OTIA

Ordine ingegneri e architetti
del Cantone Ticino

Bellinzona, 11 settembre 2023

Scheda informativa OTIA 2023-1

Applicazione della nuova Legge federale sulla protezione dei dati

La protezione dei dati è un tema di attualità, anche per gli studi attivi nei settori regolamentati da OTIA. Risulta quindi necessario conoscere le novità introdotte dalla revisione della Legge federale sulla protezione dei dati (nLPD) e della relativa Ordinanza (nOPDa), entrate in vigore il 1° settembre 2023, e adottare le giuste misure alfine di rispettare le nuove disposizioni legali.

In sintesi, la revisione impone un maggiore controllo dei dati che uno studio acquisisce, al fine di tutelare la privacy dei propri clienti, dei propri dipendenti e di altre presone fisiche con cui collabora.

Con la presente scheda informativa, OTIA desidera quindi informare i propri membri, in particolare i titolari di studi, delle novità legislative e delle misure da adottare per essere conformi alle nuove condizioni poste dalla nLPD e dalla nOPDa.

A. Campo di applicazione

Le nuove disposizioni legali si applicano al trattamento dei dati personali da parte di privati e quindi pure da parte degli studi attivi nei settori regolamentati da OTIA, in qualità di aziende private.

Le nuove disposizioni legali concernono il trattamento dei dati delle persone fisiche (e non di persone giuridiche), ad esempio di un proprio cliente, di persone fisiche che lavorano in studi con i quali avete una collaborazione (p. es. gruppi mandatari), dei propri dipendenti o degli utenti che visitano il vostro sito web o dei dati generati dai servizi di comunicazione e marketing a cui vi affidate.

Vale la pena ricordare che sussistono alcune situazioni non regolamentate dalla nLPD, ma che hanno delle norme di riferimento che vanno rispettate. Ad esempio: il divieto di sorveglianza ingiustificata sul luogo di lavoro è regolamentato dall'Ordinanza sul lavoro, le informative inerenti le cookies di navigazione e la profilazione (google analytics) dalla Legge sulle Telecomunicazioni e la limitazione del trattamento dati personali da parte del datore di lavoro dal Codice delle Obbligazioni. Per questo motivo la costellazione di norme che devono essere rispettate va conosciuta e analizzata sulla base delle singole situazioni. Una consulenza esterna da parte di uno specialista in queste materie diventa in pratica indispensabile.

Prima di presentare gli aspetti che gli studi devono considerare per adempiere alle nuove condizioni legali è necessario capire cosa si intende per *dati personali* e per *trattamento* di tali dati.

B. Dati personali

La nozione di *dati personali* comprende "tutte le informazioni relative a una persona identificata o identificabile" (art. 5 lett. a nLDP).

Una persona fisica, ad esempio un vostro dipendente, il mandante di un vostro progetto o un collega membro di un gruppo mandatario, è identificata o almeno identificabile se la sua identità può esser riconosciuta direttamente o indirettamente, in base a un solo elemento oppure correlando varie informazione risultanti dalle circostanze o dal contesto, come ad esempio il suo nome e cognome, un numero di telefono, il numero dell'immobile o il numero AVS o elementi specifici riguardanti le sue caratteristiche fisiche (uomo, donna o altro) ed economiche.

Anche se si tratta di un'evidenza, per i dati che trattate, dovete accertarvi, giusta l'art. 6 cpv. 5 nLPD, della loro esattezza. Ciò significa ad esempio la messa a giorno continua della propria banca dati.

C. Il trattamento dei dati

La nozione di *trattamento* concerne "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" (art. 5 lett. d nLPD). La lista non è esaustiva e quindi con trattamento di dati si deve pure intendere ad esempio la loro classificazione, archiviazione o analisi.

I dati possono essere raccolti, e di conseguenza trattati, soltanto per uno scopo determinato e riconoscibile per la persona interessata (vedi punto E.4 della presente scheda informativa). Non appena non sono più necessari per lo scopo del trattamento, essi devono essere distrutti. Con *distruzione*, che va oltre alla *cancellazione*, i dati devono essere eliminati in modo irreversibile.

> *Nella pratica:*
> *Se i dati sono su carta, essa dovrà essere bruciata o sminuzzata. Se i dati si trovano su un supporto informatico, come un CD o una chiave USB, occorre rendere inutilizzabili tali supporti. La situazione diventa più problematica in caso di memorizzazione dei dati su un server esterno. Inoltre, tutte le copie devono essere trattate in maniera tale che i dati non siano più leggibili. Se i dati personali sono allegati a un messaggio di posta elettronica, devono essere distrutti anche gli eventuali salvataggi intermedi del messaggio.*

D. I principi

Tra i principi (art. 6 nLDP) più importanti che devono sempre essere rispettati, troviamo il *principio della finalità* dei dati raccolti. I dati personali possono essere raccolti e usati soltanto per un determinato scopo e riconoscibile per la persona interessata, ossia per la persona a cui i dati si riferiscono (cliente, dipendente, ecc.).

Un altro principio introdotto dalla revisione è il *principio di distruzione e anonimizzazione*. I dati personali devono essere distrutti o resi anonimi appena non sono più necessari per lo scopo del trattamento e non appena il termine di conservazione è scaduto.

Nella pratica:
Gli studi non possono servirsi dei dati, ottenuti grazie a un contratto di mandato, per scopi promozionali, ad esempio inviare una e-mail al mandante per annunciare la vendita di appartamenti appena terminati, se il destinatario non ha accettato o non è stato informato in merito.

E. Le misure da adottare

Di seguito le misure da adottare per rispondere alle esigenze legali introdotte dalla revisione della LPD e della relativa Ordinanza.

1. Adozione di provvedimenti tecnici e organizzativi

Lo studio deve adottare adeguati *provvedimenti tecnici e organizzativi* necessari affinché siano rispettate tutte le disposizioni legislative e soprattutto i principi regolati dalla nLDP (art. 7 nLDP).

Tali provvedimenti devono essere adottati il più presto possibile (principio denominato privacy by design). L'idea soggiacente è che delle misure di protezione devono essere previste e implementate fin dall'avvio di qualsiasi attività relativa al trattamento di dati.

OTIA consiglia quindi di agire da subito, effettuando un'analisi dei dati da voi raccolti e definire le misure di protezione da adottare, istaurando, se non ancora fatto, delle procedure interne volte a garantire il rispetto della protezione dei dati.

I provvedimenti sono da attuare per tutta la durata d'esistenza dei dati raccolti.

Nella pratica:
Dalla definizione dei dati necessari per svolgere una determinata attività (come la partecipazione a un concorso di progetto, dove lo studio capofila raccoglie i dati degli studi che partecipano assieme al concorso), alla scelta dei software e dei programmi informatici, alla raccolta, all'utilizzo, all'archiviazione e all'eliminazione di documenti cartacei e digitali.

Una misura è adeguata se tiene conto dei costi di attuazione, della natura, del contesto e delle finalità del trattamento dei dati, nonché dei probabili rischi e della loro gravità per i diritti e le libertà delle persone interessate. Per quanto riguarda gli studi attivi nei settori regolamentati da OTIA, le nuove disposizioni legali non dovrebbero imporre l'adozione di complicate e costose misure.

OTIA consiglia comunque *agli studi di svolgere una specifica analisi dei dati che raccoglie e confrontarsi con uno specialista in ambito di protezione dei dati, in particolare per i dati raccolti di natura digitale.*

Il nuovo art. 7 nLDP esige pure una protezione tramite delle impostazioni predefinite (cosiddetta privacy by default), volte a proteggere la privacy. Ciò concerne essenzialmente le pagine web degli studi.

Le *misure tecniche* possono comprendere ad esempio, autorizzazioni e restrizioni di accesso ai dati personali dei propri collaboratori o dei propri clienti, sistemi di sicurezza informatici all'avanguardia, firewall, metodi di crittografia, autenticazione degli utenti, anonimizzazione, back-up dei dati,

cancellazione automatica. Le *misure organizzative* possono invece comprendere ad esempio, oltre l'implementazione di una cultura interna della gestione dei dati personali raccolti, la nomina di un responsabile per l'effettiva attuazione dei requisiti di protezione dei dati, la definizione e la gestione del trasferimento dei dati a terzi, la documentazione delle attività di trattamento, l'organizzazione di corsi di formazione interna e l'implementazione di controlli.

2. Analisi dei rischi per la gestione sicura dei dati

Lo studio che è titolare del trattamento deve garantire, tramite le misure tecniche e organizzative, una *sicurezza* dei dati personali adeguata al rischio (art. 8 nLDP). Ciò significa che gli studi dovranno intraprendere *un'analisi dei rischi* per la privacy e i diritti delle persone interessate.

> *Nella pratica:*
> *I rischi che si possono riscontrare sono l'accesso al proprio server da parte di persone non autorizzate, dei dati non corretti, la perdita/distruzione dei dati (quindi effettuare frequenti e regolari salvaguardie dei dati (back up)), la divulgazione accidentale ad estranei (p. es. di un preventivo dei costi con dati per la richiesta del credito di costruzione a una banca, inviati tramite e-mail a un altro cliente) o la conservazione più del necessario dei dati raccolti.*

Anche i fattori di rischio devono essere identificati, come ad esempio l'utilizzo di tecnologie non più attuali, decisioni individuali automatizzate, trattamento di dati personali degni di particolare attenzione ai sensi dell'art. 5 lett. c nLDP (ad esempio i dati concernenti le opinioni o attività religiose, filosofiche, politiche, sindacali, i dati riguardanti la salute o l'appartenenza a una razza o etnia, i dati biometrici che identifichino in modo univoco una persona fisica (p. es. riconoscimento facciale), le procedure e le sanzioni amministrative o penali, come il casellario giudiziale e le misure di assistenza sociale come gli assegni familiari) o combinazione di dati ottenuta attraverso processi diversi.

Anche se sussiste uno stretto legame tra la protezione dei dati e la sicurezza dei dati, le due nozioni vanno distinte. La protezione dei dati riguarda la tutela della personalità del singolo individuo. La sicurezza dei dati concerne invece in generale i dati presso un titolare o un responsabile del trattamento e riguarda il quadro tecnico e organizzativo del trattamento. La protezione dei dati della singola persona è pertanto possibile soltanto se sono implementati provvedimenti tecnici e organizzativi che garantiscono la sicurezza dei dati.

In caso di un elevato rischio e la sicurezza dei dati è violata, ovvero qualora avvenga la perdita, la cancellazione, la distruzione, l'alterazione involontaria o illecita oppure la divulgazione o accessibilità di dati personali a persone non autorizzate, il titolare del trattamento deve contattare senza indugio l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT; www.edoeb.admin.ch/ edoeb/it/ home.html).

3. Registro delle attività di trattamento

Le aziende con almeno 250 collaboratori sono obbligate a tenere un registro delle attività di trattamento. Le informazioni minime che deve contenere il registro sono regolate all'art. 12 nLDP.

Il registro è uno strumento pratico per conservare una visione d'insieme sulle attività di trattamento ed è consigliabile anche per le aziende più piccole. La legge non prescrive alcuna forma specifica, per

cui una tabella Excel è sufficiente. Se il trattamento dei dati personali comporta un alto rischio di violazione della personalità dei soggetti interessati, decade il numero minimo di 250. È quindi sufficiente che l'azienda gestisca uno dei dati citati al punto E.2 (dati personali degni di particolare attenzione) che automaticamente diventa necessario predisporre il registro delle attività di trattamento.

4. L'obbligo di informare e diritto d'accesso ai dati

L'*obbligo di informare* sulla raccolta di dati è stato esteso di principio a tutti i dati personali (art. 19 nLDP), contrariamente alla previgente legge che prevedeva un obbligo solo per i dati degni di particolare importanza. Dunque, al momento della raccolta dei dati di una persona, spetterà allo studio comunicare in modo chiaro e trasparente quali dati sono raccolti, da chi (identità e dati di contatto del titolare del trattamento), per quale scopo, eventuali destinatari o categorie di destinatari a cui vengono comunicati i dati personali e se i dati sono divulgati all'estero. Sono comunque previste delle eccezioni (art. 20 nLDP).

Consigliamo agli studi di dotarsi di una *dichiarazione di protezione dei dati* nella quale sono spiegati le sopra elencate informazioni (OTIA mette a disposizione sul suo sito un esempio di dichiarazione di protezione dei dati).

La dichiarazione deve essere visionata dai propri clienti all'inizio del mandato.

> *OTIA consiglia di redigere una direttiva (policy)* interna, per quanto concerne il trattamento dei dati personali dei propri dipendenti.
> *Per quanto riguarda invece il sito web, è necessario pubblicare sul sito in modo facilmente accessibile un'informativa sulla privacy completa, ovvero che fornisca informazioni sulle attività di trattamento dei dati e spieghi i diritti degli utenti.*
>
> *La persona interessata ha un diritto d'accesso ai propri dati, che è stato ampliato dalla revisione in esame. In particolar modo sono state estese le informazioni che un'azienda privata deve essere in grado di fornire alla persona richiedente (art. 25 cpv. 2 nLDP), ad esempio l'identità e i dati di contatto dello studio titolare del trattamento, i dati personali del dipendente o del cliente trattati, lo scopo del trattamento, la durata di conservazione dei dati personali o, se ciò non è possibile e i criteri per stabilire tale durata. Le informazioni devono essere comunicate di norma entro 30 giorni e senza alcun costo per il soggetto interessato.*

5. Dati trattati da terzi

Se terzi (p. es. fornitori di servizi Cloud, partner IT, Web host o fiduciarie) elaborano dati personali per conto dello studio (il cosiddetto *outsourcing*), lo studio rimane responsabile della protezione dei dati che ha raccolto e deve assicurarsi che i dati siano elaborati dai terzi (cosiddetto responsabile del trattamento) conformemente alla legge o al contratto firmato con i terzi. Un *accordo di trattamento dei dati* che regoli l'elaborazione e la sicurezza dei dati, tra lo studio, ovvero il titolare del trattamento, e il fornitore di servizi, ovvero il responsabile del trattamento, è necessario (art. 9 nLDP). I clienti, i dipendenti o gli utenti del sito web dello studio devono essere informati in merito all'outsourcing.

OTIA

In caso di *trasferimento dei dati personali all'estero* (art. 16 seg. nLDP), bisogna verificare che il Paese terzo disponga di un livello adeguato di protezione dei dati oppure è necessario adottare misure aggiuntive.

> *Nella pratica*
> *Molti studi utilizzano sistemi cloud per l'archiviazione dati e ciò implica la verifica che il provider del cloud abbia una struttura di archiviazione all'interno della Svizzera oppure in una giurisdizione in cui un Paese offre un livello adeguato di protezione dei dati. Per questo motivo i fornitori di servizi devono essere scelti con cura.*

F. Disposizioni penali

In merito alle disposizioni penali, si deve tener conto specialmente del fatto che la violazione intenzionale di alcuni obblighi previsti dalla legge comporterà una punibilità che non riguarda l'azienda, bensì la persona fisica responsabile, generalmente chi ricopre una funzione dirigenziale: non sono permesse deroghe alla responsabilità a meno che non si evidenzi in modo chiaro un grave errore del soggetto titolato a svolgere determinati compiti, cosa spesso difficile da dimostrare. Sono previste multe fino a 250'000 Fr.

Il contenuto della presente scheda informativa costituisce una sintesi illustrativa dei nuovi obblighi legali introdotti dalla revisione della LPD e della relativa ordinanza e, vista la complessità della materia, non sostituisce una specifica consulenza tecnica e legale. OTIA consiglia quindi di affidarsi a un esperto in materia.

Per maggiori informazioni: serviziogiuridico@otia.swiss