da oltre 100 anni
CAMERA DI COMMERCIO CANTONE TICINO
industria | artigianato | servizi

Cosa regola la Legge federale sulla protezione dei dati (nLPD)?

La nuova versione della LPD disciplina la protezione dei dati delle «persone fisiche» (definite nella nLPD come «persone interessate»).

Si parla di dati personali.

Nella nLPD i dati personali sono definiti come «tutte le informazioni concernenti una persona fisica identificata o identificabile», cioè che fanno riferimento a persone).

Coloro che trattano dati personali e determinano gli scopi e i mezzi del trattamento sono chiamati **titolari del trattamento**. Qualora i titolari del trattamento ricorrano a prestatori di servizi che trattano i dati personali per loro conto e secondo le loro istruzioni, tali prestatori coinvolti sono considerati responsabili del trattamento.

Nell'ambito di applicazione della nLPD, i titolari e (in misura minore) anche i responsabili del trattamento devono rispettare le disposizioni della nLPD. Inoltre, i responsabili del trattamento sono obbligati contrattualmente dal titolare del trattamento a rispettare determinate disposizioni. In questo modo, anche i responsabili del trattamento sono tenuti a rispettare la nLPD.

Grazie alla nLPD, le persone interessate possono avanzare pretese nei confronti dei titolari del trattamento dei dati se questi trattano i loro dati personali in maniera eccessiva, scorretta o altrimenti illecita e comunque non conforme allo scopo per i quali i dati vengono raccolti.
In tal caso vi possono essere pretese di diritto privato che portano a chiedere una modifica del comportamento nei confronti del titolare del trattamento interessato.

I titolari del trattamento possono essere controllati anche dall'IFPDT (Incaricato federale della protezione dei dati e della trasparenza).
Inoltre, i collaboratori dei titolari o dei responsabili del trattamento aventi potere decisionale (di regola persone con funzioni manageriali) possono essere perseguiti penalmente per determinate violazioni della nLPD.

La nLPD viene integrata e precisata dalle disposizioni d'esecuzione contenute nella nuova Ordinanza sulla protezione dei dati (OPDa) e nella nuova Ordinanza sulle certificazioni in materia di protezione dei dati (OCPD).

Entrata in vigore della nLPD

La nuova nLPD è entrata in vigore il **1° settembre 2023**.

In dettaglio:

La nuova LPD entra in vigore il 1° settembre 2023. Essa sostituisce in tale data la legge precedente, in vigore in Svizzera dal 1° gennaio 1993.
Il testo definitivo della nuova LPD è stato approvato dal Parlamento il 25 settembre 2020.
Le aziende avevano quindi 3 anni di tempo per adeguare il loro trattamento dei dati ai nuovi requisiti. Per questo motivo, la legge non concede nessun ulteriore periodo di tolleranza.

Alcune disposizioni della nLPD (art. 7 nLPD: protezione dei dati personali sin dalla progettazione e per impostazione predefinita; art. 22 e seg. nLPD: valutazione d'impatto sulla protezione dei dati) non si applicano ai trattamenti di dati iniziati prima dell'entrata in vigore della nLPD (cosiddetto «grandfathering»).

Tuttavia, ciò avviene solo se e nella misura in cui:

(a) lo scopo del trattamento dei dati non è cambiato e
(b) non vengono raccolti nuovi dati nel quadro del trattamento dei dati.

È quindi possibile trasferire un «database di dati vecchi» su un nuovo sistema informatico senza adeguare la tecnologia al nuovo stato giuridico più elevato.

Non devono però mai esserci compromessi sulla sicurezza dei dati (art. 8 nLPD), pertanto per questi motivi sono necessari aggiornamenti tecnici anche per i database di dati preesistenti.

Le inchieste dell'IFPDT già pendenti al momento della sua entrata in vigore restano soggette alla legislazione precedente.

Se l'IF DT ha intentato un'azione legale presso il Tribunale amministrativo federale prima del 1° settembre 2023, l'azione sarà giudicata secondo il diritto previgente.

Per quali trattamenti di dati si applica la nLPD?

La nLPD si applica ai trattamenti di dati effettuati in Svizzera o con effetto in Svizzera (principio degli effetti).

Chi deve rispettare la nLPD?

La nLPD si applica in ambito privato e per le autorità federali. Protegge le persone private. Per i dati sulle aziende vige una regolamentazione speciale per 5 anni che si rivolge alle autorità federali.
In ambito privato, già a partire dal 1° settembre 2023 la nLPD tutelerà solo gli individui e non più le persone giuridiche.

In dettaglio:

In breve, la nLPD vale «in Svizzera» per «coloro che le sottostanno».
Questi due aspetti sono definiti «campo di applicazione territoriale» e «campo di applicazione personale».

Campo di applicazione personale
La nLPD si applica alle autorità federali.
La nLPD si applica anche a tutte le organizzazioni private che trattano dati personali in qualità di titolari o responsabili del trattamento nel campo di applicazione territoriale. Sono quindi considerate tutte le ditte individuali, le società anonime di diritto privato, le Sagl, le associazioni e le fondazioni.
La nLPD non si applica a comuni e cantoni e alle relative autorità. Pertanto, la nLPD non si applica, ad esempio, alle scuole, per le quali valgono le leggi cantonali sulla protezione dei dati, con regole in gran parte simili a quelle della nLPD.
In Ticino si sta modificando la relativa base legale cantonale.
Per gli ospedali organizzati a livello cantonale, le centrali elettriche e simili la situazione giuridica è un po' più complicata.

Campo di applicazione territoriale
la nLPD si applica quando si producono effetti in Svizzera (principio degli effetti). In tali casi vanno rispettati gli obblighi della nLPD. Ciò vale per i provvedimenti dell'IFPDT e per l'applicazione del diritto privato.
Per l'applicazione del diritto penale, invece, si applica il principio di territorialità penale: sono punibili solo le violazioni delle disposizioni penali della nLPD commesse in Svizzera.

Chi è protetto dalla nLPD?

La nLPD protegge le persone, mentre in linea di massima non protegge più le aziende (esistono tuttavia regole speciali per i dati aziendali per 5 anni dall'entrata in vigore; tali regole si rivolgono alle Autorità federali).

In dettaglio:

Dati personali: si tratta di informazioni che descrivono una persona in modo direttamente o indirettamente identificabile. La legge parla di «informazioni concernenti una persona fisica identificata o identificabile», ossia hanno un «riferimento a persone».

Dati aziendali: in virtù della legislazione federale in vigore, le autorità federali hanno ancora il diritto, per cinque anni, di trasmettere (comunicare) ad altri uffici federali i dati ricevuti da un'azienda. In tale contesto devono essere rispettate le disposizioni giuridiche della Legge sull'organizzazione del Governo *e* dell'Amministrazione (LOGA).

Per quanto riguarda l'utilizzo di tali dati, esiste una regolamentazione specifica che, pur non essendo particolarmente chiara, recita: «Per gli organi federali, le disposizioni di altri atti normativi federali che si riferiscono a dati personali continuano ad applicarsi ai dati concernenti persone giuridiche durante cinque anni dall'entrata in vigore della presente legge.»

Quali ruoli bisogna conoscere per comprendere l'economia dei dati?

L'economia dei dati si svolge tra i titolari del trattamento e le persone interessate per quanto riguarda i loro dati personali. L'economia dei dati si estende anche a eventuali dati ulteriori (altri dati, ovvero quelli che non sono dati personali; chiamati anche «dati non personali»). Nell'ambito di applicazione della nLPD, i prestatori di servizi coinvolti dai titolari del trattamento vengono definiti «responsabili del trattamento».

Anche lo scambio dai titolari ad altri titolari è un processo importante. Al di fuori del campo di applicazione della nLPD si può parlare, ad esempio per i «dati non personali», di fornitore di dati (provider di dati) o di destinatario di dati (utente di dati). Nel linguaggio della nLPD, lo scambio tra fornitore e destinatario dei dati verrebbe trattato come uno scambio tra due titolari indipendenti l'uno dall'altro (cosiddetto «trasferimento controller-to-controller»).

In dettaglio:

Chi tratta dati personali determinando a tal fine scopi e mezzi è considerato titolare del trattamento.
Qualora il titolare ricorra a prestatori di servizi che trattano i dati personali per suo conto e secondo le sue istruzioni, tali prestatori di servizi coinvolti sono considerati responsabili del trattamento.
Chi riceve dati personali dal titolare del trattamento e decide (può decidere) autonomamente in merito alle finalità e ai mezzi del loro trattamento *è* di per sé titolare del trattamento (in qualità di «destinatario dei dati»).

Qual è la differenza tra LPD e RGPD?

Il RGPD UE (il regolamento generale sulla protezione dei dati dell'UE) è la legge sulla protezione dei dati dell'UE. La nLPD è l'equivalente per la Svizzera. Le regole non sono identiche, ma dal punto di vista attuale sono equivalenti.

In dettaglio:

Una delle grandi differenze concettuali tra il RGPD e la nLPD è il sistema di sanzioni. Il RGPD non prevede sanzioni penali, ma consente alle autorità preposte alla protezione dei dati di emettere sanzioni amministrative di importo considerevole.
Anche secondo la nLPD sono possibili sanzioni amministrative in via eccezionale (sanzionamento del titolare con una multa massima di CHF 50'000. -). In linea di massima, tuttavia, i sanzionamenti si basano sul diritto penale.
La persona che agisce nello specifico può essere punita con una multa fino a CHF 250'000.-.

da oltre 100 anni
CAMERA DI COMMERCIO CANTONE TICINO
industria | artigianato | servizi

Diritto penale: chi è responsabile della protezione dei dati?

Secondo l'intenzione del legislatore le sanzioni penali della nLPD devono essere rivolte agli amministratori. Tuttavia, la legge non esclude del tutto la punibilità dei collaboratori.
Si è così creata una regola piuttosto complessa, in base alla quale anche l'azienda può rispondere penalmente.

In dettaglio:

Se qualcosa va storto nel diritto sulla protezione dei dati, ciò avviene perlopiù nelle aziende. Di conseguenza, la nLPD (nello specifico: art. 64 nLPD) indica come direttamente applicabile una regola speciale (nello specifico: artt. 6 e 7 della Legge federale sul diritto penale amministrativo) ai sensi della quale gli amministratori sono sanzionati per le violazioni della protezione dei dati che non hanno evitato «in violazione di un obbligo giuridico». La regola prevede anche una fattispecie residuale in base alla quale l'azienda può essere sanzionata.

Di conseguenza, rispondono penalmente le seguenti persone:

Amministrazione: il diritto in materia di protezione dei dati è rivolto ai titolari, e quindi spesso alle aziende, e poiché un amministratore è responsabile dell'organizzazione dell'attività aziendale, gli amministratori potrebbero essere regolarmente responsabili in caso di violazioni della protezione dei dati (questo aspetto è tuttavia oggetto di critiche).

L'amministratore può già essere punito se è stato negligente *e* se la violazione della protezione dei dati si sarebbe potuta evitare senza il comportamento negligente.
Inoltre, deve essere dimostrato che si è verificata una fattispecie secondo l'elenco dei reati della nLPD; devono sussistere almeno la tipicità della fattispecie e l'illiceità. Almeno questo è quanto dice la legge.

Bisognerà vedere cosa porterà la pratica. Gli amministratori possono essere punibili, secondo la norma, anche se l'individuo che ha commesso l'azione non può essere punito. Gli amministratori potrebbero quindi essere sanzionati in tempi relativamente brevi per le violazioni della protezione dei dati, secondo quanto previsto dalla legge. L'importo massimo della multa ammonta a CHF 250’000. - .

Diritto amministrativo: chi è responsabile della protezione dei dati?

In caso di violazioni della protezione dei dati, l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) può aprire una procedura d'inchiesta amministrativa, nell'ambito della quale può emanare decisioni.

In dettaglio:

L'IFPDT può imporre al titolare del trattamento, mediante disposizioni emanate nell'ambito delle proprie inchieste, di adottare misure volte a favorire il successo della protezione dei dati. Chi non ottempera a tali disposizioni rischia sanzioni penali (si veda sopra).

L'IFPDT da solo non può tuttavia imporre sanzioni penali.

Diritto civile: chi è responsabile della protezione dei dati?

Chi, sulla base di un contratto, è tenuto alla diligenza prevista dal diritto in materia di protezione dei dati nei confronti di terzi, può essere ritenuto responsabile di una violazione della protezione dei dati. Le basi sono stabilite nella nLPD o eventualmente in un contratto in cui il titolare del trattamento si è impegnato a rispettare il diritto in materia di protezione dei dati.

In dettaglio:

Molto spesso la persona interessata non ha un rapporto contrattuale diretto con il titolare del trattamento che ha violato la legge sulla protezione dei dati. La persona interessata può quindi avvalersi dei mezzi di ricorso legali *e* intentare un'azione di cessazione della violazione della protezione dei dati o un'azione inibitoria preventiva di ulteriori comportamenti che violano il diritto.
In teoria, alla persona interessata è aperta anche un'azione di risarcimento del danno. Tuttavia, sarà spesso molto difficile individuare un danno direttamente risultante. E il risarcimento di ulteriori danni potrebbe fallire a causa di altri requisiti del diritto in materia di responsabilità.
Le azioni di risarcimento del danno sono plausibili se il titolare o il responsabile del trattamento dei dati si è impegnato in un contratto a rispettare la legge sulla protezione dei dati. In caso di violazione della protezione dei dati può rispondere, ad esempio, dei danni diretti (costi del monitoraggio del dark web dopo un data breach) o, di solito a condizioni più severe, anche dei danni indiretti (perdita di fatturato a causa di un danno alla reputazione).

Quali sono le responsabilità in qualità di fornitore di servizi IT coinvolto?

In qualità di fornitore di servizi IT, solitamente vi è un cosiddetto «responsabile del trattamento» e ha un rapporto contrattuale con il titolare del trattamento. In questo modo si risponde secondo le regole contrattuali nei confronti del titolare del trattamento, ma quasi mai anche nei confronti della persona interessata. Tuttavia, la violazione intenzionale delle disposizioni in materia di protezione dei dati può comportare sanzioni penali.

In dettaglio:

I fornitori di servizi IT ricoprono spesso il ruolo di responsabili del trattamento. Ciò avviene quando si è coinvolti concretamente nel trattamento dei dati nell'ambito della propria attività per conto del titolare del trattamento.

Esempio:

Hosting di dati: Il provider del servizio di hosting dei dati è un responsabile del trattamento anche quando misure tecniche gli impediscono di accedere ai dati personali direttamente.
Tuttavia, nel valutare le disposizioni di legge applicabili occorre tenere conto del fatto che il provider di dati nell'esempio non ha accesso ai dati personali direttamente.

Quali altre disposizioni in materia di protezione dei dati devono essere rispettate?

Con protezione dei dati si intende spesso qualcosa di più di ciò che è disciplinato nella nLPD.
Nello specifico si può intendere quanto segue:

- regole per la protezione delle informazioni, perché si è obbligati a farlo per contratto (ad es. accordo di non divulgazione);
- regole che richiedono una certa diligenza o altri obblighi comportamentali nel trattamento delle informazioni per conto di terzi, ad esempio al fine di tutelare il sistema del mercato finanziario (regole della FINMA);
- regole che l'azienda si è autoimposta per realizzare il proprio obiettivo costruttivo (politica aziendale propria: qui non si tratta di dovere o potere, ma di volere);
- e, da ultimo, anche le regole per la protezione dei dati personali. In tale contesto possono essere considerate le regole della nLPD così come le regole del Regolamento generale europeo sulla protezione dei dati (RGPD), a seconda della loro applicazione.

In dettaglio:

Sul RGPD
Chi, in qualità di titolare del trattamento, orienta in modo chiaro i propri servizi al mercato dei consumatori dell'UE è tenuto a rispettare il RGPD relativamente al trattamento di tali dati.
Chi osserva persone interessate nell'UE in qualità di titolare del trattamento deve attenersi al RGPD.
Chi opera in qualità di responsabile del trattamento con sede in Svizzera per un titolare del trattamento con sede nell'UE deve fornire un servizio che consenta al titolare del trattamento di rispettare le disposizioni del RGPD; tuttavia, il RGPD non si applica direttamente al responsabile del trattamento.

Viceversa, il titolare del trattamento in Svizzera che si avvale di un responsabile del trattamento con sede nell'UE deve rispettare le disposizioni del RGPD non solo per il coinvolgimento di un responsabile del trattamento UE; ciò vale indipendentemente dal fatto che il responsabile del trattamento stesso sia direttamente soggetto al RGPD.

Regole specifiche per settore
Chi opera in un particolare settore deve rispettare le regole applicabili nel settore stesso. Le banche devono ad esempio rispettare le regole della FINMA (vigilanza bancaria). A differenza delle disposizioni della nLPD, le regole della vigilanza bancaria hanno lo scopo di proteggere il sistema, mentre la nLPD e il GDPR hanno lo scopo di proteggere gli individui.
Le assicurazioni malattia devono inoltre rispettare le regole dell'Ufficio federale della sanità pubblica, anch'esse finalizzate alla protezione del sistema.
Le banche sono anche tenute a rispettare il segreto bancario, a sua volta finalizzato alla protezione individuale, proprio come la nLPD.
Regole per l'amministrazione pubblica: Alle autorità amministrative si applica una forma particolare di regole «settoriali». I comuni, le scuole e, ad esempio, le aziende elettriche sono tenuti a rispettare le disposizioni cantonali e, in determinate circostanze, le leggi cantonali.
Le autorità sono inoltre tenute a mantenere la segretezza.
Autoregolamentazione in materia di riciclaggio di denaro: In un mondo digitale sono molteplici le attività che hanno un legame con i dati e talvolta anche con i dati personali, motivo per cui anche i regolamenti per la protezione contro il riciclaggio di denaro contengono riferimenti a dati personali e affini, sebbene i relativi regolamenti (ad es. ARIF o OAD Fiduciari Suisse) servano più alla protezione del sistema che alla protezione individuale.

Disposizioni speciali
Se una determinata attività stabilisce una disposizione di protezione supplementare, si può concludere che ciò comporterebbe un inasprimento, al quale occorre prestare particolare attenzione.
A titolo di esempio si possono citare le disposizioni del diritto obbligazionario per il datore di lavoro a tutela del proprio personale, nonché le disposizioni di legge particolari del diritto cantonale, che disciplinano, ad esempio, l'obbligo di riservatezza nel diritto di adozione o nel settore fiscale («segreto fiscale»).
Tuttavia, questa conclusione intuitivamente comprensibile è spesso infondata; spesso tali disposizioni speciali si limitano ai diritti e agli obblighi generali che derivano già dal diritto in materia di segretezza o dal diritto generale sulla protezione dei dati.
Nella maggior parte dei casi vale la pena di esaminare con obiettività la finalità di tali regole.

Obbligo di conservazione e cancellazione

Per quanto tempo è consentito conservare la documentazione di collaboratori o candidati?

Il datore di lavoro può conservare i fascicoli personali dei collaboratori per tutta la durata del rapporto di lavoro e in seguito per un periodo di tempo limitato a fini di archiviazione (regola generale: più cinque anni). Il periodo di conservazione per i candidati respinti è più breve, ma il fascicolo deve essere conservato per tre anni interi e successivamente fino alla fine dell'esercizio finanziario in corso in quel momento.
In alcuni settori (ad esempio nella previdenza professionale) i periodi di conservazione possono essere più lunghi.

Il datore di lavoro può conservare i fascicoli personali dei collaboratori per tutta la durata del rapporto di lavoro e in seguito per un periodo di tempo limitato a fini di archiviazione (regola generale: più cinque anni). Il periodo di conservazione per i candidati respinti è più breve, ma il fascicolo può essere conservato per tre anni interi e successivamente fino alla fine del rapporto di lavoro.

In dettaglio:

Il datore di lavoro può conservare i fascicoli personali dei collaboratori per tutta la durata del rapporto di lavoro e in seguito, sulla base delle regole generali, per ben cinque anni dopo la sua cessazione fino alla fine dell'esercizio finanziario in corso (quindi in singoli casi quasi fino a sei anni dopo la cessazione del rapporto di lavoro).
Dopo la cessazione del rapporto di lavoro, lo scopo del trattamento deve tuttavia essere limitato (scopo di archiviazione). Tali dati possono essere utilizzati per la difesa da rivendicazioni legali o in presenza di un interesse altrimenti preponderante.
In caso contrario non si dovrebbe più accedere a tali dati (già in precedenza, quando si accede ai dati personali di collaboratori occorre tutelare in modo particolare la loro personalità sul posto di lavoro: «nessuna sorveglianza dei collaboratori»).

I candidati respinti non hanno instaurato un rapporto di lavoro valido e pertanto si applicano le regole della responsabilità precontrattuale. Tali diritti sono soggetti a un termine di prescrizione di tre anni, per cui la responsabilità può essere esclusa solo al termine dell'anno fiscale in cui cade il termine del termine di prescrizione. Ciò autorizza il titolare del trattamento a conservare i dossier relativi ai candidati fino a tale data. Nella pratica, tuttavia, i periodi di conservazione dei candidati respinti sono spesso più brevi.

Se i dossier sono giunti in copia cartacea per posta, si usa la formula «ritorno a nostro discarico»; se i documenti arrivassero via e-mail, potrebbe essere utile una formulazione corrispondente («Cancelleremo dopo x [periodo]») per garantire trasparenza.
I titolari del trattamento dovrebbero predisporre un'informativa sulla protezione dei dati per i candidati respinti e per il proprio personale.

Per quanto tempo è concesso conservare i dati dei clienti?

I dati dei clienti possono essere conservati per il tempo necessario allo scopo. I clienti intrattengono con l'azienda un rapporto contrattuale di scambio. Dai contratti risultano termini di prescrizione che vanno dai cinque ai dieci anni. A seconda del settore, tuttavia, i periodi di conservazione possono essere notevolmente più lunghi (ad esempio nella previdenza professionale).

In dettaglio:

Un titolare del trattamento è autorizzato alla conservazione dei dati personali dei propri clienti per tutto il tempo in cui persegue un proprio interesse superiore. Quest'ultimo consiste nel fatto che il titolare del trattamento deve potersi difendere nei confronti delle pretese del cliente e, a tal fine, basarsi su contratti e altri documenti che riguardano il cliente. La protezione dei dati non deve portare a minare la «parità delle armi» per eventuali processi civili.

Una volta scaduti i termini di prescrizione, di regola non sussiste più alcun motivo per conservare tali documenti, che quindi devono essere cancellati. Dopo la cessazione del rapporto di lavoro, lo scopo del trattamento deve tuttavia essere limitato (scopo di archiviazione).
Tali dati possono essere utilizzati per la difesa da rivendicazioni legali o in presenza di un interesse altrimenti preponderante. In caso contrario non si deve più accedere a tali dati.

Esempi:

Documenti fiscali (dichiarazione d'imposta) presso i fiduciari
Risposta: 6 anni dopo la scadenza della valutazione definitiva per il periodo fiscale interessato. Un fiduciario che redige la dichiarazione dei redditi per un contribuente risponde in qualità di mandatario. I diritti cadono in prescrizione dopo cinque anni dalla valutazione definitiva da parte de/l'autorità fiscale per il periodo fiscale in questione (o dopo la cessazione del mandato relativo al periodo fiscale, se quest'ultimo è cessato prima della ricezione della valutazione definitiva). A sua volta, si applica la regola secondo cui la facoltà di custodia cessa alla fine dell'esercizio finanziario nel quale scade il termine di prescrizione. La risposta «6 anni» va quindi interpretata come approssimazione.

Lista dei partecipanti a un evento
Risposta:11 anni. Motivazione: I partecipanti a un evento intrattengono con /'organizzatore un rapporto contrattuale, a seconda dei casi. Se fosse così, potrebbero far valere le loro pretese nei confronti dell'organizzatore per dieci anni.
A sua volta, si applica la regola secondo cui la facoltà di custodia cessa alla fine de/l'esercizio finanziario nel quale scade il termine di prescrizione. La risposta «11 anni» va quindi interpretata come approssimazione.

Elenco dei destinatari di un invio
Risposta: 4 anni. Il semplice opt-in per l'invio di un'e-mail non dovrebbe costituire un rapporto contrattuale. Vanno quindi applicate le regole della responsabilità precontrattuale e dell'atto illecito. Vige un termine di prescrizione di tre anni. A sua volta, si applica la regola secondo cui la facoltà di custodia cessa alla fine de/l'esercizio finanziario nel quale scade il termine di prescrizione. La risposta «4 anni» va quindi interpretata come approssimazione.

Elenco degli interessi delle persone in relazione a un prodotto
In generale, la conservazione delle preferenze di una persona è una raccolta di dati che deve essere strutturata in modo trasparente e rispettare il principio di proporzionalità. Il periodo di conservazione non può essere definito in modo schematico e dipende anche dalla durata di vita del prodotto (l'interesse per le offerte del Food Truck nel centro commerciale è molto breve, l'interesse per le offerte di una pompa di alimentazione per una centrale idroelettrica dovrebbe durare molto più tempo; a ciò si aggiunge il fatto che la personalità della persona interessata a una centrale idroelettrica passa in secondo piano rispetto all'azienda che rappresenta, per cui già per questo motivo sorge un'altra ponderazione degli interessi: «Contesto B2B»).
Le newsletter con opzione di opt-out aiutano in questo caso a rinnovare /'interesse e a dare alla persona interessata la possibilità di disdire l'iscrizione alla newsletter, esprimendo così di non avere più interesse per il prodotto in questione.

Come si garantisce l'obbligo di conservazione quando i dati personali devono essere cancellati?

Se i dati personali devono ancora essere conservati per ottemperare a un obbligo legale di conservazione, non è necessario cancellarli.

In dettaglio:

Gli esempi sopra illustrati mostrano da quali considerazioni scaturiscono gli obblighi di conservazione e perché, nell'ambito della proporzionalità, ciò comporta che i dati personali non devono essere cancellati prima della scadenza di tali obblighi.
Una volta che i dati personali non sono più necessari per l'adempimento del contratto, è opportuno conservarli solo a scopo di archiviazione. Non si dovrebbe quindi più accedere a questi dati nella quotidianità.

La persona interessata può contattare il titolare del trattamento prima della scadenza del periodo di conservazione e richiedere la cancellazione dei propri dati. In determinate circostanze è già possibile cancellare aspetti parziali dei propri dati che non sono più necessari prima della scadenza del periodo di conservazione dell'archivio (ad esempio dati di marketing relativi alla persona, come interessi o cronologia delle attività), ma non i documenti relativi ai propri contratti.

Se le parti concordano sul fatto che il cliente non intenda più avanzare pretese nei confronti del titolare del trattamento, anche se il termine di prescrizione non è ancora scaduto, è possibile ottenere la cancellazione dei documenti contrattuali.

Marketing

È obbligatorio inserire un banner sui cookie sul sito web?

No, secondo il diritto svizzero il banner sui cookie non è obbligatorio.

In dettaglio:

I banner sui cookie sono regole che non derivano dal diritto in materia di protezione dei dati in senso stretto (ad es. nLPD o RGPD). Ciononostante, si sono consolidati nell'area dell'UE, poiché difficilmente i requisiti di consenso vigenti in tale area nell'ambito dei cookie e di tecnologie analoghe possono essere attuati diversamente.

In Svizzera non c'è ancora una regola di opt-in, bastano solo un'indicazione di trasparenza e un avviso che indica la possibilità di rifiutare (che può trovarsi anche nelle impostazioni del browser). L'indicazione di trasparenza può essere realizzata anche con un banner sui cookie. Tuttavia, l'indicazione di trasparenza può essere riportata anche nell'informativa sulla privacy o in una dichiarazione di trasparenza separata per il sito web.

Se l'indicazione di trasparenza è inserita in un banner sui cookie, questo può essere configurato in modo tale che scompaia o si chiuda automaticamente dopo alcuni clic («navigazione sul sito»), oppure si può configurare la funzione clic sul banner con «Chiudi avviso» o «Ho capito». La chiusura tramite clic può essere impostata come consenso («Accetta» anziché «Chiudi avviso»), ma è piuttosto sconsigliato. Perché? l'utente potrebbe infatti dedurre che il gestore del sito web si sia sottoposto di propria iniziativa a un regime di consenso (nel quale i cookie devono essere cancellati in caso di consenso negato o revocato).

I banner sui cookie possono quindi avere persino effetti negativi in Svizzera (a parte il fatto che sono fastidiosi). Si consiglia di rinunciarvi o comunque di utilizzarli solo se la trasparenza non è possibile in altro modo, come nell'informativa sulla protezione dei dati (ma in questo caso solo cliccando su «Chiudi avviso», non con l'invito «Accetta»).

Cosa deve essere menzionato nell'informativa sulla privacy presente sul sito web?

Le informazioni minime di un'informativa sulla privacy sono le seguenti:

- Chi è il titolare del trattamento e come lo si può contattare?
- A quale scopo vengono trattati i dati? (Finalità del trattamento)
- Chi riceve dal titolare del trattamento i dati personali della persona interessata?
- Si tratta di destinatari o categorie di destinatari; con questo termine non si intendono solo i titolari del trattamento, ma anche i responsabili del trattamento (anche se questi ultimi in realtà sono in contraddizione con il sistema).
- In quali Paesi vengono trasmessi i dati personali? (indicazione del Paese di destinazione con garanzie).

Se i dati personali vengono raccolti presso terzi e non presso la persona interessata, è necessario indicare anche quali categorie di dati personali vengono raccolte dal titolare del trattamento.

Bisogna considerare quanto segue: l'informativa sulla protezione dei dati è una «dichiarazione», non fa parte di un contratto. Quindi non comprende l'opzione «Accetto...», ma «Le informazioni sul nostro trattamento dei suoi dati personali sono reperibili...» oppure «... e prendo atto della dichiarazione sulla protezione dei dati.» (senza casella di controllo!) l'implementazione online è possibile e sensata anche per il trattamento offline.

Rimando alla dichiarazione sulla protezione dei dati (indicando l'URL o con link) nelle e-mail o offerte scritte.

Cosa cambia per l'invio di una newsletter? Le newsletter ai nuovi clienti possono essere inviate solo previo consenso esplicito (single opt-in o double opt-in)?

Con la nLPD non cambia nulla per quanto riguarda l'invio delle newsletter.

In dettaglio:

Per l'invio delle newsletter occorre distinguere tra diverse fasi di trattamento:

Raccolta dei dati: la raccolta dei dati deve essere conforme ai principi della nLPD.

Invio: l'invio deve essere conforme alle regole della Legge federale contro la concorrenza sleale (LCSI). Senza opt-in è possibile recapitare a una singola persona solo comunicazioni di massa via e-mail se si tratta di un cliente preesistente per gli argomenti pubblicizzati. Se non è richiesto un opt-in, occorre comunque dare la possibilità di opt-out.

Osservazione: Poiché i reparti di marketing controllano anche i tassi di apertura e altri elementi simili, il che costituisce di per sé un trattamento dei dati, è opportuno inserire già nella newsletter un link all'informativa sulla protezione dei dati a cui si fa riferimento.

L'utilizzo di Google Analytics è consentito (senza consenso)?

Sì, è possibile secondo la legge svizzera.

I gestori di siti web possono utilizzare Google Analytics senza il consenso dei visitatori del sito. Tuttavia, in qualità di gestori di siti web, potete migliorare la situazione adottando misure di conformità.

Tuttavia, è sempre più difficile ignorare il fatto che molti visitatori di siti web si sentono ancora a disagio. Questo disagio è legato al fatto che l'ecosistema globale attraverso il quale vengono intermediati gli spazi pubblicitari sembra poco trasparente sia dal punto di vista del gestore del sito web sia da quello dell'utente. Ci si dovrebbe chiedere seriamente se non sia meglio utilizzare soluzioni che si conoscono davvero.

In dettaglio:

Nella misura in cui Google Analytics viene ancora utilizzato in una versione basata sui cookie, è necessario osservare le norme speciali in materia di cookie previste dalla legislazione svizzera: La legge sulle telecomunicazioni (LTC) deve essere rispettata quando si tratta di cookie. Tuttavia, queste regole non sono cambiate con la revisione della protezione dei dati.
La LTC richiede (a) informazioni sullo scopo dei cookie utilizzati e (b) un riferimento al diritto di

opt-out (possibilità di rifiuto). Sono pertanto necessarie misure sul sito web, in particolare avvisi di trasparenza. Sono poi necessarie misure nei confronti di Google: un contratto di outsourcing dell'elaborazione dati e l'impostazione della funzione di anonimizzazione dell'IP.

Gli avvisi di trasparenza sul sito web sono (a) spiegazioni sui motivi per cui viene utilizzato Google Analytics e (b) avvisi sulle opzioni di opt-out, in base ai quali gli utenti possono anche scegliere di rinunciare tramite il proprio browser se il gestore del sito web non fornisce uno strumento (volontario) di preferenza per i cookie. Le aziende possono fornire informazioni sullo scopo dell'utilizzo di Google Analytics nella loro informativa sulla privacy sul sito web:
L'analisi web viene utilizzata per valutare l'utilizzo del sito web e per ottenere informazioni per la sua ottimizzazione.
Se si desidera trattare in modo specifico i cookie sul sito web: un «banner dei cookie» non è richiesto dalla legge svizzera finché la legge dell'UE non diventa applicabile (a causa dell'orientamento del sito web verso i clienti finali dell'UE). Tuttavia, uno strumento di preferenza per i cookie può essere utile. Può aiutare il gestore del sito web a rispettare i requisiti di trasparenza e a fornire agli utenti delle scelte.

Se si utilizza Google Analytics 4 (senza cookie), le misure per stabilire la "conformità ai cookie" passano in secondo piano. La trasparenza deve essere comunque garantita.

A cosa bisogna prestare attenzione per i moduli di contatto sul sito web?

In qualità di gestori di siti web, dovreste inoltre adottare le seguenti misure nei confronti di Google: (1) stipulare un contratto di outsourcing dell'elaborazione dati e (2) attivare la funzione di anonimizzazione dell'IP.
Per concludere, è necessario dire che: Google Analytics si inserisce in un ecosistema mondiale di notevole portata. Gli utenti si sentono osservati perché i dati raccolti nell'ambito dell'utilizzo del loro sito web confluiscono in un sistema mondiale per gli inserzionisti. Nota bene: quasi mai si tratta di dati personali. Eppure, non si può più semplicemente negare che gli utenti siano consapevoli del problema.
La sensazione di essere osservati rimane. E i gestori dei siti web non riescono quasi mai a creare trasparenza. Questo non significa che si debba ottenere il consenso (la mancanza di trasparenza non può essere curata dal consenso, perché un consenso non informato non è valido).
Ma significa comunque che è necessario gestire il proprio sito web in modo controllato. Si dovrebbe valutare seriamente se non sia meglio utilizzare una soluzione che si comprende da soli.

A cosa bisogna prestare attenzione per i moduli di contatto sul sito web?

I moduli di contatto devono fare riferimento alla dichiarazione generale sulla protezione dei dati sul sito web dell'azienda (senza casella di controllo per «Accettare»!). Scopo: garantire trasparenza sulle modalità di utilizzo dei messaggi ricevuti da parte del titolare del trattamento.

In dettaglio:

Chi rimanda alla Dichiarazione generale di protezione dei dati può rendere disponibili in questo modo le informazioni obbligatorie.
In particolare, si dovrebbe anche menzionare se tali richieste giungono nel sistema CRM (Customer Relationship Management System) a livello aziendale (non sussiste ancora una relazione con il cliente e l'archiviazione a lungo termine senza preavviso potrebbe essere

inaspettata e quindi poco trasparente).

Salvare e trattare i dati

Backup e conservazione dei dati: come si può conciliare questo aspetto con il diritto degli individui di richiedere la cancellazione dei dati?

Se i dati personali devono ancora essere conservati per ottemperare a un obbligo legale di conservazione, non è necessario cancellarli.

In dettaglio:

esistono sistemi tecnici che possono essere impiegati in modo lecito, ma che non consentono una cancellazione fisica dei dati personali (ad es.: «funzione journaling» di una soluzione di conservazione).

Con il requisito della «cancellazione», il diritto sulla protezione dei dati mira a impedire l'ulteriore utilizzo dei dati personali e a evitare di cadere vittime di un data breach quando qualcuno perde di vista un sistema già da tempo rimosso dalla circolazione («legacy system»).

Fintanto che misure tecniche e organizzative impediscono ai collaboratori di accedere ai dati in condizioni di normale funzionamento del sistema, non è necessaria alcuna cancellazione fisica; può essere sufficiente disattivare i collegamenti trasversali (link) da un sistema di recupero all'elemento fisicamente ancora disponibile.

Si può parlare di un «near-to-delete» o di una «quasi-cancellazione». In tali situazioni occorre continuare a dare grande importanza alle misure tecniche di protezione e si dovrebbe anche verificare in che misura i sistemi di archiviazione fisici impiegati possano comunque essere destinati regolarmente alla cancellazione (con monitoraggio della distruzione fisica).

Ai sensi della LPD, i dati personali possono essere archiviati nel cloud (ad es. SharePoint, OneDrive, Dropbox)?

Sì.

In dettaglio:

I dati personali possono essere memorizzati su qualsiasi sistema tecnico, a condizione che si possano rispettare i requisiti in materia di protezione dei dati.
Il diritto sulla protezione dei dati è tecnologicamente neutro. In altre parole, regola gli obiettivi di protezione e, in maniera determinante, lo scopo del trattamento e quindi l'«obiettivo» di un'azione, ma non il «percorso per raggiungere l'obiettivo». Il cloud è una tecnologia e quindi un «percorso per raggiungere l'obiettivo». La soluzione cloud in sé non dovrebbe essere la pietra dello scandalo. Tuttavia, una configurazione inadeguata della soluzione cloud non può essere accettata se comporta una violazione delle disposizioni in materia di protezione dei dati.

Occorre quindi scegliere con cura le soluzioni cloud. Il cloud Canvas di Laux Lawyers AG è un modello di verifica consolidato che consente ai clienti di impostare con cura i propri processi di sourcing. Con il cloud Canvas, i clienti di tutti i settori beneficiano dell'esperienza pluriennale di Laux Lawyers nell'acquisto di soluzioni cloud (ad esempio, Laux Lawyers è stato il primo studio legale in Svizzera ad affiancare l'outsourcing completo di una compagnia di assicurazioni in Svizzera su una soluzione cloud di un hyperscaler estero e le soluzioni proposte da Laux Lawyers sono ancora oggi all'avanguardia).
Se nel contesto di una soluzione cloud vengono creati rapporti con l'estero, anche questi devono essere rappresentati correttamente ai sensi della normativa in materia di protezione dei dati. Tuttavia, al giorno d'oggi è generalmente possibile.

A cosa prestare attenzione quando i collaboratori utilizzano laptop o telefoni cellulari privati oppure inviano documenti al proprio indirizzo e-mail privato?

In questi si parla delle cosiddette regole BYOD.
BYOD sta per «Bring Your Own Device». L'azienda deve avere il controllo sui propri dati, anche quando i collaboratori non li trattano su dispositivi di proprietà dell'azienda. Attraverso i regolamenti, le aziende possono effettuare controlli di tipo organizzativo e contrattuale. Esistono anche soluzioni tecniche («sandbox») che possono essere configurate su dispositivi privati per istituire una protezione tecnica.

In dettaglio:

Se i collaboratori trattano i dati sui propri dispositivi, ciò non esclude che l'azienda mantenga il controllo. Occorre però definire le regole di base per il controllo dei dati, al fine di garantire quanto segue:
Solo le persone autorizzate devono poter accedere ai dati personali e ad altri dati dell'azienda.
L'uso improprio dei dati deve essere accertato. Occorre garantire con delle direttive che determinati dati non vengano salvati sugli apparecchi privati.
L'azienda deve poter cancellare i dati personali dagli apparecchi dei collaboratori e poterne accertare la cancellazione prima che il collaboratore interessato lasci l'azienda.

L'apparecchio deve essere dotato di misure tecniche di sicurezza.

In che modo i dati stampati, ad es. contratti ed e-mail stampati, sono soggetti alla nLPD?

Anche i documenti fisici come le stampe cartacee sono disciplinati dalla nLPD.

In dettaglio:

Anche per quanto riguarda le copie cartacee vale il principio per cui possono essere conservate solo per il tempo strettamente necessario.
Anche per i documenti cartacei sono necessarie opportune misure di protezione. In questo caso si tratta in particolare di misure come le «Clean Desk Policy» e gli armadietti di archiviazione chiudibili a chiave. Il personale di pulizia, ad esempio, non deve avere la possibilità di prendere visione di documenti riservati o documenti contenenti dati personali.

È possibile trasmettere i dati dei clienti a fornitori (ad es. tipografia) o partner?

Sì, è legalmente possibile. A seconda delle mansioni assegnate, i fornitori o altri provider di servizi devono essere coinvolti contrattualmente nell'organizzazione del cliente in qualità di responsabili del trattamento. Sono quindi necessari contratti con misure di protezione. Il cliente deve selezionare con cura i prestatori di servizi.

In dettaglio:

Il diritto sulla protezione dei dati non determina l'impossibilità di scegliere dei partner. È possibile selezionare i partner, ma è necessario selezionarli accuratamente e integrarli nella propria organizzazione di protezione dei dati (coinvolgimento nel proprio perimetro organizzativo e personale). Si tratta di un incarico per il reparto Sourcing dell'azienda.

Cosa devono contenere come minimo tali contratti?

- Direttive sull'impiego dei dati.
- Disposizioni di riservatezza.
- Obblighi di cancellazione per il periodo successivo all'esecuzione del mandato
- Regolamentazione in merito all'eventuale coinvolgimento di subappaltatori *e* alle relative modalità (divieto o autorizzazione preventiva).
- Misure tecniche per la protezione dei dati personali.
- Obblighi di assistenza in relazione a richieste delle persone interessate *e* data breach.

Si possono inviare dati personali per e-mail? Serve una cifratura per farlo?

I dati personali dovrebbero essere inviati via e-mail sempre meno *e* solo con molta cautela.

In dettaglio:

I sistemi di posta elettronica dovrebbero ormai appartenere al passato. Per motivi legati non solo alla protezione dei dati è vantaggioso impiegare sistemi di collaborazione con aree di accesso circoscritte e protette da password. Scegliendo questa soluzione tecnica, chi utilizza attivamente tali sistemi può fornire un grande contributo non solo alla sicurezza informatica, ma

anche alla protezione dei dati.

È possibile avvalersi dei servizi di messaggistica (ad es. WhatsApp, Signal, Microsoft Teams) per condividere dati personali?

La nLPD non disciplina la tecnica («percorso per raggiungere l'obiettivo»), ma richiede che un titolare del trattamento controlli il trattamento dei dati. Pertanto, i servizi di messaggistica non sono di per sé conformi o contrari alla protezione dei dati. Quindi non è possibile dare una risposta astratta positiva o negativa.

In dettaglio:

Chi utilizza i servizi di messaggistica per scopi privati non è soggetto al diritto sulla protezione dei dati a tal proposito. Il motivo è il seguente: la nLPD non si applica se una persona privata tratta dati personali propri o di terzi esclusivamente per uso personale.
Nel contesto aziendale occorre fare una distinzione:

WhatsApp ha una soluzione per i clienti aziendali che può essere utilizzata in conformità al diritto sulla protezione dei dati. Per quanto riguarda la funzione di messaggistica utilizzata in ambito privato, però, difficilmente il titolare del trattamento sarà in grado di applicare i controlli necessari per ottemperare alla formula di base della normativa sulla protezione dei dati: «Si può controllare solo ciò che si comprende».

Lo stesso vale per gli altri servizi di messaggistica utilizzati in modo isolato.
L'utilizzo di Microsoft Teams è assolutamente controllabile per il contesto aziendale se il titolare del trattamento utilizza Teams come parte di una soluzione M365, che nel complesso è ben strutturata e ben illustrata a livello contrattuale.

Deve essere effettuato il backup dei dati?

Sì, si consiglia di effettuare un backup e, dal punto di vista della normativa sulla protezione dei dati, può essere addirittura necessario.

In dettaglio:

In linea di principio, i dati dovrebbero sempre essere ben protetti. In questo frangente un fornitore di servizi IT può aiutare a garantire la sicurezza informatica.
Il Consiglio federale ha annotato nell'Ordinanza sulla protezione dei dati il seguente principio: «Conformemente alla necessità di protezione, il titolare del trattamento e il responsabile del trattamento adottano provvedimenti tecnici e organizzativi affinché i dati trattati (...) siano disponibili quando necessario (disponibilità). Tale principio può valere quando si deve rispondere a una richiesta di informazioni.
Viceversa, non occorre disporre un lungo periodo di conservazione solo per poter rispondere a una richiesta di informazioni.
Se i dati sono stati cancellati lecitamente, non è un problema se alla richiesta di informazioni può essere data soltanto la seguente risposta: «Nei nostri sistemi non è archiviato nessun dato relativo alla Sua persona.»

Quando bisogna nominare un rappresentante in Svizzera?

In Svizzera esistono analogie con il RGPD per quanto riguarda l'obbligo di nominare un rappresentante. A determinate condizioni, le imprese straniere devono nominare un rappresentante affinché l'IFPDT abbia un punto di contatto in Svizzera per le comunicazioni relative all'applicazione della nLPD anche alle aziende estere.

In dettaglio:

Requisiti per la notifica del rappresentante:

- Legame con l'offerta di beni e servizi in Svizzera.
- Trattamento su grande scala.
- Trattamento periodico.

Quali sono le conseguenze giuridiche se dati personali degni di particolare protezione vengono trattati su larga scala in un cloud?

Se dati personali degni di particolare protezione vengono trattati su larga scala in un cloud, può essere necessaria una valutazione d'impatto sulla protezione dei dati, la redazione di un registro delle attività di trattamento e di un regolamento per il trattamento.

Può sussistere l'obbligo di consultare l'IFPDT e può essere necessario registrare i trattamenti nei sistemi (creazione di log di sistema).

In dettaglio:

Valutazione d'impatto sulla protezione dei dati:

Se il trattamento dei dati personali degni di particolare protezione avviene «su grande scala», in caso di utilizzo di un cloud («nuova tecnologia») può essere giustificato l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati (art. 22 cpv. 2 nLPD), purché esso non decada per determinati motivi (art. 22 cpv. 4 o 5 nLPD).

Conservazione per due anni. Se avvenisse su base volontaria, dovrebbe essere documentata anche la volontarietà (altrimenti rischio di interpretazione contraria).

Consultazione dell'IFPDT: In casi estremi, può seguire una fase di consultazione da due a tre mesi presso l'IFPDT (art. 23 nLPD), che però si può evitare nominando un consulente per la protezione dei dati (art. 23 cpv. 4 nLPD).

Registrazione in log: Se il trattamento dei dati personali degni di particolare protezione è «su vasta scala», occorre provvedere alla verbalizzazione (logging, art. 3 cpv. 3 lett. a nOPDa e art. 4 cpv. 1 nOPDa). Conservazione di un anno per i log. Tuttavia, la registrazione in log non è un obbligo del cloud di per sé.

Regolamento per il trattamento: Se il trattamento dei dati personali degni di particolare protezione avviene «su vasta scala», è necessario un regolamento per il trattamento (art. 5 nOPDa; tale obbligo ricade anche sul fornitore di servizi cloud).
Tuttavia, il regolamento per il trattamento dei dati non è di per sé un obbligo per il cloud.

Registro delle attività di trattamento:
Se il trattamento dei dati personali degni di particolare protezione è su «vasta scala», è necessario redigere un registro delle attività di trattamento (art. 24 lett. a nOPDa), il quale (con descrizione del cloud) non è una conseguenza del cloud.

La profilazione ad alto rischio presenta particolarità?

Sì, ci sono diverse misure di compliance che devono essere adottate.

In dettaglio:

Può essere necessario adottare le seguenti misure:

- Applicare requisiti di sicurezza più elevati.
- Spiegare in modo più dettagliato per ottenere una maggiore trasparenza.
- La verifica della solvibilità non costituisce un motivo giustificativo (art. 31 cpv. 2 lett. c punto 1 nLPD).
  Nel caso in cui sia necessario (e solo in questo caso) in virtù di un'altra disposizione della nLPD, il consenso deve essere espresso (art. 6 cpv. 7 lett. b nLPD).
- La registrazione in log *è* obbligatoria (art. 4 nOPDa).
- Il regolamento per il trattamento *è* obbligatorio anche per i privati (art. 5 cpv. 1 lett. b nOPDa).
- Il registro delle attività di trattamento *è* obbligatorio anche per i privati (art. 24 lett. b nOPDa).

Si parla di profilazione ad alto rischio quando:

- Il trattamento *è* automatizzato.
- È possibile una valutazione su *determinati* aspetti personali.
- Analisi (raccolta di dati pericolosa).
- Previsione (affermazione pericolosa).
- Vi è un collegamento con i dati che consentono di valutare aspetti essenziali.

Ci sono particolarità per quanto riguarda i dati personali degni di particolare protezione?

Sì, ci sono diversi obblighi che devono essere verificati.

In dettaglio:

Può essere necessario adottare le seguenti misure:

- Applicare requisiti di sicurezza più elevati.
- Spiegare in modo molto dettagliato per una maggiore trasparenza.
- Adottare misure di sicurezza particolarmente buone.
- La verifica della solvibilità non costituisce un motivo giustificativo (art. 31 cpv. 2 lett. c punto 1 nLPD).
- Nel caso in cui sia necessario (e solo in questo caso) in virtù di un'altra disposizione della nLPD, il consenso deve essere espresso (art. 6 cpv. 7 lett. a nLPD).
- La registrazione in log è obbligatoria (art. 4 nOPDa).

- Il regolamento per il trattamento è obbligatorio anche per i privati (art. 5 cpv.1 lett. b nOPDa).
- Il registro delle attività di trattamento è obbligatorio anche per i privati (art. 24 lett. b nOPDa).
- Comunicazione solo con una giustificazione particolare (art. 30 cpv. 2 lett. c nLPD).
- Regolamentazione speciale in caso di giustificazione per scopi di ricerca (art. 31 cpv. 2 lett. e nLPD e art. 39 cpv. 1 lett. b nLPD).

Quali sono le parole chiave importanti sul tema «violazioni della sicurezza dei dati»?

Purtroppo, le violazioni della sicurezza dei dati (data breach) sono in aumento, al momento a causa di attacchi dall'esterno. Si può dire qualcosa al riguardo anche in merito alla protezione dei dati. Si tratta soprattutto di obblighi di notifica. In singoli casi, tuttavia, tali eventi possono anche condurre a punibilità.

In dettaglio:

- La mancanza di sicurezza dei dati può comportare punibilità ai sensi dell'ar t. 64 cpv. 2 LPD (violazione dell'art. 8 LPD);
- la notifica può essere utilizzata nei confronti della «persona soggetta all'obbligo di notifica» solo previo suo consenso (lo stesso vale anche per l'azienda).
- Obbligo di notifica all'IFPDT in caso di rischio elevato. Tempistica: «quanto prima».
- Obbligo di notifica alla persona interessata (a) se necessario o (b) su richiesta dell'IFPDT.
- Tempistica: aperta.
- Obbligo di documentare l'incidente di sicurezza e di conservare la documentazione per due anni dalla notifica all'IFPDT (sempreché la notifica venga effettuata, indipendentemente dal fatto che adempia o meno a un obbligo; è tutta via solo diritto regolamentare).

Quali sono le parole chiave importanti sul tema «violazioni della sicurezza dei dati»?

La nLPD prevede sanzioni penali per diversi casi (cfr. testo apribile). Fino al limite di CHF 50'000.- può risultare anche una multa per l'azienda (art. 64 cpv. 2 LPD)

In dettaglio:

Può essere applicata una sanzione penale nei seguenti casi:

- Informazioni proattive assenti, errate o incomplete in caso di rilevazione direttamente presso la persona interessata, immediatamente.
  Contenuto: (i) chi, (ii) perché, (iii) destinatari o categorie di destinatari; (iv) Paese di destinazione con garanzie.
- Informazioni proattive assenti, errate o incomplete in caso di rilevazione presso terzi. 1 mese (salvo comunicazione anticipata). Contenuto: (i) chi, (ii) cosa, (iii) perché, (iv) destinatari o categorie di destinatari; (v) Paese di destinazione con garanzie.
- Informazioni proattive assenti, errate o incomplete in caso di AEFE rilevante.
- Informazioni reattive errate o incomplete (devono essere fornite le informazioni nello scenario).

- «presso terzi» e (vi) periodo di conservazione; (vii) origine; (viii) AEFE (esistenza e logica)). Il ritardo (alla scadenza dei 30 giorni, senza notifica ai sensi dell'art. 18 cpv. 2 OPDa) o la mancata informazione non sono punibili.
- Trasmissione all'estero contraria ai requisiti.
- Coinvolgimento insufficiente dei responsabili del trattamento: ad es. ricorso al responsabile del trattamento senza garanzia dei requisiti (limitazioni d'uso e disposizioni di sicurezza).
- Violazione della sicurezza dei dati, ovvero senza esecuzione dell'analisi delle esigenze di protezione né misure tecniche e organizzative.
- Violazione del segreto (art. 62 LPD).
- Inosservanza di decisioni (art. 63 nLPD).
- Furto d'identità (Art. 179decies CP).

L'IFPDT ha poteri d'inchiesta anche nei confronti di aziende private?

Sì. Con la nLPD l'Incaricato federale della protezione dei dati e della trasparenza ha ricevuto ulteriori poteri d'inchiesta, che vanno oltre rispetto a quanto previsto in passato, e un'inchiesta può essere avviata più rapidamente rispetto alla legislazione precedente («se indizi sufficienti lasciano presumere che un trattamento di dati potrebbe violare le disposizioni sulla protezione dei dati»).

In dettaglio:

L'IFPDT può indagare nelle seguenti situazioni:

Inchiesta nei confronti di privati anche d'ufficio se indizi sufficienti lasciano presumere che un trattamento di dati potrebbe violare le disposizioni sulla protezione dei dati» (art. 49 nLPD; eccezione: violazioni di poca importanza).
Potere di inchiesta in qualità di autorità di vigilanza nei confronti delle autorità della Confederazione.

L'IFPDT ha le seguenti facoltà:

- Diritto di disporre diretto (modifica, interruzione o sospensione di un trattamento; cancellazione dei dati personali; informazione degli interessati).
- Esecuzione di una valutazione d'impatto sulla protezione dei dati ecc.
- Facoltà d'inchiesta (art. 50 nLPD): (a) accesso alle informazioni/documenti; (b) accesso ai locali e agli impianti; (e) interrogatori di testimoni; (d) perizie di esperti.
- Competenza decisionale in qualità di autorità di vigilanza nei confronti delle autorità della Confederazione.

Quali termini occorre ricordare quando si parla della nLPD?

Nella nLPD i termini possono essere rilevanti in diversi contesti.

In dettaglio:

A titolo di riepilogo, qui vengono menzionati i diversi termini indicati nella nLPD:

- Quanto prima: data breach Notification all'IFPDT.
- Termine ragionevole: data Breach Notification alla persona interessata (non è sempre richiesta).
- 1 mese: informazione proattiva secondo l'art. 19 cpv. 5 nLPD.
- 30 giorni: informazione reattiva (art. 25 cpv. 7 nLPD; art.18 OPDa).
- 1 anno: conservazione di log (art. 4 OPDa).
- 2 anni: conservazione della valutazione d'impatto sulla protezione dei dati (art. 14 OPDa)
- 5 anni (dall'entrata in vigore della nLPD): diritto delle autorità federali di comunicare dati di persone giuridiche ai sensi della LOGA (art. 71 nLPD) sussiste fino al 31 agosto 2028.
- 5 anni: Prescrizione dell'azione penale (art. 66 nLPD).
- 10 anni: La verifica della solvibilità non costituisce più un motivo giustificativo se i dati sono più vecchi (art. 31 cpv. 2 lett. c punto 4 nLPD).

Quali diritti ho come persona nei confronti del titolare del trattamento ai sensi della nLPD?

Con il termine «diritti della persona interessata» si intendono i diritti che le persone interessate hanno nei confronti dei titolari del trattamento.

In dettaglio:

La nLPD menziona i seguenti diritti della persona interessata:

- Diritto di accesso: Art. 25 nLPD.
- Diritto di rettifica: Art. 32 cpv. 1 nLPD.
- Diritto alla cancellazione o alla distruzione dei dati personali: Art. 32 cpv. 2 lett. c nLPD.
- Diritto di farsi consegnare dati o di esigerne la trasmissione a terzi (portabilità dei dati): Art. 28 nLPD.

Va inoltre menzionato il fatto che il titolare del trattamento ha obblighi di informazione nei confronti della persona interessata:

- Trasparenza proattiva (art. 19 nLPD), AEFE (art. 21 nLPD).
- Data Breach Notice (art. 24 cpv. 4 nLPD).
- Indicazione dei dati di contatto del consulente per la protezione dei dati (art. 10 cpv. 3 lett. d nLPD).

Vi sono obblighi di notifica ai sensi della nLPD?

Sì, in diversi casi la nLPD prescrive una notifica all'IFPDT.

In dettaglio:

Si tratta dei seguenti obblighi di notifica:

Dati di contatto del consulente per la protezione dei dati (art.10 cpv. 3 lett. C nLPD):

Se un'azienda si avvale di un consulente per la protezione dei dati, quest'ultimo deve essere segnalato all'IFPDT.
In caso contrario, l'effetto di privilegio previsto dalla legge (nel contesto della valutazione d'impatto sulla protezione dei dati) non trova applicazione. È quindi possibile disporre di un consulente per la protezione dei dati e non notificarlo all'IFPDT.

Le valutazioni d'impatto sulla protezione dei dati devono essere preparate e presentate all'IFPDT se, dopo la loro esecuzione, il rischio netto rimane «elevato» e l'azienda non ha nominato un consulente per la protezione dei dati.

e Data breach con rischio alto: eventuali violazioni della sicurezza dei dati devono essere segnalate all'IFPDT.

I trasferimenti all'estero sulla base di clausole sulla protezione dei dati, di garanzie specifiche o di Binding Corporate Rules (BCR) devono essere notificati all'IFPDT.

Il rappresentante ai sensi dell'art. 14 nLPD deve essere notificato all'IFPDT.

In qualità di titolare del trattamento, è possibile presentare una richiesta di autorizzazione all'IFPDT per determinate azioni affinché il rischio personale ai sensi della nLPD diminuisca?

In generale, il diritto in materia di protezione dei dati è un ambito giuridico in cui è necessario trovare autonomamente delle soluzioni. Solo a posteriori si decide se ciò che è stato fatto era legittimo. A prima vista si tratta di una condizione insoddisfacente, ma nella pratica può essere gestita facilmente. Chi si attiene alle seguenti regole generali dovrebbe in ogni caso riuscire a evitare sanzioni:

- Avere la propria attività sotto controllo (solo chi capisce una cosa può controllarla).
- Non essere scorretto.

In dettaglio:

Ciononostante, la nLPD prevede in parte l'obbligo di notificare le azioni all'IFPDT affinché quest'ultimo possa approvarle (o negare l'approvazione nel singolo caso). Ma si tratta piuttosto di un'eccezione.

Vale la pena citare i seguenti casi:

- Certificazione di sistemi o programmi (art.13 nLPD).
- Le clausole standard di protezione dei dati devono essere in parte approvate.
- Devono essere approvate anche le disposizioni in materia di protezione dei dati a livello aziendale, le cosiddette BCR o Binding Corporate Rules.
- Anche i codici di condotta (art. 11 nLPD) dovrebbero essere approvati, ma sarà necessario attendere che questo strumento si affermi.

Eccezione:
procedimenti pendenti; fattispecie grandfathering, per cui continua a valere il vecchio diritto.

Grandfathering:
solo in caso di volume di dati e scopo invariati («raccolte di dati passive»). In questo ambito, «Grandfathering» significa che per questi casi, ad esempio, non vi è nessun obbligo di informazione, nessuna valutazione d'impatto sulla protezione dei dati e nessun obbligo di Privacy by Design e by Default.
Ma secondo la legge non è chiaro se la regola transitoria valga anche per le misure di sicurezza.

Bisogna considerare che la sicurezza informatica è una sfida costante, non si dovrebbe mai avere un dispositivo di sicurezza obsoleto. Deve essere rispettato almeno lo stato della tecnica, ma questo può cambiare.

Dati di persone giuridiche: le autorità hanno ancora un diritto di comunicazione fino al 31 agosto 2028.

A cosa occorre pensare se si coinvolge un responsabile del trattamento dei dati su commissione?

Durante la selezione e il controllo, assicuratevi che il responsabile del trattamento protegga adeguatamente i dati personali dal rischio di violazioni della sicurezza dei dati. Ciò significa che occorre selezionare accuratamente i responsabili del trattamento e monitorarli. Inoltre, è necessario tutelarsi a livello contrattuale.

In dettaglio:

I contratti con responsabili del trattamento dei dati su commissione devono includere almeno i seguenti contenuti:

- Descrizione dell'oggetto e della portata del trattamento commissionato.
- Vincolo del responsabile del trattamento ad osservare le istruzioni ricevute.
- È necessario prescrivere sufficienti misure tecniche e organizzative per la sicurezza dei dati e, idealmente, sostanziarle anche in altro modo.
- Regolamenti sufficienti relativi ai sub-incaricati (si veda anche l'art. 7 nOPDa).
- Obblighi di informazione, cooperazione e riservatezza del responsabile del trattamento
- Diritti di verifica del titolare del trattamento (controlli nel corso della durata del contratto).
- Regolamentazione sulla protezione dei segreti professionali.
- Regolamenti sufficienti per i rapporti con l'estero.

Esistono consigli di attuazione per le PMI in materia di sicurezza?

Creare sicurezza è un compito importante, nel quale bisognerebbe farsi aiutare da un esperto. Pertanto, non è possibile fornire una breve risposta nell'ambito di queste FAQ.

da oltre 100 anni
CAMERA DI COMMERCIO CANTONE TICINO
industria | artigianato | servizi

Esistono delle buone liste di controllo per la sicurezza informatica?

Il Centro nazionale per la cybersicurezza (NCSC) ha emanato alcune istruzioni sulla sicurezza dei dati. Tuttavia, queste sono più l'inizio della conversazione sulla sicurezza che la scorciatoia verso la fine.
Anche l'articolo della rivista B2B di Swisscom offre un'introduzione alle misure di base per la protezione dagli attacchi informatici.

In dettaglio:

I seguenti punti possono essere citati come un piccolo kit domestico per la creazione di una rete interna in una PMI:

- Apparecchi «single purpose» incapsulati per determinate attività (pagamenti).
- Misure di incapsulamento nella rete (per impedire l'ulteriore diffusione).
- Proteggere i backup dal contagio.
- Esecuzione di aggiornamenti.
- Tenere d'occhio, controllare e monitorare i diritti degli utenti.
- Diritti da amministratore: gli amministratori dovrebbero inoltre rispettare il principio dell'assegnazione minima dei diritti.
- Bloccare le macro.
- Bloccare i siti web negli elenchi di siti sospetti (ad esempio su abuse.ch).
- Bloccare gli indirizzi IP (vedi abuse.ch).
- Log (periodi di archiviazione): impostare i periodi al massimo. Spesso i periodi di conservazione dei log sono troppo brevi. 90 giorni sono il minimo, alcuni log dovrebbero essere impostati su un periodo di tempo più lungo.