Incaricato cantonale della protezione dei dati
6501 Bellinzona
www.ti.ch/protezionedati

26.04.2023

Principali obblighi derivanti dalla LPDP

Motivo giustificativo dell'elaborazione di dati (art. 6 LPDP)

L'elaborazione sistematica di dati personali deve essere giustificata da una base legale. L'elaborazione puntuale di dati personali può essere giustificata, oltre che da una base legale, anche dalla necessità dei dati per l'adempimento di un compito legale o dal consenso libero e informato della persona interessata (per le definizioni di elaborazione sistematica e elaborazione puntuale – le quali rimangono sostanzialmente invariate rispetto alle definizioni previste dalla revisione totale della LPDP in corso - vedi: https://www4.ti.ch//fileadmin/CAN/SGCDS/ICPD/PDF/LPDP/Definizioni.pdf).

Sui motivi giustificativi di un'elaborazione di dati vedi anche il Messaggio n. 7061 del 18 marzo 2015 concernente la Modifica della Legge sulla protezione dei dati personali del 9 marzo 1987 (LPDP) riguardante i motivi giustificativi e i principi che reggono l'elaborazione di dati personali (art. 6 e 7 LPDP): https://www4.ti.ch/fileadmin/CAN/SGCDS/ICPD/PDF/DIRITTO_TI/m7061_01.pdf.

Osservanza dei principi generali della protezione dei dati (art. 7 LPDP e art. 4 cpv. 1 R LPDP)

L'elaborazione deve essere:

- **Lecita:** Il principio della liceità prescrive di esaminare la conformità delle elaborazioni di dati con l'insieme del diritto, e non soltanto con la legislazione sulla protezione dei dati. Una violazione del principio della liceità è data, ad esempio, quando dati personali sono elaborati usando violenza, minaccia, negligenza o dolo;
- **Trasparente:** la persona interessata deve essere adeguatamente informata (principio della buona fede);
- **Proporzionata:** i dati e il modo della loro elaborazione devono essere idonei e necessari e deve sussistere un rapporto ragionevole tra lo scopo perseguito dall'elaborazione e la violazione della personalità che ne risulta;
- **Limitata alle finalità** originariamente e trasparentemente indicate; Protetta è la fiducia del cittadino nello scopo dell'elaborazione legalmente previsto o deducibile dalle circostanze concrete secondo il principio della buona fede;
- **Esattezza dei dati:** i dati devono essere corretti, completi, veritieri e aggiornati;
- **Sicurezza dei dati:** l'elaborazione deve essere rispettosa delle esigenze tecniche e organizzative di sicurezza dei dati a garanzia della loro confidenzialità, autenticità, integrità e disponibilità.

Responsabilità per la protezione dei dati (art. 8 LPDP)

L'organo che elabora o fa elaborare dati personali per lo svolgimento dei suoi compiti legali è responsabile della protezione dei dati. Garantisce l'elaborazione dei dati in particolare nel rispetto dei motivi giustificativi, dei principi generali e degli obblighi previsti dalla LPDP. In caso di danni causati in seguito all'elaborazione di dati personali, l'organo responsabile ne risponde conformemente alla legge sulla responsabilità civile degli enti pubblici e degli agenti pubblici.

Obbligo d'informazione della persona interessata (art. 9 cpv. 2 LPDP e art. 7 R LPDP)

L'informazione migliora la trasparenza e rafforza la consapevolezza del cittadino riguardo all'insieme di elaborazioni di dati che lo concernono e riguardo ai suoi diritti, in particolare quando i dati vengono raccolti presso terzi. L'organo responsabile deve in particolare informare la persona interessata se i dati personali che la concernono sono utilizzati per uno scopo diverso da quello originario.

Obblighi relativi alla trasmissione di dati all'estero (art. 14*a* LPDP e art. 12*a* R LPDP)

I dati personali non possono essere trasmessi all'estero qualora la personalità della persona interessata possa subirne grave pregiudizio, dovuto in particolare all'assenza di una legislazione che assicuri una protezione adeguata. Se manca una legislazione che assicuri una protezione adeguata, dati personali possono essere trasmessi all'estero soltanto se:

a) garanzie sufficienti, segnatamente contrattuali, assicurano una protezione adeguata all'estero;
b) la persona interessata ha dato il suo consenso nel caso specifico;
c) nel caso specifico la trasmissione è indispensabile per tutelare un interesse pubblico preponderante oppure per accertare, esercitare o far valere un diritto in giustizia;
d) nel caso specifico la trasmissione è necessaria per proteggere la vita o l'incolumità fisica della persona interessata;
e) la persona interessata ha reso i dati accessibili a chiunque e non si è opposta formalmente alla loro elaborazione.

L'organo responsabile informa l'Incaricato cantonale della protezione dei dati sulle garanzie ai sensi del cpv. 2 lett. a). Laddove una protezione adeguata sia assicurata, la trasmissione è lecita se sono adempiute le condizioni valide per la trasmissione di dati in Svizzera.

Convenzione sulla protezione dei dati (art. 10 R LPDP)

La trasmissione di dati personali deve essere preceduta dalla stipulazione di una convenzione tra l'organo responsabile, proprietario dei dati, e il richiedente.

La convenzione deve indicare:

a) la base legale;
b) l'elenco dei dati personali soggetti alla trasmissione;
c) l'origine dei dati personali;
d) l'obbligo per il richiedente di garantire alla persona interessata il diritto d'accesso e le informazioni relative all'origine dei dati;
e) le misure di sicurezza incombenti al richiedente;
f) la riserva, a favore dell'Incaricato, di poter controllare in ogni momento l'utilizzazione dei dati trasmessi;
g) l'obbligo per il richiedente di ossequiare i principi della legislazione in materia di protezione dei dati;
h) le spese a carico del richiedente;
i) l'importo della pena convenzionale che verrà applicata in caso di violazione degli obblighi da parte del richiedente.

Se la trasmissione di dati personali è periodica, la convenzione deve pure contenere la frequenza della trasmissione e il riferimento all'ultimo aggiornamento dei dati.

Sicurezza dei dati (art. 17 LPDP e art. 14 R LPDP)

La sicurezza dei dati implica la protezione dei dati per il tramite di misure tecniche e organizzative intese a proteggere gli stessi dalla perdita, dall'abuso e dal danneggiamento, rispettivamente a garantirne l'integrità, la disponibilità, la confidenzialità e l'autenticità. Più il rischio per l'integrità, la disponibilità e la confidenzialità dei dati è elevato, più elevato deve essere il grado di sicurezza che le misure adottate offrono (approccio basato sui rischi). Gli accorgimenti tecnici devono perciò essere adeguati allo stato della tecnica, alla natura e all'estensione dell'elaborazione dei dati come pure al grado di probabilità e di gravità del rischio che l'elaborazione implica per i diritti delle persone.

Tra le misure di sicurezza figurano, in particolare:
a) l'autenticazione personalizzata a due fattori disponibile unicamente al personale autorizzato, con configurazione qualificata del tempo di validità, lunghezza, composizione e non ripetibilità;
b) la crittografia end-to-end;
c) il Backup di sicurezza;
d) gli impedimenti fisici di intrusione nei Data Center;
e) gli impianti ridondanti per prevenire l'interruzione di servizio;
f) la giornalizzazione degli accessi per la ricostruzione di eventi o responsabilità legate all'abuso dei dati;
g) le certificazioni (in particolare, ISO 27001);
h) il Networking isolato da altre reti (specialmente, da internet pubblico);
i) le configurazioni adeguate dei Firewalls
l) il regolare aggiornamento delle misure di sicurezza.

Registro degli archivi di dati (art. 19 LPDP e art. 15 R LPDP)

La LPDP prescrive all'organo responsabile di creare il registro degli archivi di dati. Vanno indicati, per ogni archivio, in particolare:
- denominazione
- base legale
- organo responsabile
- scopi
- categorie di dati elaborati
- modalità di elaborazione
- organi partecipanti e utenti
- mandatari
- destinatari di dati
- durata di conservazione
- misure di sicurezza.

Privacy by design (art. 18 cpv. 1 LPDP)

L'organo responsabile dell'elaborazione è tenuto ad adottare, fin dalla progettazione del trattamento, le misure appropriate per attuare le disposizioni sulla protezione dei dati (privacy by design). In generale, la protezione dei dati fin dalla progettazione non è legata a una determinata tecnologia. Si tratta piuttosto di progettare, sotto il profilo tecnico e organizzativo, i sistemi per l'elaborazione dei dati in modo tale da conformarli in particolare ai principi della protezione dei dati. In altre parole, il sistema deve attuare i requisiti per un'elaborazione dei dati conforme alla legge in modo tale da ridurre o escludere il rischio di violazioni delle disposizioni sulla protezione dei dati. È ad esempio possibile impostare un sistema di modo che i dati siano cancellati a intervalli regolari o anonimizzati in maniera standardizzata. Per la protezione fin dalla progettazione è d'importanza particolare che i dati raccolti siano ridotti al minimo indispensabile, affinché sia rispettato il principio della proporzionalità. Sin dall'inizio, l'elaborazione deve essere pertanto progettata in modo tale da raccogliere e trattare il minor numero possibile di dati o perlomeno in modo tale da doverli conservare meno tempo possibile. I provvedimenti da adottare devono essere adeguati in particolare allo stato della tecnica, alla natura e all'estensione dell'elaborazione dei dati come pure al grado di probabilità e di gravità del rischio che l'elaborazione implica per la personalità e i diritti fondamentali della persona interessata. La disposizione si basa su un approccio basato sui rischi. Il rischio che consegue da un'elaborazione deve essere messo in relazione con le possibilità tecniche di ridurlo. Quanto più alto è il rischio e la probabilità che si verifichi e quanto più ampia è l'elaborazione di dati, tanto più elevati dovranno essere i requisiti posti ai provvedimenti tecnici, affinché siano da ritenersi adeguati.

Obbligo di collaborazione con l'Incaricato (art. 30b cpv. 2, seconda frase)

L'organo responsabile dell'elaborazione deve collaborare con l'Incaricato nello svolgimento delle sue funzioni, in particolare collaborare all'istruttoria. L'Incaricato può esigere dall'organo responsabile, dal mandatario, dai destinatari di dati o dalla persona interessata, informazioni orali o scritte riguardanti l'elaborazione di dati. Può consultare tutti i documenti e incarti relativi a determinate elaborazioni, effettuare ispezioni e chiedere la presentazione di elaborazioni nonché gli accessi ai loro sistemi informatici. All'Incaricato non può essere opposto il segreto d'ufficio.

Consultazione preventiva dell'Incaricato (art. 18 cpv. 2 LPDP)

La norma prescrive di sottoporre determinati progetti di elaborazione di dati all'Incaricato per una consultazione preventiva (preavviso). Si tratta di progetti le cui elaborazioni sono effettuate con nuovi meccanismi, tecnologie o procedure che presentano dei rischi elevati. Anche i progetti legislativi che toccano la protezione dei dati vanno sottoposti preventivamente all'Incaricato. La consultazione preventiva permette all'Incaricato di intervenire a titolo preventivo e di consulenza, permettendo di risolvere eventuali problemi di protezione dei dati in una fase precoce del progetto.