ARTISET

Guida all'implementazione della protezione dei dati

Misure da adottare da parte delle istituzioni e strutture per le persone bisognose di sostegno

1. Introduzione

In vista dell'entrata in vigore della revisione totale della Legge federale sulla protezione dei dati (LPD) il 1° settembre 2023, molte aziende e organizzazioni devono adottare determinate misure tecniche e organizzative per soddisfare i relativi requisiti, ora più severi. Questa guida è pensata per condurre nel processo di attuazione le istituzioni e le strutture che accompagnano persone bisognose di assistenza

Tutte le disposizioni delle leggi e ordinanze sulla protezione dei dati indicate in questo documento si riferiscono alle versioni riviste di questi testi, che entrano in vigore il 1° settembre 2023:

- Nuova Legge federale sulla protezione dei dati («LPD»)
- Nuova Ordinanza sulla protezione dei dati («OPDa»)

Il termine «istituti» utilizzato in questo documento si riferisce a istituzioni e strutture per persone con bisogni di assistenza (persone anziane, persone in situazione di disabilità, bambini e adolescenti con bisogni particolari).

2. Punto della situazione

Per prima cosa, gli istituti dovrebbero fare il **punto della situazione attuale delle loro raccolte e collezioni di dati**. Sul sito web della federazione ARTISET è disponibile un'apposita **lista di controllo** pensata per facilitare loro questo compito. L'obiettivo è ottenere una visione d'insieme del tipo e dell'entità degli interventi cui gli istituti dovranno provvedere per garantire la protezione dei dati.

3. Piano per la protezione dei dati

È consigliabile mettere a punto un concetto sulla base del modello **Piano per la protezione dei dati** messo a disposizione da ARTISET. Si raccomanda di produrre il documento anche quando la legge non lo prescrive. Il piano per la protezione dei dati, infatti, tiene conto dell'importanza della protezione dei dati in termini di rispetto della sfera privata e dei diritti della personalità di chi riceve prestazioni, di chi risiede negli istituti, del personale di tali aziende e, se del caso, anche dei loro partner commerciali. L'**obiettivo principale** del piano è garantire la protezione della personalità delle persone fisiche dal trattamento illecito o sproporzionato dei loro dati personali. Il piano, inteso come linea guida vincolante, fungerà infatti da ausilio che permetterà al personale degli istituti interessati di agire in conformità al diritto in materia di protezione dei dati. La messa a punto del piano è facoltativa; la legge non impone lo sviluppo di un tale strumento in modo vincolante.

Inoltre, si consiglia di invitare le persone ed aziende terze che hanno rapporti commerciali con l'istituto a dichiarare per iscritto che rispetteranno il piano per la protezione dei dati dell'istituto.

ARTISET

Zieglerstrasse 53, 3007 Berna
T +41 31 385 33 33
info@artiset.ch, artiset.ch

Föderation der Dienstleister
für Menschen mit Unterstützungsbedarf

4. Mansionario per il/la titolare aziendale della protezione dei dati

Ogni istituto deve nominare un/una «titolare del trattamento» dei dati personali. Questa persona, che può essere una collaboratrice o un collaboratore dell'istituto o una persona esterna, anche una persona giuridica (per es. ufficio fiduciario), determina lo scopo e i mezzi del trattamento dei dati personali nell'istituto (cfr. art. 5 lett j LPD). Può delegare compiti a «responsabili del trattamento» (cfr. art. 5 lett. k LPD).

Le informazioni sugli obblighi del/della titolare del trattamento degli istituti sono sparse qua e là nella Legge e nell'Ordinanza sulla protezione dei dati (cfr. art. 5 lett. j LPD, ecc.). Per questo, è utile produrre un mansionario per il/la titolare aziendale della protezione dei dati che riporti gli obblighi di tale figura in modo chiaro e sintetico. ARTISET ha creato un apposito **modello**.

5. Registri delle attività di trattamento

Per gli istituti con meno di 250 dipendenti, la produzione di uno o più registri delle attività di trattamento non è obbligatoria (cfr. art. 12 LPD, art. 24 OPDa) ma comunque consigliata. Affinché tali registri possano adempiere appieno al loro scopo, andranno aggiornati costantemente, o perlomeno a brevi intervalli regolari. ARTISET ha creato un apposito **modello**.

6. Collezioni di dati personali: accesso e aggiornamento

Si raccomanda di stabilire per iscritto chi, in azienda, sia autorizzato ad accedere alle collezioni di dati personali e di definire le relative autorizzazioni (password per l'archivio elettronico, chiavi per quello cartaceo).

Si consiglia anche di stabilire per iscritto chi debba comunicare al/alla titolare aziendale della protezione dei dati eventuali modifiche ai contenuti delle collezioni di dati affinché il/la titolare o una persona terza incaricata da quest'ultimo/a modifichi di conseguenza i registri delle attività.

7. Provvedimenti di protezione tecnici e organizzativi

Si raccomanda di attuare le misure necessarie a garantire la protezione dei dati dell'istituto fin dalla progettazione («Privacy by Design») e attraverso preimpostazioni a tutela della protezione dei dati («Privacy by Default»; cfr. art. 7 LPD, art. 3 OPDa). In questo modo deve essere garantita la sicurezza dei dati (cfr. art. 8 LPD). I controlli sull'accesso e sui supporti di dati personali devono impedire a persone non autorizzate di accedere alle raccolte elettroniche di dati, di alterarle, distruggerle o rubarle.

Data la costante evoluzione della tecnologia, la nuova legislazione sulla protezione dei dati si astiene deliberatamente dall'imporre soluzioni tecniche specifiche: la legge si limita a richiedere agli istituti di adottare i provvedimenti tecnici e organizzativi necessari affinché il trattamento dei dati personali sia conforme alle disposizioni sulla protezione dei dati (art. 7 cpv. 1 LPD).

I provvedimenti tecnici e organizzativi devono essere adeguati in particolare allo stato della tecnica, al tipo e all'entità del trattamento dei dati personali come pure ai rischi derivanti dal trattamento per la personalità o i diritti fondamentali delle persone interessate (art. 7 cpv. 2 LPD). Una sicurezza dei dati adeguata al rischio deve essere garantita (art. 8 cpv. 1 LPD).

L'utilizzo di indirizzi HIN (criptati) per le e-mail contenenti dati personali sensibili è, ad esempio, una buona cosa. Non si può affermare senz'altro che il traffico attraverso i canali di trasmissione e-mail convenzionali sarebbe inammissibile. Tuttavia, l'utilizzo di indirizzi HIN migliorerà indubbiamente la sicurezza.

Dovranno essere attuati i seguenti provvedimenti a tutela dei dati personali soggetti a trattamento elettronico:

- crittografia;
- installazione di firewalls, software antivirus e indirizzi HIN;
- attuazione di eventuali altre misure tecniche di protezione; e
- registrazione degli accessi.

8. Consenso alla raccolta e al trattamento dei dati

In linea di principio, la persona interessata deve essere informata dal responsabile della protezione dei dati in merito alla raccolta dei dati personali che la riguardano (art. 19 cpv. 1 LPD; esistono tuttavia delle eccezioni, cfr. la sezione successiva). Questo obbligo di informazione si applica anche quando i dati non vengono raccolti presso la persona interessata. Inoltre, i dati personali possono essere raccolti soltanto per uno scopo determinato e riconoscibile per la persona interessata (art. 6 cpv. 3 LPD). Inoltre, i dati personali non possono essere elaborati se la persona interessata si oppone espressamente (art. 30 cpv. 2 lett. b LPD a contrario).

Da questo intreccio di disposizioni di legge si evince che la persona interessata deve essere preventivamente informata dei vari scopi per i quali i suoi dati personali saranno utilizzati (e quindi trattati). Il modo in cui viene ottenuto il consenso non deve necessariamente assumere una forma particolare (di per sé, è sufficiente un semplice segno).

Il trattamento di *dati personali sensibili* (come le informazioni sullo stato di salute) richiede il consenso esplicito della persona interessata (cfr. art. 6 cpv. 7 lett. a LPD).

Di regola non vi è lesione della personalità se la persona interessata ha reso i suoi dati personali accessibili a chiunque e non si è opposta espressamente al trattamento (cfr. art. 30 cpv. 3 LPD).

9. Obbligo dell'istituto di informare

Si raccomanda di prevedere il rispetto delle seguenti istruzioni / dei seguenti limiti mediante linea guida affinché il/la titolare del trattamento e gli uffici coinvolti possano adempiere al loro obbligo di informare in conformità agli artt. 19–20 LPD e all'art. 13 OPDa nei confronti di chi riceve prestazioni, di partner commerciali e del personale:

- Il/la titolare del trattamento informa la persona interessata quando l'istituto raccoglie i dati della persona stessa. Ciò vale anche nel caso in cui i dati non vengano raccolti presso la persona interessata.
- La legge obbliga il/la titolare del trattamento a comunicare alla persona interessata almeno:
  - l'identità e i dati di contatto del/della titolare del trattamento;
  - lo scopo del trattamento;
  - eventuali destinatari o categorie di destinatari cui verranno comunicati i dati personali;
  - le categorie dei dati personali trattati, nel caso in cui non siano stati raccolti presso la persona interessata;
  - lo Stato o l'organismo internazionale destinatario e, se del caso, le garanzie previste dall'art. 16 cpv. 2 LPD o l'applicazione di una delle eccezioni stabilite dall'art. 17 LPD nel caso in cui i dati personali vengano trasmessi all'estero.

Inoltre, devono essere osservate le seguenti modalità:

- Se i dati personali non sono raccolti presso la persona interessata, il/la titolare del trattamento le fornisce queste informazioni entro un mese dalla ricezione dei dati.
- Se comunica questi dati personali prima della scadenza di detto termine, il/la titolare del trattamento fornisce alla persona interessata tali informazioni al più tardi al momento della comunicazione dei dati.
- L'obbligo di informare non sussiste se:
  - la persona interessata dispone già delle informazioni pertinenti;
  - il trattamento dei dati personali è previsto dalla legge;
  - il/la titolare del trattamento è un privato tenuto per legge a serbare il segreto.
- Se i dati personali non vengono raccolti presso la persona interessata, l'obbligo di informare non si applica nei casi seguenti:
  - non sia possibile, oppure;
  - richieda un onere sproporzionato.
- Inoltre, il/la titolare del trattamento può limitare o differire l'informazione oppure rinunciarvi se:
  - interessi preponderanti di terzi lo esigono;
  - l'informazione pregiudica lo scopo del trattamento;
  - lo esigono i suoi interessi preponderanti;
  - non comunica i dati personali a terzi (precisazione: in questo contesto li istituti che fanno parte dello stesso gruppo non sono considerati soggetti terzi).

10. Diritto di consultazione e accesso delle persone interessate

Affinché le persone i cui dati vengono trattati dall'istituto («persone interessate») possano far valere efficacemente il loro diritto di accesso e consultazione come da artt. 25–26 LPD e artt. 16–19 OPDa si raccomanda di prevedere il rispetto delle seguenti istruzioni / dei seguenti limiti mediante linea guida:

- Chiunque può domandare al/alla titolare del trattamento se i dati personali che lo concernono sono oggetto di trattamento.
- Alla persona interessata sono fornite le informazioni necessarie affinché possa far valere i suoi diritti e sia garantito un trattamento trasparente dei dati. In ogni caso devono essere fornite le informazioni seguenti:
  - l'identità e i dati di contatto del/della titolare del trattamento;
  - i dati personali trattati;
  - i soggetti che partecipano alla raccolta;
  - casomai: i destinatari dei dati;
  - lo scopo del trattamento dei dati personali;
  - la durata di conservazione dei dati personali o, se ciò non è possibile, i criteri per stabilire tale durata;
  - le informazioni disponibili sulla provenienza dei dati personali che non sono stati raccolti presso la persona interessata.
- L'informazione deve essere fornita entro 30 giorni dall'istituto per iscritto e formulata in modo comprensibile.
- Il/La titolare del trattamento deve fornire gratuitamente le informazioni se ciò non richiede un onere sproporzionato.
- L'istituto ha l'obbligo di rettificare o eliminare i dati non corretti o trattati in modo illecito o non corretto.
- Qualsiasi persona interessata può ottenere il blocco della comunicazione dei propri dati se dimostra di avere un interesse degno di protezione.
- Se del caso, va comunicata alla persona interessata l'esistenza di una decisione individuale automatizzata e la logica su cui si fonda la decisione (le decisioni individuali automatizzate sono eppure rare nel caso degli istituti).

ARTISET

Zieglerstrasse 53, 3007 Berna
T +41 31 385 33 33
info@artiset.ch, artiset.ch

- La persona interessata è informata degli eventuali destinatari o delle eventuali categorie di destinatari cui vengono comunicati i suoi dati personali.
- Se i dati personali vengono trasferiti all'estero:
  - le informazioni di cui all'art. 19 cpv. 4 LPD.
  - lo Stato o l'organismo internazionale destinatario e, se del caso, le garanzie previste dall'art. 16 cpv. 2 LPD o l'applicazione di una delle eccezioni stabilite dall'art. 17 LPD.
- In casi eccezionali, la messa a disposizione di informazioni e i diritti di consultazione possono essere limitati o negati quando lo prevede una legge, quando confliggono con interessi preponderanti di terzi o dell'istituto, quando i dati personali non vengono comunicati a terzi o quando la richiesta di accesso è manifestamente infondata.

Si consiglia di attuare una procedura (sommaria) di notifica affinché la persona interessata possa far valere il suo diritto di accesso e il/la titolare del trattamento nonché gli uffici coinvolti dell'istituto possano rispondere in modo efficiente alle richieste di accesso.

11. Affidamento del trattamento a un responsabile

Il trattamento dei dati personali può essere affidato a un responsabile del trattamento (cfr. art. 9 LPD e art. 7 OPDa). In tale ambito occorre osservare:

un simile mandato non deve necessariamente essere conferito per iscritto, ma può essere anche conferito verbalmente o addirittura mediante atti concludenti. ARTISET mette a disposizione un **modello** per un contratto di affidamento scritto dettagliato, che formalizza in modo completo e compatto le disposizioni legali rilevanti (cfr. art. 9 LPD e anche art. 7 OPDa) nonché ulteriori disposizioni e principi del diritto in materia di protezione dei dati e del Codice delle obbligazioni). Sebbene non sia assolutamente necessario sottoscrivere un contratto così dettagliato, può comunque rivelarsi più sicuro: infatti, il titolare del trattamento deve assicurarsi che il responsabile del trattamento rispetti la legge nella sua stessa misura (dovere di diligenza). Un contratto scritto offre il vantaggio di chiarire e formalizzare il quadro legale.

Inoltre occorre precisare:

- per il trattamento dei dati da parte del responsabile del trattamento non occorre il consenso della persona i cui dati vengono trattati;
- il responsabile del trattamento dei dati può trasferire il trattamento a terzi solo previa approvazione del titolare del trattamento;
- il trattamento dei dati all'interno della medesima persona giuridica (filiale, unità amministrativa, personale) non rappresenta in via di principio un affidamento del trattamento a un responsabile, sarebbe quindi superfluo stilare un contratto di affidamento di trattamento per ogni scambio interno di dati personali tra settori dello stesso istituto;
- se i dati sono conservati in un cosiddetto cloud, nella fattispecie si tratta in via di principio di un caso di applicazione dell'affidamento del trattamento a un responsabile per il quale devono essere soddisfatti i relativi presupposti. Se a tale scopo è necessario rendere noti dati personali all'estero, occorre inoltre soddisfare i rispettivi presupposti (cfr. sotto).

12. Diritto di farsi consegnare dati o di esigerne la trasmissione a terzi

Secondo gli artt. 28–29 LPD e 20–22 OPDa chiunque può esigere dagli istituti che i dati personali che lo concernono e che ha comunicato loro gli siano consegnati in un formato elettronico usuale e, di norma, a titolo gratuito quando i dati sono trattati in modo automatizzato. I casi di trattamento automatizzato dei dati sono però rari tra gli istituti.

13. Comunicazione di dati personali all'estero

Se i dati personali vengono comunicati all'estero l'istituto deve adottare i provvedimenti stabiliti dagli artt. 16–18 LPD e artt. 8–12 OPDa.

14. Valutazione d'impatto sulla protezione dei dati

Se l'istituto elabora dati personali che comportino un rischio elevato per la personalità e i diritti fondamentali della persona interessata, il/la titolare del trattamento deve effettuare previamente una valutazione d'impatto sulla protezione dei dati come previsto dall'art. 22 LPD. La valutazione d'impatto deve contenere una descrizione del trattamento previsto, una valutazione dei rischi per la personalità o per i diritti fondamentali della persona interessata nonché i provvedimenti previsti a loro tutela (art. 22 cpv. 3 LPD).

A seconda dell'esito della valutazione d'impatto effettuata può rendersi necessario consultare l'incaricato federale della protezione dei dati e della trasparenza (IFPDT) come da art. 23 LPD.

Nella pratica, i casi in cui gli istituti trattino dati personali che implicano un rischio elevato per la personalità e i diritti fondamentali delle persone interessate sono frequenti. Le valutazioni d'impatto sono altrettanto frequenti.

15. Archiviazione e distruzione dei dati personali

I dati personali sono distrutti o resi anonimi appena non sono più necessari per lo scopo del trattamento

I dati personali raccolti per uno scopo specifico possono essere conservati solo per il tempo necessario a raggiungere tale scopo (art. 6 cpv. 4 LPD). Se non sono più utili, devono essere anonimizzati o cancellati/distrutti, a meno che non vi siano motivi preponderanti per conservarli.

È quindi necessario verificare caso per caso:
- per quanto tempo è necessario conservare dati personali in questione,
- se esiste un obbligo legale di conservazione
- oppure se esiste un interesse prevalente alla loro conservazione.

È quindi consigliabile di garantire mediante linea guida che:
- i dati personali di cui l'istituto non ha più bisogno vengano trattati e archiviati a tempo determinato o indeterminato;
- i dati personali di minore importanza vengano distrutti (eliminati fisicamente o cancellati elettronicamente in modo irreversibile) subito dopo il raggiungimento dello scopo del trattamento.

16. Trattamento automatizzato di dati personali

Come già accennato, i trattamenti automatizzati di dati personali da parte di istituti sono rari. Qualora vengano eppure effettuati, è necessario tenere in considerazione i seguenti punti:
- La registrazione, la modifica, la consultazione, la comunicazione, la cancellazione e la distruzione dei dati vanno verbalizzate (cfr. art. 4 OPDa) ovunque vengano trattati in modo automatizzato e su grande scala dati degni di particolare protezione. Tuttavia, ciò non è obbligatorio quando la protezione è garantita da misure di prevenzione.
- L'istituto deve elaborare un regolamento ai sensi dell'art. 5 OPDa nella misura in cui effettui trattamenti automatizzati su grande scala di dati personali degni di particolare protezione. Il regolamento deve contenere in particolare indicazioni sull'organizzazione interna, sulla procedura di trattamento e di controllo dei dati nonché sui provvedimenti per garantire la sicurezza dei dati (cfr. art. 5 cpv. 2 OPDa).

17. Profilazione

Per profilazione si intende l'utilizzazione di dati per valutare determinati aspetti personali di una persona, ad esempio 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 (cfr. art. 5 lett. f LPD). La profilazione presuppone il trattamento automatizzato di dati personali.

I casi di trattamento automatizzato di dati sono però rari tra gli istituti. In questo contesto, perciò, i meccanismi particolari di protezione previsti dalla legge in caso di profilazione sono irrilevanti e non verranno quindi descritti in dettaglio.

18. Notifica di violazioni della protezione dei dati

Si consiglia di attuare una procedura (sommaria) di notifica o perlomeno di elaborare un relativo modello affinché il/la titolare del trattamento possa segnalare eventuali violazioni della protezione dei dati da parte dell'istituto all'incaricato federale della protezione dei dati e della trasparenza (IFPDT) in modo efficiente (cfr. art. 24 LPD e art. 15 OPDa).

19. Esenzione

L'istituto può rilasciare un'esenzione dal pagamento di multe a seguito di violazioni delle disposizioni penali della LPD (cfr. art. 60ss. LPD) in favore del/della titolare aziendale dei dati personali e di eventuali responsabili del trattamento. Lo scopo di tale "esenzione" è quello di agevolare il reclutamento di tali figure. ARTISET ha messo a punto un **modello** di esenzione.

Yann Golay Trechsel / 4.3.2024