Nuova Legge federale sulla protezione dei dati

avv. Michele Barchi

Jardin Suisse Ticino

INDICE DELLA FORMAZIONE

Parte 1

Nozioni fondamentali della protezione della personalità in genere e nel rapporto di lavoro (a titolo esemplificativo)

Personalità e diritti fondamentali = ?

diritti e attributi più fondamentali di ogni essere umano, inalienabili e intrasmissibili, fra cui:

- il diritto alla vita;
- l'integrità fisica e psicofisica;
- la libertà personale;
- la protezione della **sfera privata** e familiare;
- il diritto all'onore;
- il diritto all'identità personale;
- il diritto al nome;
- la libertà di opinione;
- la libertà di credo e coscienza;
- ecc.

Art. 13 Costituzione federale

« Ognuno ha diritto al rispetto della sua vita privata e familiare, della sua abitazione, della sua corrispondenza epistolare nonché delle sue relazioni via posta e telecomunicazioni (cpv. 1). Ognuno ha diritto di essere protetto da un impiego abusivo dei suoi dati personali (cpv. 2).»

Art. 28 Codice civile

« Chi è illecitamente leso nella sua personalità può, a sua tutela, chiedere l'intervento del giudice contro chiunque partecipi all'offesa (cpv. 1). La lesione è illecita quando non è giustificata dal consenso della persona lesa (cvp. 2).»

Art. 1 Legge sulla protezione dei dati

« Scopo della presente legge è proteggere la personalità e i diritti fondamentali delle persone fisiche i cui dati personali sono oggetto di trattamento.»

Protezione della personalità del lavoratore

art. 328 CO e 6 LL

Il datore di lavoro deve **rispettare** e **proteggere la personalità** del lavoratore, avere il dovuto riguardo per la sua salute e vigilare alla salvaguardia della moralità, prendendo tutti i **provvedimenti** necessari, dimostrati necessari secondo l'esperienza.

Personalità del lavoratore nel senso più ampio:

→ Vita e salute

→ Integrità fisica e psichica

→ Onore personale e professionale

→ Sfera intima e sessuale

→ Libertà di espressione e sindacale

Come proteggere il lavoratore?

Prendendo tutti i **provvedimenti**, che l'esperienza ha dimostrato **necessari, realizzabili** secondo lo stato della tecnica e adeguati alle condizioni di esercizio.

Trattamento di dati personali del lavoratore

Art. 328b CO

*Il datore di lavoro può trattare dati concernenti il lavoratore soltanto in quanto si riferiscano all'**idoneità lavorativa** o siano **necessari all'esecuzione** del contratto di lavoro.*

Inoltre, sono applicabili le disposizioni della Legge federale del 25 settembre 2020 sulla protezione dei dati (!!!)

Trattamento di dati personali del lavoratore

Dati personali

Tutte le informazioni concernenti una persona **fisica identificata o identificabile** (art. 5 let. a LPD).

Trattamento

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 let. d LPD).

Trattamento dei dati del lavoratore

è possibile per quanto si riferiscano all'**idoneità lavorativa** o siano **necessari all'esecuzione** del contratto di lavoro

Esempi:

→ Sì a informazioni relative a formazione, esperienze lavorative, conoscenze linguistiche;
→ Sì a informazioni relative a caratteristiche personali che permettono di valutare idoneità a lavoro o a inserimento in un team;
→ Sì / No a informazioni su abuso di alcol o droghe;
→ Sì a informazioni su appartenenza sindacale;
→ No a informazioni su gravidanza;
→ No a informazioni su orientamento sessuale, religioso, politico o a stato di salute in generale;
→ No a precedenti penali (con eccezioni);
→ No a sorveglianza del lavoratore (con eccezioni);
→ Si a indirizzo completo, IBAN, numero AVS, ecc.

Casi particolari: sentenze CEDU – Barbulescu c. Romania ; Lopez Ribalda c. Spagna

Parte 2

Nuova normativa sulla protezione dei dati

Rivoluzione tecnologica e informatica

digitalizzazione uso di internet, e-mail, smartphone, reti sociali, cloud, ecc.

→ necessità di **adeguare la normativa sulla protezione dei dati**, per migliorare la trasparenza del trattamento dei dati e la protezione delle persone.

Scandali recenti

Facebook-Cambridge analytica

87 mio di persone coinvolte

pubblicità elettorale mirata

Clearview

3 mia di persone coinvolte

database di volti umani

GDPR – General Data Protection Regulation

→ Regolamento dell'**Unione europea** sulla protezione dei dati;

→ Possibile applicazione anche per aziende con sede in **CH** (se la volontà di vendere beni e servizi nell'UE è manifesta oppure se vi è monitoraggio del comportamento di persone nell'UE tramite per esempio cookie o programmi tipo Google Analytics);

→ Norme analoghe all'attuale normativa CH (nLPD), ma con **differenze!**;

→ Obbligo di informare e ottenere il consenso dell'interessato;

→ Obbligo di tenere un registro delle attività di trattamento dei dati;

→ Sanzioni.

Nuova Legge federale sulla protezione dei dati (nLPD) del 25 settembre 2020

→ riprende in buona parte la normativa europea e il GDPR (ma non pari-pari!)

→ entrata in vigore il **1. settembre 2023!**

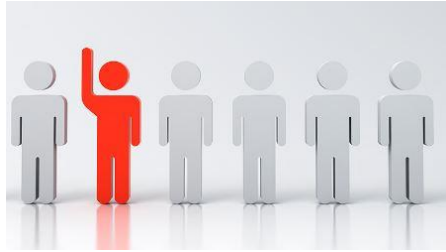
→ con relativa **ordinanza** del 31 agosto 2022 (e.v. 1. settembre 2023).

→ la nuova normativa si applica a tutti i dati trattati o modificati dal 1. settembre 2023 in poi.

Molte **novità** con la nLPD:

- Solo dati delle **persone fisiche**;
- Rafforzamento e nuovi **principi**: legalità, BF, proporzionalità, sicurezza, finalità, esattezza, «privacy by design» e «privacy by default»;
- Estensione del diritto/obbligo di **informazione** sul trattamento;
- **Consenso** libero, informato e specifico;
- Nuovi dati personali degni di **particolare protezione** (genetici e biometrici);
- **Analisi di impatto** in caso di rischio elevato;
- Possibilità, ma non obbligo, di nominare un **consulente** per la protezione dei dati;
- **Registro** delle attività di trattamento, sia per titolare sia per responsabile (obbligatorio in alcuni casi);

- Comunicazione dati all'**estero** solo se destinatario sicuro, in particolare se considerato tale dal Consiglio federale (v. lista paesi nell'allegato I OPDa);
- Nozione di **profilazione**;
- Obbligo di annuncio rapido all'**IFPDT** (Incaricato federale per la protezione dei dati e della trasparenza) in caso di violazione della sicurezza con rischio elevato;
- Nuove competenze dell'IFPDT;
- **Multe** fino a CHF 250'000 in caso di violazione;
- Disposizioni transitorie: solo a dati trattati o modificati dopo l'entrata in vigore;
- Ecc.



1. Protezione unicamente delle persone fisiche (art. 1 nLPD)

« *scopo della presente legge è proteggere la personalità e diritti fondamentali delle* ***persone fisiche*** *i cui dati personali sono oggetto di* ***trattamento***».

trattamento = qualsiasi operazione relativa a dati personali, indipendentemente dai mezzi e dalle procedure impiegati (raccolta, registrazione, conservazione, utilizzazione, modificazione, comunicazione, archiviazione, cancellazione, distruzione, ecc.)

→ La protezione delle **persone giuridiche** rimarrà possibile per il tramite di altre norme:

- LPDP (cantonale!)
- art. 179decies CP: usurpazione di identità;
- art. 28 e segg. CC;
- LF sui diritti di autore;
- LF contro la concorrenza sleale;
- ecc.

Protezione per rispetto all'agire di chi ?

→ privati

purché non si tratti di uso esclusivamente personale; cfr. DTF 5C_15/2001: impiegato dell'UNIGE che ha chiesto dei rapporti psicologici redatti su suo conto → ottenuti, ad eccezione dei «promemoria».

→ organi federali

di principio non i Comuni e i Cantoni; salvo se agiscono come «privati». Si attende una nuova Legge cantonale sulla protezione dei dati, ora in elaborazione, che definirà anche i compiti dell'Incaricato cantonale della protezione dei dati (il quale ha anche competenze di sorveglianza e controllo).

es. assicurazioni malattia e infortuni (LAMal).

Protezione di che cosa?

→ Dati personali = tutte le informazioni concernenti una persona fisica **identificata o identificabile**.

→ Dati personali degni di particolare protezione (art. 5 let. c nLDP):

- i dati concernenti le opinioni o attività religiose, filosofiche, politiche o sindacali;
- i dati concernenti la salute, la sfera intima o l'appartenenza a una razza o a un'etnia;
- i dati **genetici***;
- i dati **biometrici*** che identificano in modo univoco una persona fisica;
- i dati concernenti perseguimenti e sanzioni amministrativi e penali;
- i dati concernenti le misure d'assistenza sociale.

*aggiunti con nLDP

Esempi emblematici di dati

→ fotografia di una persona;
→ indirizzo di casa;
→ indirizzo IP (?);
→ numero AVS;
→ stato di salute;
→ peso e altezza;
→ origine;
→ fede religiosa;
→ orientamento sessuale;
→ condanne penali;
→ etnia
→ salario annuale;
→ ecc.

Se i dati sono **anonimizzati**?
es. i ticinesi / Luca trascorrono / trascorre in media 1 ora al giorno sullo smartphone.

2. Nuovi principi (art. 7)

Il trattamento deve rispettare i seguenti principi:

Privacy by design = protezione dei dati sin dalla **concezione e progettazione**; gli sviluppatori devono integrare la protezione e il rispetto della vita privata nella struttura medesima del prodotto o del servizio chiamato a raccogliere i dati personali.

Privacy by default = protezione dei dati per impostazione predefinita, con attivazione automatica (senza intervento degli utenti) di tutte le misure necessarie alla protezione dei dati e alla limitazione del loro utilizzo (trattamenti devono essere limitati al **minimo indispensabile**).

3. Liceità del trattamento (art. 6 e segg. LPD)

→ Un trattamento è lecito, anzitutto, se avviene nel **rispetto dei principi generali**, fra cui i nuovi «privacy by design» e «privacy by default»,

ma anche degli ulteriori principi già noti che sono stati «**rinforzati**» dalla nuova normativa, in particolare:

- **Legalità** (con consenso o per legge, senza violazione alcuna della nLPD);
- **Buona fede** (divieto di inganni,…);
- **Proporzionalità** (idoneo, necessario e proporzionato → stretto necessario e poi distruzione o anonimizzazione);
- **Sicurezza** (da garantire con provvedimenti tecnici e organizzativi adeguati al rischio → art. 3 OPDa);
- **Finalità** (determinata e riconoscibile);
- **Esattezza** (in caso contrario rettificare, cancellare o distruggere);
- Ecc.

→ Per essere lecito, il trattamento deve inoltre di norma **prevedere un motivo giustificativo**.

Quali possono essere i **motivi giustificativi** che rendono lecito un trattamento?

a) Il **consenso** della persona interessata, libero e informato, specifico o generale, semplice o espresso:

- il consenso è valido solo se dopo debita informazione è dato in modo libero e in riferimento a uno o più trattamenti specifici;

- il consenso dev'essere espresso per
  a) il trattamento di dati personali degni di particolare protezione;
  b) la profilazione a rischio elevato da parte di privati;
  c) la profilazione da parte di un organo federale.

- il consenso può essere revocato (es. DTF 5A.827/2009: fotografie e video su piattaforma internet per escort → revocabile e indennizzo).

b) **L’interesse preponderante** pubblico o privato giusta l’art. 31 nLPD (conclusione o esecuzione di un contratto, ricerca, statistica, esame della solvibilità di una parte contrattuale, trattamento a titolo personale, o per un mezzo di comunicazione di massa, ecc.);

c) **Legge** formale (es. Legge tributaria, assicurazioni sociali obbligatorie del dipendente, contabilità commerciale, art. 3 cvp. 3 let o LCSI, art. 328b CO)

4. Nuovi attori (art. 5)

Persona interessata = persona fisica i cui dati sono oggetto di trattamento.

Titolare del trattamento = il privato o l'organo federale che, singolarmente o insieme ad altri, determina lo scopo e i mezzi del trattamento.

Responsabile del trattamento = il privato o l'organo federale che tratta dati personali per conto del titolare del trattamento (non il lavoratore dipendente «incaricato» della protezione dei dati!)

Consulente per la protezione dei dati = interlocutore, che può essere nominato dal titolare (non obbligatorio), per le persone interessate come pure per le autorità competenti in Svizzera per la protezione dei dati. Egli ha segnatamente il compito di fornire formazione e consulenza al titolare, ed implementare le nuove normative. Dev'essere indipendente (non nella direzione, né nel team informatico o giuridico) e beneficiare di conoscenze tecniche (di tipo giuridico e/o informatiche).

*rimane sempre attuale ma con «maggiori poteri» la figura dell'**Incaricato federale della protezione dei dati e della trasparenza** (IFPDT)

5. Nuove nozioni (art. 5)

Profilazione = trattamento automatizzato di dati personali consistente nell'utilizzazione degli stessi per valutare determinati aspetti personali di una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze, gli interessi, l'affidabilità, il comportamento, i luoghi di permanenza e gli spostamenti di tale persona.

Profilazione a rischio elevato = profilazione che comporta un rischio elevato per la personalità o i diritti fondamentali della persona interessata poiché comporta un collegamento tra dati che permette di valutare aspetti essenziali della personalità di una persona fisica.

es. forze dell'ordine vogliono prevedere la possibilità che un soggetto sia portato a delinquere;
es. assicurazioni malattie complementari vogliono valutare lo stato di salute e le possibilità che un soggetto si possa ammalare;
es. pubblicità mirata;
es. offerte commerciali mirate.

6. Registro delle attività di trattamento (art. 12)

→ I titolari e i responsabili del trattamento tengono ognuno un **registro delle rispettive attività di trattamento;**

→ Il registro del **titolare** deve contenere almeno:

- sua identità;
- scopo (es. distinguere per dipartimento: RH, finanze, vendite & marketing, giuridico, ricerca e sviluppo);
- categoria di persone (es. candidati, impiegati, consumatori, contraenti, fornitori,..);
- categorie di dati (come contratti, salari, valutazioni; o sensibili: come salute, biometrici, giustizia);
- categorie di destinatari (interni, esterni, CH, EU, mondo,…);
- descrizione generale dei provvedimenti tesi a garantire la sicurezza [CSA (cloud security alliance), sec. datasheet (documentazione es. di un software), certif. ISO o altro (art. 13 nLPD e cfr. OCPD) , firewall, back-up, criptaggio, anti-virus, accesso fisico e controllo, password, formazione base collaboratori, test di penetrazione e vulnerabilità];
- se dati verso l'estero, indicare lo Stato e le garanzie offerte.

→ Il registro del **responsabile** deve contenere almeno:

- sua identità;
- identità del titolare;
- categorie di trattamenti eseguiti su incarico del titolare;
- descrizione generale dei provvedimenti per la sicurezza;
- se dati verso estero, indicare lo Stato e le garanzie offerte.

!!! Non vi è l'obbligo di tenere un registro per imprese con meno di **250 collaboratori** i cui trattamenti di dati personali comportano soltanto un **rischio esiguo** di violazione della personalità delle persone interessate !!! Secondo l'art. 23 OPDa il **rischio non è esiguo** se sono trattati su vasta scala dati personali degni di particolare protezione o se viene eseguita una profilazione ad alto rischio !!!

7. Valutazione d'impatto sulla protezione dei dati (art. 22)

Il titolare del trattamento effettua **previamente** una valutazione d'impatto sulla protezione dei dati quando il trattamento dei dati personali può comportare un **rischio elevato** per la personalità o i diritti fondamentali della persona interessata.

→ Vi è **rischio elevato** segnatamente in caso di trattamento su **grande scala** (n.ro persone, volume e ventaglio dati, durata e permanenza, vastità geografica) di dati personali degni di particolare protezione e in caso di sorveglianza di ampi spazi pubblici.

→ Contenuto della valutazione:
- Descrizione del trattamento previsto;
- Valutazione dei rischi;
- Provvedimenti volti alla tutela.

→ Il titolare può rinunciarvi se si avvale di un sistema, prodotto o servizio **certificato** secondo l'art. 13 nLDP (es. ISO 27001 → OCPD) o se rispetta un **codice di condotta** secondo l'art. 11 nLPD (quest'ultimo deve basarsi su di una valutazione d'impatto, prevedere delle misure a tutela della personalità e dei diritti fondamentali, e dev'essere stato sottoposto all'IFPDT).

8. Obbligo di informare sulla raccolta dati (art. 19)

Il titolare del trattamento informa in modo adeguato la persona interessata sulla raccolta di dati personali; tale obbligo sussiste anche se i dati non sono raccolti presso la persona interessata

→ **Quando informare?** Al **momento della raccolta**! Cfr. per es. privacy policy e cookies policy.

* se i dati sono raccolti presso la persona interessata, le informazioni di cui sopra vanno comunicate **al momento della raccolta**.
** se i dati non sono raccolti presso la persona interessata, le informazioni di cui sopra vanno comunicate entro **1 mese**.

→ **Contenuto minimo dell'informazione:**

- identità e dati di contatto del **titolare** (nome e cognome o ragione sociale, indirizzo completo, e-mail, telefono);
- **scopo** del trattamento;
- **destinatari** o categorie di destinatari;
- categorie di **dati** trattati (di principio solo necessario se non raccolti presso la persona interessata);
- **stato estero** o organismo internazionale destinatario e garanzie nel caso il paese non fosse sicuro (garanzie contrattuali e misure tecniche; circostanza secondo cui sono comunicati all'interno della stessa impresa o del gruppo di imprese).

→ **Come informare?** In modo adeguato = in forma precisa, trasparente, comprensibile e facilmente accessibile
(art. 13 OPDa; tramite sito internet, formulari, regolamenti d'impresa, ecc.)

esempi: https://www.swisscom.ch/it/clienti-privati/informazioni-legali/protezione-dei-dati.html
https://www.ubs.com/global/it/legal/privacy.html
https://www.sbb.ch/it/meta/legallines/datenschutz.html
https://www.amag-group.ch/it/footer/datenschutzerklaerung.html

→ **Eccezioni all'obbligo di comunicare** (art. 20 nLPD), in particolare se:

- persona interessata dispone già le informazioni;
- il trattamento è previsto dalla **legge** (es. numero AVS nel contratto di lavoro);
- non è possibile o richiede un onere sproporzionato (se non raccolti presso la persona interessata).
- ecc.

* vi è anche possibilità di differire o limitare; per esempio: in caso di interessi preponderanti di terzi, salvaguardia sicurezza nazionale, indagine giudiziaria, tutelare i mezzi di informazione (art. 27 nLPD).

9. Obbligo di informare sulle decisioni individuali automatizzate (art. 21 nLPD)

Il titolare del trattamento informa la persona interessata di ogni decisione basata esclusivamente su un trattamento di dati personali automatizzato che abbia per lei effetti giuridici o conseguenze significative (decisione individuale automatizzata).

→ Automatizzata = fondata su algoritmi;
→ La persona interessata può esprimere un parere sulla decisione e anche esigere che la decisione venga riesaminata da una persona fisica;
→ Gli organi federali devono designarla come tale;
→ **Eccezioni** all'obbligo di informare, in particolare:

- se la decisione è in relazione diretta con la **conclusione o esecuzione di un contratto** fra il titolare e la persona interessata e la richiesta di quest'ultima è soddisfatta;
- se la persona interessata ha dato il suo **espresso consenso** a che la decisione sia presa in maniera automatizzata;
- se previsto per legge (per gli organi federali).

Es. multa per eccesso di velocità rilevata sulla base di telecamere e dispositivo di rilevamento della velocità;
Es. diniego di un credito ipotecario;
Es. diniego di forme di assistenza sociale;
Es. mancata assunzione;
Es. adozione di misure di sicurezza da parte di un Autorità regionale di protezione;
Es. diniego o revoca di un permesso di soggiorno.

10. Obbligo di informare in caso di violazione (art. 24 nLPD)

Violazione della sicurezza dei dati (art. 5 let h) = *violazione della sicurezza in seguito alla quale, in modo accidentale o illecito, dati personali vengono persi, cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate.*

Esempi di violazione: hacking, invio e-mail ad un altro destinatario, perdita dati,…). → es. furto 2018 dati fiscali 5'000 abitanti del Comune di Rolle (VD).

*Il responsabile del trattamento **informa quanto prima il titolare** del trattamento su ogni violazione della sicurezza dei dati.*

*Il titolare del trattamento **notifica quanto prima all'IFPDT** ogni violazione della sicurezza dei dati che comporta verosimilmente un **rischio elevato** per la personalità o i diritti fondamentali della persona interessata.*

→ **Contenuto minimo** dell'informazione (cfr. art. 15 OPDa):

- tipo di violazione;
- momento e durata;
- categorie e numero di dati;
- categorie e numero delle persone interessate;
- conseguenze e rischi;
- misure disposte o previste;
- persona di contatto.

*Il titolare del trattamento informa la **persona interessata** sulla violazione della sicurezza dei dati, se ciò è necessario per proteggere la persona interessata o se lo esige l'IFPDT.*

Eccezioni? Possibile limitare, differire o rinunciarvi se:

- restrizioni del diritto d'accesso secondo art. 26 nLDP (legge, interesse preponderante,…);
- informazione impossibile o con onere disproporzionato;
- comunicazione pubblica equivalente (attenzione caso Sainsbury's! cibo avariato letale per i gatti).

11. Diritto d'accesso (art. 25 nLPD)

Chiunque può domandare al titolare del trattamento se dati personali che lo concernono sono oggetto di trattamento (per avere un controllo, eventualmente correggere i dati, cancellarli, ecc.).

→ **Contenuto minimo** dell'informazione fornita affinché la persona possa fare valere i suoi diritti:

- identità del titolare;
- dati trattati in quanto tale;
- scopo;
- durata di conservazione;
- informazione su raccolta presso terzi;
- esistenza di una decisione individuale automatizzata e la relativa logica;
- destinatari.

→ Domanda di norma per **iscritto** (anche per via elettronica), nonché oralmente con accordo.

→ Informazione entro **30 giorni**: in forma comprensibile, per iscritto (anche per via elettronica), o nella forma dei dati; per accordo anche in forma orale, o consultate sul posto.

→ Di principio, **gratuità**: ma possibile una partecipazione di max. CHF 300.00 se onere sproporzionato (informando preventivamente la persona sul costo; se non viene confermata entro 10 giorni, la richiesta è ritenuta ritirata).

→ Impossibilità di rinunciarvi preventivamente.

→ **Restrizione** del diritto di accesso (art. 26 nLPD): il titolare può rifiutare, limitare o differire:

- se previsto da una legge (es. a tutela del segreto professionale);
- in caso di interessi preponderanti di terzi, salvaguardia sicurezza nazionale, indagine giudiziaria, ecc. ;
- se la domanda è manifestamente infondata o se querulosa (nuovo motivo con la nuova legge!).

→ Restrizione del diritto d'accesso nei confronti dei mezzi di comunicazione (art. 27 nLPD): il titolare può rifiutare, limitare o differire:

- se i dati forniscono indicazioni sulle fonti;
- l'informazione permette di accedere a progetti di pubblicazioni;
- la libera formazione dell'opinione del pubblico rischia di essere compromessa;
- se i dati servono esclusivamente a titolo di strumento personale di lavoro per i giornalisti.

12. Diritto alla consegna o trasmissione (art. 28 nLPD)

Chiunque può esigere che i dati personali che lo concernono e che ha comunicato al titolare del trattamento gli siano riconsegnati o trasmessi a un terzo in un formato elettronico usuale, se:

- *il titolare tratta i dati personali in modo automatizzato; e*
- *il trattamento è effettuato con il consenso della persona interessata oppure in relazione diretta con la conclusione o l'esecuzione di un contratto fra il titolare e la persona interessata.*

→ Nozione di dati personali che la persona interessata a comunicato al titolare (art. 20 OPDa)
= si intendono:

- i dati messi consapevolmente e volutamente a disposizione;
- i dati che il titolare ha rilevato sulla persona interessata e sul suo comportamento nel quadro dell'utilizzo di un servizio o di un apparecchio.

* (non sono invece «dati comunicati» i dati prodotti in un'analisi separata dei dati personali messi a disposizione o osservati!)

→ Per quanto concerne le **questioni formali della richiesta e le restrizioni**, valgono sostanzialmente le stesse regole relative al diritto di accesso (cfr. art. 22 OPDa e 29 nLPD)

13. IFPDT e provvedimenti amministrativi (art. 49 nLPD)

IFPDT = Incaricato federale per la protezione dei dati e la trasparenza

- eletto dall'Assemblea federale;
- indipendente con personale proprio;
- risiede a Berna.

→ *L'IFPDT* ***apre, d'ufficio o su denuncia, un'inchiesta*** *nei confronti di un organo federale o di un privato se indizi sufficienti lasciano presumere che un trattamento di dati potrebbe violare le disposizioni sulla protezione dei dati.*

→ Chi è sospettato di un violazione delle disposizioni sulla protezione dei dati ha l'**obbligo di collaborare**.

→ In caso di mancata collaborazione, **l'IFPDT può ordinare** in particolare:

- l'accesso a ogni informazione e documento necessario all'inchiesta;
- l'accesso a locali e impianti;
- l'interrogatorio di testimoni;
- perizie di esperti.

→ l'IFPDT può prendere **provvedimenti amministrativi**, in particolare:
- ordinare di adeguare, sospendere o cessare del tutto o parte del trattamento, nonché cancellare o distruggere del tutto o parte dei dati;
- sospendere o vietare la comunicazione di dati all'estero;
- ordinare che vengano presi determinati provvedimenti tecnici e organizzativi (ai sensi degli art. 7 e 8 nLDP);
- ordinare che il titolare informi le persone interessate come da artt. 19, 21 e 24 nLPD;
- ordinare che venga consultato;
- ordinare che si proceda a una valutazione di impatto.

→ l'IFPDT non può sanzionare, ma può **sporgere denuncia penale** presso il Ministero pubblico cantonale (l'azione penale che si prescrive in 5 anni)

14. SANZIONI PENALI (art. 60 e segg. nLPD)

→ Tutti reati **intenzionali** (dolo eventuale?)

→ Chi viene punito? «i **privati** che…»

→ **5 tipi di reati:**

a) Violazione degli obblighi di informare, di concedere l'accesso e di collaborare (art. 60 nLPD) → multa fino a CHF 250'000.-.

b) Violazione degli obblighi di diligenza (art. 61 nLPD) → multa fino a CHF 250'000.-.

- in caso di comunicazione di dati all'estero in violazione della legge;
- in caso di affidamento del trattamento a un responsabile senza che siano adempiute le condizioni dell'art. 9 cpv. 1 e 2 LPD (es. effettua trattamenti non consentiti o non sicuri);
- in caso di non rispetto dei requisiti minimi in materia di sicurezza come da art. 8 cpv. 3 nLPD e 3 OPDa (necessità di prendere provvedimenti tecnici e organizzativi al fine di garantire la confidenzialità, la disponibilità, l'integrità e la tracciabilità dei dati).

c) Violazione dell'obbligo del segreto (art. 62 nLPD) → multa fino a CHF 250'000.-.

= rivelazione di dati personali segreti di cui si è venuto a conoscenza nell'esercizio di un professione.

e) Inosservanza di decisioni dell'IFPDT o di un autorità di ricorso (art. 62 nLPD) → multa fino a CHF 250'000.-.

f) Infrazioni commesse nell'azienda (art. 63 nLPD).

= se la multa applicabile non supera CHF 50'000 e se la determinazione delle persone punibili esige provvedimenti d'inchiesta sproporzionati all'entità della pena, l'autorità può prescindere da un procedimento contro dette persone e, in loro vece, condannare al pagamento della multa l'azienda.

Parte 3

Misure concrete da adottare

ALCUNE MISURE IMPORTANTI DA ADOTTARE:

- Procedere con una **formazione** adeguata dei collaboratori sulla protezione dei dati e la nuova normativa;
- Redigere **direttive** sul trattamento dei dati in seno all'impresa;
- Preparare un **vademecum** per rispondere rapidamente alle domande delle persone interessate (es. per l'informazione o l'eliminazione di dati);
- Controllare e modificare le **dichiarazioni sulla protezione** dei dati (sito web, contratti, contenuti pubblicitari, ecc.);
- Assicurare la **sicurezza** dei dati tramite misure tecniche e organizzative appropriate e adeguate in funzione del rischio;
- Predisporre una procedura di **segnalazioni** delle violazioni della protezione dei dati;
- Predisporre un **registro** di trattamento dei dati (salvo in caso di imprese con meno di 250 impiegati e in assenza di rischio elevato di lesione della personalità e dei diritti fondamentali);

Misure concrete da adottare

- Stabilire un procedimento per le **analisi d'impatto** che sono necessarie nel caso in cui il trattamento dei dati presenti un rischio elevato;
- Analizzare i **contratti** con i subappaltatori per verificare se la sicurezza dei dati è assicurata e aggiungere delle clausole specifiche (in particolare sulla segnalazione di ogni eventuale violazione, confidenzialità, responsabilità, ecc.);
- Prevedere la **soppressione** o **anonimizzazione** dei dati personali non appena non siano più necessari allo scopo del trattamento iniziale;
- Assicurarsi in caso di trasmissione all'**estero** che le esigenze e le garanzie stabilite dal Consiglio federale siano assicurate;
- Garantire la fornitura dei dati in forma **elettronica** (in caso di trattamento automatizzato dei dati e in particolare nell'ambito della stipula o dell'applicazione di un contratto);
- Designare per quanto possibile un **consulente** alla protezione dei dati, annunciandolo all'IFPDT;

Misure concrete da adottare

- Avvalersi se del caso del sostegno e **consiglio** di un avvocato, rispettivamente informatico esterno;
- Strutturare un approccio interno all'azienda **separato** per dipartimenti, in funzione del flusso dei dati trattati (HR, finanze, vendita e marketing, ricerca e sviluppo, reparto giuridico), responsabilizzando i rispettivi capisettori e imponendo un processo interno ad ogni unità;
- Allocare le **risorse finanziarie** necessarie ad un adeguata protezione dei dati;
- Sottoporre i sistemi di trattamento dati personali, i prodotti e i servizi a una valutazione da parte di organismi di **certificazione** indipendenti riconosciuti (certificazione secondo art. 13 nLDP e Ordinanza CF sulle certificazioni in materia di protezione dei dati);
- Adottare un **approccio sistematico** e un **controllo regolare** per garantire un'implementazione effettiva e efficace, anche in funzione della continua evoluzione tecnologica.

Parte 4

Casi concreti di interesse per affiliati Jardin Suisse Ticino

Breve riepilogo dei principi faro

(per sapere come agire in ogni situazione)

a) Informare la persona interessata del trattamento dati (cfr. slide 30):

- identità e dati di contatto del **titolare** (indirizzo completo, e-mail, telefono);
- **scopo** del trattamento;
- **destinatari** o categorie di destinatari;
- categorie di **dati** trattati;
- **Stato estero** o organismo internazionale destinatario e garanzie (se dati comunicati all'estero);

b) Assicurarsi di avere il «consenso» o un' «altrimenti legittimità» per il trattamento dei dati (cfr. slide 24):

- semplicemente **informandolo** (v. sopra pt. 1);
- in maniera **espressa** (se dati personali degni di particolare protezione o se profilazione a rischio elevato).

* se il trattamento e necessario per l'esecuzione di un contratto o se lo impone una legge non è necessario ottenere il consenso (cfr. slide 25).
** è sempre preferibile e consigliabile ottenere un consenso esplicito controfirmato (anche se non fosse necessario) !!!

c) Garantire la sicurezza del trattamento.

d) Conservare i dati fintanto che vi è un interesse legittimo → poi cancellare, distruggere o anonimizzare.

1) Videosorveglianza

→ Verificare la **liceità** (suolo privato SI; suolo pubblico NO; lavoratori di principio NO)

→ **Informare** tramite avviso, contratto di lavoro, regolamento aziendale, ecc.

→ **Conservare** i dati fin tanto che necessario (il meno possibile).

2) Sito internet

→ Verificare **quali dati** personali vengono trattati tramite il sito internet.

→ Munire il sito internet di **link** (ben visibile in calce) per visualizzare rapidamente l'informativa sulla protezione dei dati (cosiddetta **privacy policy**), nonché il link per la **cookies policy**.

→ **Informare** tramite privacy policy e cookies policy in maniera chiara e completa sul tipo di trattamento.

→ Munire il sito internet di **banner** (a rapida comparsa automatica) per offrire la scelta dei **cookie** non strettamente necessari (ossia i cosiddetti cookie di «esperienza», di «analisi» e di «marketing»).

3) Vendita diretta

→ Raccogliere/trattare dati con il **«consenso»** della persona interessata, **informandola** immediatamente in maniera chiara e completa (cfr. contenuto minimo della slide 47).

→ Informare e ottenere il consenso per esempio della possibilità di contattare ulteriormente il potenziale cliente per sottoporgli delle ulteriori **offerte promozionali**.

→ Informare e ottenere il consenso anche per esempio dell'eventuale **trasmissione di dati a terzi** (casa madre, fornitori, aziende-partner, ecc.) e per esempio della possibilità per questi terzi di trattare a loro volta i dati (trasmettere promozioni, ecc.).

4) Marketing

→ Chiedere alla persona interessata il **consenso** per venire contattati per finalità di marketing (e-mail, cartacea, telefono, ecc.).

→ Di principio non necessario ottenere il preventivo consenso per trasmettere e-mail per finalità di marketing a indirizzi non riconducibili a una persona specifica (**info@**azienda.ch).

→ Non è necessario chiedere il consenso per potere trasmettere tramite telecomunicazione (p. es. e-mail e telefono) a clienti o «quasi-clienti», per quanto riguarda la pubblicità di **prodotti e servizi analoghi di cui il cliente o il «quasi cliente»** ha già usufruito o è in procinto di usufruire; è sufficiente dare la possibilità di revocare il consenso in maniera rapida e semplice (e-mail con link in calce con «opt-out»).

→ È necessario chiedere il preventivo consenso in caso di pubblicità trasmessa per **posta cartacea** (anche se già clienti).

5) Servizi esternalizzati

→ In caso di esternalizzazione di qualsiasi operazione, per esempio di tipo contabile (per il tramite di una fiduciaria), oppure per l' incasso di fatture scoperte (tramite società di incasso), occorre **informare** la persona interessata della possibilità di comunicare i suoi dati a terzi per tali specifiche finalità. Si tratterà dunque di indicare che i dati verranno trasmessi a terzi per eseguire la gestione contabile corrente dell'azienda o per l'incasso di fatture scoperte (ciò segnatamente per il mezzo della privacy policy).

→ Si chiede così implicitamente l'**autorizzazione** a trattare i dati con tale scopo.

→ Si cercherà di **limitare le proprie responsabilità** in caso di eventuali violazioni della protezione dei dati da parte del terzo, scegliendolo in maniera accurata, regolamentando la **relazione contrattuale** con quest'ultimo, prevedendo clausole di confidenzialità e di garanzia della sicurezza dei dati.

N.B.: vige il di principio di **corresponsabilità**!

6) Risorse umane

→ I dati dei collaboratori possono essere trattati per quanto si riferiscano all'**idoneità lavorativa** o siano **necessari all'esecuzione** del contratto di lavoro (cfr. slide 9).

→ I dati vengono **conservati** fin tanto che ciò risulti necessario (es. certificato di lavoro fino max. 10 anni del termine di prescrizione).

→ È opportuno inserire delle **clausole** relativamente alla protezione dei dati nei contratti di lavoro e/o nel regolamento aziendale e/o per mezzo di direttive aziendali, in cui viene richiamata una più generale privacy policy.

→ Occorre **formare** i collaboratori sulla protezione dei dati (in particolare sulla comunicazione dei dati ai clienti e ai terzi, sulla sicurezza informatica, sui rischi in genere) nonché **regolamentare**/limitare gli accessi ai dati e ai locali contenenti i dati.

7) Infrastruttura informatica

→ Occorre accertarsi che sotto il profilo tecnico-informatico (**hardware e software**), ma anche **organizzativo** (gestione accessi), la **sicurezza** del trattamento dei dati personali è sufficientemente garantito.

→ Bisogna procedere con un **aggiornamento regolare** dell'infrastruttura informatica.

→ Occorre in particolare garantire una corretta **conservazione** dei dati, prevenire e impedire perdite di dati, soppressioni, **violazioni** e furti dei dati personali, ma anche accessi ai dati personali da parte di persone non autorizzate.

Studio legale
Barchi Nicoli Trisconi Gianini SA
T +41 91 912 20 00
Via S. Balestra 17
CP 1170
6901 Lugano
www.bnta.ch

Grazie per l‘attenzione!