Revisione della legge federale sulla protezione dei dati (LPG)

Lista di controllo per una valutazione in materia di protezione dei dati

Lo scopo della lista di controllo è aiutare gli istituti a:

- effettuare una valutazione della propria situazione in materia di diritto sulla protezione dei dati;
- accertare e a valutare lo stato attuale del trattamento dei dati personali delle persone fisiche (principalmente clienti e collaboratori);
- ricavare possibili provvedimenti e modifiche in vista dell'entrata in vigore della LPG riveduta.

Nel presente documento, il termine «cliente» si riferisce a tutte le persone bisognose di assistenza che vivono o lavorano in un istituto o che usufruiscono di prestazioni istituzionali individuali.

La presente lista di controllo deve essere intesa come un ausilio e non ha la pretesa di essere esaustiva.

Per eventuali domande è possibile rivolgersi ai consulenti legali di ARTISET.

- Hans-Ulrich Zürcher | 031 351 58 85 | zuercher@advokatur-zuercher.ch
- Christian Streit | 031 385 33 39 | rechtsberatung@artiset.ch
- Yann Golay | 031 385 33 36 | yann.golay@artiset.ch

Una breve panoramica dei contenuti rilevanti della legge federale sulla protezione dei dati riveduta

1. Lo scopo della **protezione dei dati** è proteggere i **dati personali**. Per dati personali si intendono «tutte le informazioni concernenti una persona fisica identificata o identificabile».

   I **dati personali degni di particolare protezione** sono
   - i dati concernenti le opinioni o attività religiose, filosofiche, politiche o sindacali;
   - i dati concernenti l'appartenenza a un gruppo etnico o di origine;
   - i dati concernenti la salute e la sfera intima;
   - i dati genetici e biometrici (ad esempio, DNA, impronte digitali, quadro ematologico sulla base di un campione di sangue);
   - i dati concernenti sanzioni e perseguimenti amministrativi e penali;
   - i dati concernenti i provvedimenti d'assistenza sociale.

2. Il **trattamento dei dati personali** consiste in «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 dati».

3. La **collezione di dati** consiste in «ogni complesso di dati personali la cui struttura permette di ricercare i dati secondo le persone interessate».
   È necessario tenere un **inventario delle collezioni di dati** (si veda l'Allegato 2).

4. **Profilazione**
   Per profilazione si intende il trattamento *automatizzato* di dati personali allo scopo di creare modelli comportamentali e profili della personalità (ad esempio, situazione economica, salute, preferenze personali, interessi ecc.).
   Se il collegamento tra dati consente di valutare aspetti significativi della personalità (ad esempio, in caso di trattamento di dati personali degni di particolare protezione), aumenta il rischio di violazione dei diritti della personalità e occorre pertanto ottenere il consenso esplicito della persona interessata.

5. **Analisi dei rischi/valutazione d'impatto sulla protezione dei dati**
   Valutazione dell'eventuale rischio per i diritti della persona interessata a seguito di un trattamento non corretto dei dati personali. Per analizzare questo rischio potenziale, è necessario stimare la probabilità di accadimento di un determinato rischio e l'entità del danno potenziale. Si deve valutare e decidere se il trattamento dei dati è giustificabile in considerazione dei rischi che comporta e come i rischi identificati possano essere ridotti al minimo. L'analisi deve essere conservata per 2 anni.

6. Campo di applicazione della LPD e applicabilità delle leggi cantonali sulla protezione dei dati

Nella LPD, la Confederazione disciplina il trattamento dei dati da parte delle autorità federali e dei privati. I Cantoni hanno l'autorità di regolamentare il trattamento dei dati da parte degli organi cantonali stessi.
Molte leggi cantonali sulla protezione dei dati designano come organi cantonali anche soggetti privati (fondazioni, associazioni di diritto privato ecc.) a cui sono stati assegnati incarichi pubblici. Questo vale in particolare per gli istituti che adempiono compiti istituzionali di assistenza sociale sulla base di un contratto di prestazioni con il Cantone. In questo contesto, essi non sono soggetti alla LPD, bensì al diritto cantonale in materia di protezione dei dati.

7. Liceità del trattamento dei dati

Il trattamento dei dati è lecito se

- la persona interessata ha fornito il suo consenso volontario (in qualsiasi forma);
- è previsto dalla legge;
- la persona interessata ha reso accessibili i propri dati e non ne ha espressamente vietato il trattamento;
- il trattamento è giustificato da un interesse pubblico o privato preponderante. – Un interesse privato comprende, tra l'altro, l'esecuzione di un contratto esistente (ad esempio, un contratto di lavoro o un contratto di assistenza).

8. Responsabile della protezione dei dati in azienda

Funzione/compiti:

- controlla il trattamento dei dati personali all'interno dell'istituto e interviene in caso di violazione delle disposizioni legali;
- ha accesso a tutte le collezioni di dati e a tutte le attività di trattamento dei dati;
- tiene un elenco delle collezioni di dati;
- redige direttive e istruzioni per garantire la protezione dei dati;
- effettua analisi dei rischi e valutazioni d'impatto sulla protezione dei dati e le documenta.

Caratteristiche/posizione:

- può essere un collaboratore dell'istituto o una terza persona incaricata;
- possiede le necessarie conoscenze specialistiche;
- è subordinato a livello organizzativo/gerarchico in modo da evitare conflitti di interesse (possibile soluzione: assoggettamento diretto al Comitato direttivo/Consiglio di fondazione).

#	Oggetto / punti da esaminare	Valutazione dei risultati Stato attuale	Provvedimenti proposti	Scadenza	Responsabile
1	**Aspetti generali / situazione inziale**				
1.1	La protezione dei dati è sistematicamente pianificata e coordinata all'interno dell'istituto?		▪ Definire i principi nel piano per la protezione dei dati ▪ Considerare la protezione dei dati fin dalla fase di pianificazione del trattamento dei dati		
1.2	Quando e come si affronta la protezione dei dati e si valuta la situazione all'interno: ▪ del Consiglio di fondazione/Comitato direttivo? ▪ della Direzione generale?		▪ Emanazione di un piano per la protezione dei dati da parte del Consiglio di fondazione/Comitato direttivo ▪ Affrontare regolarmente la protezione dei dati a livello dirigenziale nell'ambito della gestione dei rischi		
1.3	I principi relativi al trattamento dei dati e i provvedimenti di protezione sono già documentati (piano per la protezione dei dati, istruzioni e regolamenti interni ecc.)?		▪ Elaborare un piano per la protezione dei dati ▪ Elaborare istruzioni per la protezione dei dati		
1.4	Si sono già verificati problemi o episodi particolari in materia di protezione dei dati?		Tenere conto delle esperienze passate		
1.5	L'istituto è soggetto (esclusivamente/parzialmente) al diritto cantonale in materia di protezione dei dati?		▪ Chiarire l'assoggettamento ▪ Verificare la conformità dello stato attuale ai requisiti del diritto cantonale e/o federale		

#	Oggetto / punti da esaminare	Valutazione dei risultati Stato attuale	Provvedimenti proposti	Scadenza	Responsabile
			▪ In caso di assoggettamento al diritto cantonale, monitorare e comprendere i futuri adeguamenti della legislazione		
1.6	Forma di trattamento dei dati (elettronica/cartacea)?		▪ Adottare decisioni consapevoli sulla forma futura ▪ Incoraggiare la digitalizzazione secondo una procedura definita		
2	**Responsabilità per la protezione dei dati nell'istituto**				
2.1	Valutazione della regolamentazione/responsabilità attuale?		Incorporare l'esperienza acquisita nella regolamentazione futura		
2.2	La responsabilità è già disciplinata?		▪ Determinare la persona responsabile (collaboratore o persona esterna) ▪ Definire il mansionario ▪ Assicurare la formazione iniziale e il successivo aggiornamento della persona responsabile		
3	**Collezioni di dati**				
3.1	Quali collezioni di dati esistono?		Redigere un registro delle attività di trattamento dei dati e aggiornarlo regolarmente *Nota* I requisiti del registro sono elencati nell'Allegato 2		
3.2	Cosa contengono queste collezioni di dati?		Creare un inventario dei dossier esistenti		
3.3	Come e da chi sono gestite?		Coordinare la gestione e la standardizzazione delle collezioni di dati		
3.4	L'istituto effettua un trattamento elettronico *automatizzato* di dati personali		Ottenere il consenso esplicito della persona interessata		

#	Oggetto / punti da esaminare	Valutazione dei risultati Stato attuale	Provvedimenti proposti	Scadenza	Responsabile
	degni di particolare protezione allo scopo di creare modelli comportamentali e profili della personalità (ad esempio, situazione economica, salute, preferenze personali, interessi ecc.)?				
4	**Sicurezza dei dati**				
4.1	Il trattamento dei dati viene effettuato sull'infrastruttura dell'istituto o su quella di un provider?		Elaborare norme contrattuali con il provider in merito al rispetto della sicurezza dei dati		
4.2	Esistono provvedimenti tecnici ed organizzativi all'interno dell'istituto per proteggere i dati trattati?		▪ Verificare i provvedimenti e, se necessario, ottimizzare la sicurezza ▪ Disciplinare i diritti di accesso in modo appropriato ▪ Impedire l'accesso a persone non autorizzate		
4.3	Come è disciplinato in generale l'accesso ai dati personali nell'istituto? Esiste una regolamentazione speciale per l'accesso a dati personali degni di particolare protezione?		Definire l'accesso a ciascuna collezione di dati, nel modo più restrittivo possibile, ma funzionale, per i dati personali degni di particolare protezione		
4.4	È garantita la disponibilità di tutti i dati rilevanti entro un periodo di tempo ragionevole?		▪ Verificare e adeguare i requisiti tecnici ▪ Definire le regole di accesso in modo che sia sempre presente almeno una persona autorizzata		

#	Oggetto / punti da esaminare	Valutazione dei risultati Stato attuale	Provvedimenti proposti	Scadenza	Responsabile
4.5	I dati sono adeguatamente protetti da furto, falsificazione, distruzione ecc.?		Verificare le autorizzazioni di accesso e la situazione tecnica (tecnico-informatica o fisica, ad esempio la conservazione dei dossier sotto chiave) e, se necessario, adeguarle		
4.6	Scambio dei dati: ▪ Come vengono scambiati i dati personali all'interno dell'istituto e con soggetti esterni? ▪ Lo scambio dei dati via e-mail è protetto?		Garantire la trasmissione sicura dei dati con e-mail criptate o in un altro modo adeguato		
5	**Ammissibilità/liceità del trattamento dei dati**				
5.1	Esiste un consenso sufficiente da parte dei soggetti interessati o un'autorizzazione legale speciale per ciascuna attività di trattamento dei dati?		Aggiornare i contratti di lavoro/dell'istituto esistenti o integrare i nuovi contratti con il seguente passaggio, applicato per analogia: *«Con la sottoscrizione del presente contratto, la persona interessata autorizza espressamente XXX [nome dell'ISTITUTO] al trattamento dei dati personali comunicati, nei limiti previsti e consentiti dalla legge o necessari per l'esecuzione del presente contratto e sempre che non vi sia un'espressa opposizione da parte della persona interessata».*		
5.2	I dati sono trattati in base a una finalità definita?		Definire le finalità del trattamento e registrarle per iscritto		
5.3	Il trattamento dei dati rientra nella finalità definita?		Effettuare verifiche periodiche (controlli a campione) del trattamento		
5.4	Il cliente ha redatto un testamento biologico o		▪ Archiviare i documenti esistenti nel dossier del cliente		

#	Oggetto / punti da esaminare	Valutazione dei risultati Stato attuale	Provvedimenti proposti	Scadenza	Responsabile
	costituito un mandato precauzionale?		▪ Raccomandare al cliente di redigere un testamento biologico/costituire un mandato precauzionale		
6	**Utilizzo/pubblicazione di registrazioni video/audio di clienti e collaboratori**				
6.1	L'istituto effettua e utilizza registrazioni video/audio? Per quali scopi?		Includere l'argomento nel registro delle attività di trattamento dei dati		
6.2	Come si ottiene il consenso dei soggetti interessati per l'utilizzo a fini di pubblicazione?		Il consenso all'utilizzo per la pubblicazione è legalmente valido solo se viene fornito volontariamente ed espressamente nei singoli casi con cognizione di causa in merito alle registrazioni specifiche e alla finalità; può anche essere revocato *Nota* Un consenso formulato in modo generico nel contratto di lavoro/dell'istituto non è sufficiente		
7	**Proporzionalità del trattamento dei dati**				
7.1	Il trattamento dei dati viene attualmente effettuato limitandosi alla misura necessaria?		Limitazione della raccolta dei dati alla finalità del trattamento (ad esempio, contratto di lavoro)		
7.2	È garantito che i dati siano raccolti per una finalità lecita, siano trattati solo per tale finalità e non siano utilizzati per finalità diverse?		Includere il requisito della finalità vincolata nel piano per la protezione dei dati		
7.3	Viene effettuata la raccolta e la registrazione di dati «di scorta» (senza		Includere il divieto di «trattamento di dati di scorta» nel piano per la protezione dei dati		

#	Oggetto / punti da esaminare	Valutazione dei risultati Stato attuale	Provvedimenti proposti	Scadenza	Responsabile
	una finalità specifica e chiara)?				
7.4	È garantito che i dati siano registrati solo per il tempo richiesto dalla finalità del trattamento?		Includere il requisito della limitazione della registrazione nel piano per la protezione dei dati *Nota* Per la necessità del trattamento si vedano anche le sezioni «Archiviazione» e «Cancellazione»		
8	**Comunicazione/trasmissione di dati a terzi**				
8.1	I dati vengono comunicati al curatore?		Documentare o registrare la comunicazione		
8.2	I dati vengono comunicati a terzi (autorità, medici/ospedali, compagnie assicurative ecc.)?		▪ Informare la persona interessata ▪ Garantire il trasferimento sicuro dei dati		
8.3	I dati vengono comunicati all'estero?		▪ Valutare i rischi (specifici del Paese) prima della comunicazione (eventualmente dopo aver consultato il provider ICT) ▪ Informare i soggetti interessati *Nota* La comunicazione all'estero include anche la registrazione dei dati in un cloud su un'infrastruttura di server che si trova fisicamente all'estero		
9	**Informare i soggetti interessati sul trattamento dei dati**				
9.1	Quando e come i soggetti interessati vengono informati del trattamento dei dati?		▪ Assicurarsi che i soggetti interessati vengano informati e, se necessario, adeguare la procedura ▪ In caso di raccolta programmata dei dati, al momento della raccolta devono essere fornite le seguenti informazioni:		

#	Oggetto / punti da esaminare	Valutazione dei risultati Stato attuale	Provvedimenti proposti	Scadenza	Responsabile
			- persona/dati di contatto del/la responsabile aziendale della protezione dei dati - finalità del trattamento - periodo di utilizzo dei dati - destinatari, se i dati sono comunicati a terzi *Nota* «Raccolta programmata dei dati» significa che i dati vengono raccolti intenzionalmente. Consiglio: le informazioni sul trattamento dei dati sono sempre fornite per iscritto (nel contratto di lavoro/dell'istituto o in un documento aggiuntivo a tali contratti)		
9.2	Esiste una dichiarazione sulla protezione dei dati sul sito web dell'istituto?		Controllare la dichiarazione sulla protezione dei dati esistente o caricarne una nuova		
10	**Diritto di accesso/consultazione da parte soggetti interessati**				
10.1	Come viene garantito attualmente il diritto di accesso/consultazione?		Registrare il diritto di accesso/consultazione nel piano per la protezione dei dati, tenendo conto dei seguenti requisiti: ▪ in linea di principio, diritto di accesso/consultazione in qualsiasi momento e senza alcun prerequisito ▪ in linea di principio, a titolo gratuito (eccezione in caso di impegno sproporzionato; il calcolo dei costi deve essere comunicato in anticipo) ▪ la limitazione o il rifiuto in caso di interesse pubblico o privato preponderante costituisce un'eccezione e i suoi presupposti sono definiti		
11	**Consegna dei dati ai soggetti interessati**				

#	Oggetto / punti da esaminare	Valutazione dei risultati Stato attuale	Provvedimenti proposti	Scadenza	Responsabile
11.1	In che modo i dati vengono attualmente consegnati ai soggetti interessati?		Creare una panoramica e documentare l'attuale procedura		
11.2	L'istituto è in grado di consegnare i dati personali «in un formato elettronico usuale» in futuro?		Adottare provvedimenti per essere in grado di consegnare i dati per via elettronica		
12	**Dossier personale**				
12.1	Il reparto del personale tiene un dossier unico completo per ogni collaboratore?		Tutti i dati rilevanti per un collaboratore devono essere riuniti in un unico dossier		
12.2	Chi vi ha accesso?		Disciplinare l'accesso in modo chiaro e possibilmente differenziato		
12.3	I dati degni di particolare protezione sono conservati in modo sicuro/separatamente?		Verificare il livello di protezione e migliorarlo, se necessario *Nota* I dati degni di particolare protezione sono, ad esempio, i certificati e i rapporti medici; le informazioni relative a infortuni, indennità giornaliere di malattia, assicurazione per l'invalidità; informazioni relative ad attività sindacali ecc.		
12.4	Esistono «dossier segreti» (presso i superiori)?		I «dossier segreti» devono essere vietati e distrutti		
13	**Dossier dei clienti**				
13.1	Viene tenuto un dossier completo per ogni cliente?		Creare una panoramica della procedura attuale e documentarla		

#	Oggetto / punti da esaminare	Valutazione dei risultati Stato attuale	Provvedimenti proposti	Scadenza	Responsabile
13.2	Chi tiene questi dossier?		Creare una panoramica della procedura attuale e documentarla		
13.3	Chi ha accesso ai dossier?		Disciplinare l'accesso in modo chiaro e possibilmente differenziato		
13.3	I dati degni di particolare protezione sono conservati in modo sicuro/separatamente?		Verificare il livello di protezione e migliorarlo, se necessario *Nota* I dati degni di particolare protezione sono, ad esempio, i certificati e i rapporti medici; i trattamenti medici e farmacologici nonché le terapie; le informazioni relative a infortuni, indennità giornaliere di malattia, assicurazione per l'invalidità; informazioni relative alla religione, alla sfera intima ecc.		
14	**Archiviazione dei dati**				
14.1	In quale forma vengono conservati attualmente i dati?		In linea di principio, incoraggiare l'archiviazione digitale *Nota* La conservazione in formato cartaceo è prescritta solo in rari casi (ad esempio, per la relazione sulla gestione e la relazione di revisione; art. 958 f cpv. 2 CO). I dati devono essere conservati separatamente per tipologia, ordinati, datati e in ordine cronologico		
14.2	Per quanto tempo vengono conservati attualmente i dati?		Definire i principi relativi all'archiviazione (nel piano per la protezione dei dati o per l'archiviazione), tenendo conto dei termini di conservazione legali o sulla base dei termini di prescrizione generali ai sensi del diritto federale e delle disposizioni cantonali (ad esempio, ai sensi della legge sull'archiviazione, della legge sull'assistenza sociale ecc.) *Nota* Le disposizioni federali relative alla conservazione e i termini di prescrizione sono riportati nell'Allegato 1		

#	Oggetto / punti da esaminare	Valutazione dei risultati Stato attuale	Provvedimenti proposti	Scadenza	Responsabile
14.3	Chi ha accesso all'archivio dati?		Disciplinare chiaramente l'accesso (principio: il numero di persone necessarie, meno persone possibile)		
14.4	La sicurezza dei dati archiviati è garantita?		▪ Verificare la situazione relativa alla sicurezza in generale ▪ Provvedimenti di protezione dei dati archiviati da furto o distruzione (acqua, fuoco, parassiti ecc.) ▪ Protezione dei dati archiviati elettronicamente da modifiche, cancellazioni ecc. ▪ Garantire la leggibilità futura dei dati archiviati elettronicamente		
15	**Cancellazione dei dati**				
15.1	La cancellazione viene effettuata a norma di legge?		▪ Garantire la cancellazione definitiva dei dati elettronici ▪ Distruggere i dati fisici in loco o conferirli in appositi contatiner adibiti a tale scopo		
15.2	I termini di cancellazione sono disciplinati e definiti in modo differenziato?		Disciplinare i termini di cancellazione (nel piano per la protezione dei dati o nel piano specifico per la cancellazione), tenendo conto ▪ dei termini di conservazione definiti dalla legge ▪ del principio secondo cui la durata dell'archiviazione deve essere adeguatamente limitata		
16	**Istruzione e sensibilizzazione dei collaboratori**				
16.1	Come vengono attualmente istruiti e sensibilizzati i collaboratori in materia di protezione dei dati ▪ in generale? ▪ in particolare?		▪ Divulgazione di tutti i regolamenti interni rilevanti in materia di protezione dei dati (piano per la di protezione dei dati, istruzioni ecc.) ▪ Istruzione e sensibilizzazione generale regolare nell'ambito del perfezionamento interno ▪ Consulenza e supporto in situazioni particolari per i singoli collaboratori e indicazioni sulla corretta gestione da		

#	Oggetto / punti da esaminare	Valutazione dei risultati Stato attuale	Provvedimenti proposti	Scadenza	Responsabile
			parte dei superiori o dei responsabili aziendali della protezione dei dati in base a specifici errori/difetti individuati		

Allegato 1: termini di conservazione / termini di prescrizione generali ai sensi del diritto federale

Oggetto	Termine di prescrizione (massimo)	Base legale	Note
Libri di commercio, relazione sulla gestione, documenti contabili importanti	10 anni	Art. 957 segg. CO	La contabilità «registra le operazioni e gli altri eventi necessari per esporre la situazione patrimoniale e finanziaria nonché i risultati d'esercizio dell'impresa (situazione economica)» (art. 957a cpv. 1 CO). In particolare, devono essere conservati i libri di commercio e i documenti contabili, che possono includere anche la corrispondenza commerciale relativa a un'operazione. I documenti importanti possono includere anche i contratti di lavoro e dell'istituto
Rivendicazioni generali in materia di diritto del lavoro	5 anni	Art. 128 CO	
Dati rilevanti per il certificato di lavoro	10 anni		Termine secondo la giurisprudenza
Dati salariali e documenti in materia di diritto del lavoro rilevanti ai fini fiscali	10 anni	Art. 958 f cpv. 1 CO; art. 126 cpv. 3 LIFD	
Documentazione del rispetto degli obblighi previsti dalla legge sul lavoro (in particolare, controllo del tempo di lavoro)	5 anni	Art. 73 cpv. 2 dell'ordinanza 1 concernente la legge sul lavoro	
Risarcimento/riparazione per lesione corporale/morte di una persona	3-20 anni	Art. 60 cpv. 1bis e art. 128 a CO	Può essere applicato ad ex collaboratori e ad ex clienti

Violazioni legate alla discriminazione di genere	3 mesi	Art. 8 cpv. 2 della legge federale sulla parità dei sessi	
Prestazioni delle assicurazioni sociali, contributi alle assicurazioni sociali o obbligo di restituzione	5 anni	Art. 24 e 25 LPGA	In caso di *infortuni* durante il rapporto di lavoro, tuttavia, si raccomanda di conservare i fascicoli del personale per 10 anni e in caso di infortuni gravi o malattie professionali per 30 anni (raccomandazione ad hoc LAINF n° 09/87; https://www.koordination.ch/fileadmin/files/ad-hoc/1987/09-87.pdf)

Allegato 2: requisiti per un registro delle attività di trattamento

I responsabili aziendali della protezione dei dati devono tenere un registro di tutte le attività di trattamento dei dati con le seguenti informazioni minime:

- identità dei responsabili aziendali della protezione dei dati
- finalità del trattamento
- categorie di persone interessate
- categorie di dati personali trattati
- categorie di destinatari dei dati
- periodo di conservazione dei dati personali o criteri per determinare tale periodo
- descrizione generale dei provvedimenti volti a garantire la sicurezza dei dati (provvedimenti di protezione tecnici e organizzativi adeguati)
- indicazione dello Stato in caso di comunicazione dei dati all'estero nonché comunicazione delle garanzie volte ad assicurare un'adeguata protezione dei dati