi capitolo 3.9).

Si ricorda inoltre che qualora Unitas Associazioni ciechi e ipovedenti della Svizzera italiana intenda utilizzare i dati raccolti per una finalità diversa da quella per cui sono stati ottenuti, prima di procedere con l'ulteriore trattamento, deve fornire all'interessato informazioni in merito a tale diversa finalità e raccogliere, qualora necessario, il dovuto consenso.

3.3 Registro dei trattamenti e degli archivi di dati

Le principali informazioni necessarie per definire l'ambito di applicazione delle normative in materia di protezione dei dati e per predisporre i necessari provvedimenti per la conformità ai requisiti normativi sono riportate nel "Registro dei trattamenti". Tra queste informazioni anche quelle che riguardano gli archivi dei dati.

Il Titolare del trattamento garantisce la predisposizione ed il continuo aggiornamento del "Registro dei Trattamenti" e del "Registro degli Archivi di Dati".

L'aggiornamento è necessario a fronte di nuovi trattamenti introdotti, da nuovi progetti o modifiche ai processi e/o ai sistemi informatici, modifiche di tipo normativo o regolamentare in materia di protezione dei dati.

Il Referente Privacy coordina l'aggiornamento dei Registri.

3.4 Informative e Consensi

I dati personali possono essere raccolti e trattati al ricorrere di una delle seguenti circostanze:

- l'interessato ha espresso il consenso al trattamento dei dati personali per una o più specifiche finalità;
- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte;
- il trattamento è necessario per adempiere un obbligo legale dell'Organizzazione;
- il trattamento è necessario per il perseguimento di un interesse preponderante del titolare del trattamento.

Nel caso di dati particolari che rivelino: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito in presenza delle seguenti basi giuridiche:

- consenso prestato dall'interessato, purché si tratti di consenso espresso e per una o più finalità specifiche;
- il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per accertare, esercitare o difendere un diritto dell'Organizzazione in sede giudiziaria;
- il trattamento è necessario per motivi di interesse pubblico rilevante;
- il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale.

L'Organizzazione fornisce l'informativa agli interessati al momento del primo utilizzo dei loro dati.

L'informativa è lo strumento che rende esplicita e trasparente la gestione dei dati degli interessati, al fine di consentire agli stessi soggetti di prendere parte attiva alla difesa dei propri diritti nell'ambito della protezione dei dati personali.

Gli interessati vengono informati per iscritto tramite idonea informativa (come indicato dalla normativa) su:

- l'identità e i dati di contatto del titolare del trattamento;
- le finalità del trattamento nonché la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- qualora il trattamento sia basato sul consenso dell'interessato, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo a un'autorità di controllo;

- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora necessario per specifiche finalità di trattamento, Unitas Associazione ciechi e ipovedenti della Svizzera italiana garantisce l'acquisizione del consenso da parte degli interessati. Il consenso deve essere precedente all'inizio del trattamento e deve essere somministrato una volta sola. Si richiederà un nuovo consenso solo se cambiano le finalità del trattamento.

L'interessato ha il diritto di revocare in ogni momento il consenso prestato. In questo caso Unitas Associazioni ciechi e ipovedenti della Svizzera italiana ha l'obbligo di cancellare i dati o trasformarli in forma anonima, a meno che il trattamento non faccia riferimento ad altra base giuridica.

3.5 Privacy policy e cookie policy del Sito web

Al fine di informare correttamente i visitatori del sito web di Unitas Associazione ciechi e ipovedenti della Svizzera italiana, devono essere definite e pubblicate:

- l'informativa privacy (c.d. "privacy policy")
- la cookie policy.

3.6 Tempi di conservazione dei dati

Uno dei principi base della normativa sulla protezione dei dati, riguarda i tempi di conservazione dei dati.

Il tempo di conservazione di un dato personale è legato alla finalità del trattamento: se lo stesso dato è trattato per diverse finalità, si devono stabilire tempi diversi di conservazione in funzione di ognuna di esse.

Al termine del tempo di conservazione stabilito, i file/documenti contenenti i suddetti dati personali devono essere distrutti, o i dati resi anonimi.

Nel Registro dei Trattamenti sono indicati i tempi e i criteri di conservazione dei dati personali, in conformità alle leggi ed ai regolamenti vigenti.

3.7 Privacy by design e Privacy by default

Unitas Associazioni ciechi e ipovedenti della Svizzera italiana garantisce l'applicazione dei principi di Privacy by Design e Privacy by Default. In caso di cambiamento e sviluppo di processi e/o sistemi informatici che trattano dati personali, tali principi vengono adottati, attraverso la preliminare definizione e la successiva implementazione di meccanismi e misure di sicurezza e protezione dei dati.

Inoltre, i dati personali trattati devono essere pertinenti, adeguati e limitati rispetto alle finalità ("*minimizzazione dei dati*"); deve essere minimizzata la quantità dei dati raccolti quanto più possibile, e limitata ai dati strettamente necessari alle finalità predeterminate.

La "*minimizzazione"* si estende anche alla configurazione dei software e dei sistemi informativi utilizzati per trattare i dati personali in modo da ridurre al minimo il loro uso (*data protection by design*); nonché allo sviluppo di tecnologie e/o processi con l'obiettivo di raccogliere ed elaborare solo i dati personali strettamente necessari per consentire all'interessato di fruire delle funzionalità richieste assicurando by default un trattamento legittimo (*data protection by default*).

Nella fase di analisi di un nuovo progetto o di un cambiamento di processi/sistemi deve essere coinvolto il Referente Privacy, ogni qualvolta ci sia un trattamento di dati personali.

Le procedure di gestione dei cambiamenti e sviluppi organizzativi e informatici di Unitas Associazioni ciechi e ipovedenti della Svizzera italiana riportano le fasi e attività che consentono di applicare i principi Privacy by Design e Privacy by Default.

3.8 Stato della tecnica e buone pratiche

I provvedimenti per il rispetto dei requisiti normativi e le misure di sicurezza dei dati devono essere definiti ed implementati, in base alla natura dei dati trattati e alle specifiche caratteristiche del trattamento, tenendo conto delle conoscenze acquisite in base al progresso tecnologico e alle buone pratiche consolidate, in modo da rispettare i requisiti normativi e ridurre al minimo i rischi di sicurezza dei dati.

3.9 Gestione richieste degli interessati

Le normative sulla protezione dei dati personali richiedono specificamente che, in caso di richieste da parte degli interessati di cui il Titolare tratta dati personali, basate sull'esercizio dei diritti in merito al trattamento dei propri dati personali, devono essere applicate specifiche modalità e rispettati specifici tempi nell'erogazione della risposta alla richiesta e nella gestione delle comunicazioni con l'interessato.

La "Procedura Gestione Richieste Interessati" riporta le modalità e responsabilità di gestione della risposta e delle comunicazioni con l'interessato, in conformità ai requisiti indicati dalle normative in materia.

3.10 Valutazione di impatto sulla protezione dei dati (VIPD)

Le normative sulla protezione di dati richiedono specificamente che, in caso di trattamenti che possano comportare elevati rischi sui diritti e le libertà individuali, deve essere effettuata una valutazione di impatto sulla protezione dei dati.

La "Procedura Valutazione di Impatto sulla Protezione dei Dati" riporta le modalità e responsabilità di svolgimento di tale valutazione, in conformità ai requisiti indicati dalle normative in materia.

3.11 Gestione e notifica della violazione dei dati personali

La violazione dei dati personali che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, non si limita alla sola perdita di riservatezza, ma anche al danneggiamento e/o alla non disponibilità dei dati.

La gestione delle violazioni dei dati personali prevedono le seguenti attività principali:

- rilevare la natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati, le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- valutare le probabili conseguenze della violazione dei dati personali;
- individuare le misure necessarie per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
- notificare quanto prima la violazione all'Autorità di controllo competente dal momento in cui se ne è venuti a conoscenza.

La "Procedura Gestione Violazione Dati" riporta le fasi di gestione, in conformità ai requisiti indicati dalle normative in materia.

4 ATTIVITA' DEL PROCESSO DI GOVERNO

Al fine di garantire un adeguato livello di sicurezza dei dati personali trattati da Unitas Associazioni ciechi e ipovedenti della Svizzera italiana, è stato definito e viene applicato un processo ciclico di Governo del Sistema di Protezione dei Dati Personali che prevede le seguenti attività.

4.1 Rilevazione, analisi e applicazione delle novità normative

Il Referente Privacy rileva, periodicamente, le novità sul quadro normativo in materia di protezione dei dati personali (qualora l'Organizzazione si avvalga di un Consulente per la protezione dei dati personali, sarà compito del professionista rilevare le novità normative).

Per tale attività il Referente Privacy può avvalersi di:

- periodica consultazione di appropriati siti Internet;
- informazioni su periodici e riviste del settore;
- comunicazioni dell'Incaricato cantonale della protezione dei dati;
- consulenti esterni.

A fronte di novità normative che interessano l'Organizzazione, il Referente Privacy coordina le attività di analisi, valutazione e definizione dei nuovi provvedimenti e misure da adottare, per il rispetto delle stesse.

Tali nuovi interventi vengono dal Referente Privacy inseriti nel Piano complessivo delle azioni di miglioramento del sistema di gestione privacy ("Piano Azioni Privacy").

4.2 Valutazione del rischio per la sicurezza dei dati personali

La valutazione del rischio per la sicurezza dei dati personali è garantita dal Titolare che si avvale della collaborazione del Referente Privacy e coinvolge i responsabili dei diversi settori/aree.

La valutazione del rischio viene svolta periodicamente con cadenza annuale e, se necessario, in particolari occasioni, eventualmente suggerite dai responsabili dei diversi settori/aree.

In particolare, la valutazione del rischio prevede:

- la valutazione del livello degli impatti che una possibile perdita di sicurezza dei dati personali (perdita di riservatezza e/o integrità e/o disponibilità del dato personale) potrebbe avere sui diritti e sulle libertà fondamentali degli interessati;
- la valutazione della probabilità di accadimento delle minacce alla sicurezza dei dati personali in relazione alle caratteristiche dell'ambiente analizzato;
- la valutazione del livello di "adeguatezza" delle misure di sicurezza (tecniche ed organizzative) implementate, capaci di contrastare e gestire i rischi.

La valutazione del rischio è effettuata facendo riferimento alla metodologia sviluppata (vedi documento "Metodologia di valutazione dei rischi").

4.3 Definizione delle misure di sicurezza dei dati personali

Attraverso la valutazione dei rischi e del livello di adeguatezza delle misure di sicurezza attualmente applicate, viene individuato il Piano delle iniziative di mitigazione dei rischi.

La definizione del Piano di mitigazione dei rischi e l'accettazione dei livelli di rischio residuo (a valle dell'implementazione delle misure di sicurezza) sono di responsabilità del Titolare.

Le nuove iniziative di mitigazione dei rischi vengono dal Referente Privacy inserite nel Piano complessivo delle azioni di miglioramento del sistema di gestione privacy ("Piano Azioni Privacy").

4.4 Realizzazione del “Piano Azioni Privacy”

Il Referente Privacy coordina le attività di realizzazione e controllo del “Piano Azioni Privacy”.

4.5 Piano di formazione e sensibilizzazione del personale

Al fine di garantire un buon livello di sicurezza dei dati personali, tutte le persone che trattano dati personali devono essere sensibilizzate alla sicurezza e formate affinché svolgano correttamente le attività di competenza adottando comportamenti “sicuri”.

Il Titolare, con il supporto del Referente Privacy, definisce ed aggiorna periodicamente (almeno una volta all’anno) il “Piano di Formazione Privacy”, che viene integrato nel complessivo “Piano Azioni Privacy”.

4.6 Monitoraggio e controllo del Sistema Gestione Privacy

Il Titolare, con il supporto del Referente Privacy (e se nominato del Consulente per la protezione dei dati), garantisce la verifica e il controllo periodico dell’adeguatezza e dell’aggiornamento del sistema di gestione della protezione dei dati personali.

Il Referente Privacy coordina l’esecuzione di opportune misurazioni e azioni di controllo del sistema di gestione della privacy e ne riporta i risultati al Titolare.

4.7 Documentazione del Sistema Gestione Privacy

È stato definito il “Modello” della documentazione del Sistema Gestione Privacy (vedi Allegato A).

Il Referente Privacy coordina la verifica e l’aggiornamento dei documenti del sistema di gestione della privacy e l’eventuale necessità di sviluppo, integrazione e aggiornamento del Modello.

5 ALLEGATO A: MODELLO DOCUMENTAZIONE PRIVACY ATTIVA IN UNITAS

AREA	*DOCUMENTO*	*UTILIZZO*
MODULISTICA E CONTRATTI	REG001: Registro dei Trattamenti e degli Archivi di Dati	Interno
	REG002: Informativa residenti	Informativa
	REG003: Informativa familiari/rappresentanti	Informativa
	REG004: Informativa dipendenti	Informativa
	REG005: Informativa collaboratori esterni	Informativa
	REG006: Informativa stagisti	Informativa
	REG007: Informativa apprendisti	Informativa
	REG002a-REG002b (c.t.. soci, residenti) REG003a-REG004a (c.t.. soci, dipendenti) REG006a-REG007a (c.t.. dipendenti)	Consenso (firma)
	REG-010: Dichiarazione Impegno Protezione Dati	Consenso (firma)
	REG-011: Nomina IT Administrator interno	Interno
	REG-012: Accordo di riservatezza (Non Disclosure Agreement - NDA)	Consenso (firma)
	REG-013: Privacy e Cookie Policy	Informativa
	REG-014a: Accordo sui requisiti di sicurezza del fornitore	Consenso (firma)
GESTIONE RISCHI	RSK-001: Metodologia di valutazione dei rischi	Interno
	RSK-002: Rapporto valutazione rischi	Interno
MISURE SICUREZZA	MS-001 Linee Guida Sicurezza Dati	Interno
	IT-001: Procedura Gestione Accessi Logici	Procedura
	IT-002: Procedura Gestione Asset	Procedura
	IT-003: Procedura Gestione LOG	Procedura
	IT-004: Procedura Gestione Change	Procedura
	IT-005: Procedura Gestione Backup IT	Procedura
	IT-006: Procedura Gestione Fornitori IT	Procedura
	IT-007: Procedura Gestione Incidenti IT	Procedura
	IT-008: IT Disaster Recovery Plan	Procedura
	FIS-001: Procedura Gestione Accessi Fisici	Procedura
GOVERNANCE	GOV-001: Manuale sistema di protezione dei dati personali	Informativa
	GOV-002: Regolamento Informatico	Informativa
	GOV-003: Procedura Valutazione Impatto Protezione Dati (VIPD)	Procedura
	GOV-004: Procedura Notifica Violazione Sicurezza Dati (Data Breach)	Procedura
	GOV-005: Procedura Gestione Richieste Interessati	Procedura
	GOV-006: Business Continuity Plan	