PROTEZIONE DEI DATI

10 passi verso la nuova legge sulla protezione dei dati Le violazioni intenzionali degli articoli contrassegnati in **rosso** comportano sanzioni penali. Altre disposizioni possono essere oggetto di azioni di diritto civile.

01 ELENCO DEI CASI DI TRATTAMENTO DEI DATI

Art. 12 Fate un elenco dei processi e delle attività per cui le vostre organizzazioni trattano dati personali (per es. vendita, cookie, marketing, after-sales, noleggio, soccorso stradale, contabilità, amministrazione del personale,
shop online, videosorveglianza). **L'elenco deve comprendere almeno:** trattamento, scopo, categorie di persone, categorie di dati, destinatari /responsabili del trattamento, durata di conservazione, eventuali ulteriori informazioni all'occorrenza.

02 DICHIARAZIONE RELATIVA ALLA PROTEZIONE DEI DATI

Art. 19 Ogni volta che acquisite o trattate dati personali non richiesti per legge, prima di procedere al trattamento dovete fornire informazioni trasparenti in merito all'interno della dichiarazione relativa alla protezione dei dati. La scelta migliore è pubblicare tale dichiarazione sul sito web e segnalarla sulle videocamere, nei contratti (rimando alla dichiarazione concernente i dati personali) e ai candidati, nonché inserire una specifica dichiarazione relativa alla protezione dei dati nel regolamento per i collaboratori. **Tale dichiarazione contiene:** i vostri dati di contatto, lo scopo del trattamento dei dati, le categorie di destinatari, l'eventuale trasmissione all'estero (Paesi), i diritti degli interessati.

03 CONTRATTO CON I RESPONSABILI DEL TRATTAMENTO

Art. 9 La maggior parte delle imprese forniscono o cedono l'accesso ai dati anche a terzi, come per esempio fornitori di servizi informatici, aziende di marketing ecc. Questi cosiddetti responsabili del trattamento possono fare solo ciò che è consentito anche a noi.

Con detti terzi deve pertanto essere stipulato un apposito contratto che stabilisca la vostra sovranità sui dati e li vincoli alla protezione e alla sicurezza dei dati. È sufficiente un contratto conforme al diritto UE con un rimando alla LPD (modello disponibile per es. presso il servizio per la protezione dei dati del Liechtenstein).

04 SICUREZZA DEI DATI – TOM & DPIA

Art. 8 Proteggiamo i dati personali attraverso provvedimenti tecnici e organizzativi (TOM, dall'inglese «technical and organizational measures»). **A livello tecnico**: accesso solo con account personale e autenticazione multifattoriale, accesso di terzi solo su richiesta e con «audit trail», firewall, software antivirus, backup. **A livello organizzativo**: «clean-desk», «need-to-know», obbligo alla protezione dei dati e alla formazione, tritadocumenti ecc. **Obbligo di notifica (art. 24):** in caso di perdita dei dati è necessario prendere in considerazione una notifica all'IFPDT, edoeb.admin.ch, così come alle persone interessate.

Art. 22: quando l'organizzazione tratta una grande quantità di dati, molto sensibili o degni di particolare protezione ed eventuali errori o altri rischi potrebbero avere serie conseguenze per le persone interessate è necessario redigere e documentare una valutazione d'impatto sulla protezione dei dati (DPIA, dall'inglese «data protection impact assessment»). Attraverso la DPIA **i provvedimenti adottati per la protezione dei dati personali vengono sottoposti a un controllo approfondito della loro effettiva idoneità.**

05 TRASMISSIONE ALL'ESTERO

Art. 16 Niente estero in assenza di una protezione adeguata dei dati **Paesi in cui è possibile comunicare i dati personali:** UE, Regno Unito, SEE e singoli altri Paesi dell'elenco. Ricordate che tali Paesi devono essere menzionati nella dichiarazione relativa alla protezione dei dati.
I dati possono essere trattati in altri Paesi qualora ciò sia necessario e stabilito in via contrattuale per il singolo caso, se la persona interessata ha rinunciato a una protezione dedicata oppure **in presenza di cosiddette SCC, ossia clausole contrattuali standard europee con riferimento alla Svizzera**.

06 DIRITTI DELLA PERSONA INTERESSATA

Art. 25 segg. Assicuriamo alla persona interessata i diritti d'**accesso** specificati nella dichiarazione relativa alla protezione dei dati in merito ai dati personali (non documenti) che la concernono e su richiesta forniamo ulteriori informazioni. La legge concede un termine di 30 giorni per la fornitura gratuita di tali informazioni. Prima, tuttavia, dobbiamo identificare la persona che presenta la richiesta di accesso. Attenzione: fornire informazioni errate o incomplete comporta sanzioni. Lo scopo di tali informazioni deve essere la protezione della personalità. Ulteriori diritti: **rettifica** dei dati errati; **cancellazione** (può essere richiesta solo se non abbiamo un motivo prioritario o un obbligo di legge alla conservazione). In caso di **decisione basata esclusivamente su un trattamento di dati personali automatizzato (art. 21)**, su richiesta la stessa va riesaminata da una persona fisica.

07 PRINCIPI DI PROTEZIONE DEI DATI

Art. 6 Nei nostri processi interni all'organizzazione mettiamo in pratica i principi della protezione dei dati: **liceità, buona fede, limitazione della finalità, obbligo di cancellazione, esattezza, trasparenza e sicurezza dei dati.**
L'organizzazione documenta questi principi e la procedura per il rispetto degli obblighi di diligenza.

08 PRIVACY BY DEFAULT

Art. 7 Quando diamo alla persona interessata una scelta, le impostazioni relative alla protezione dei dati e alla sicurezza di un sistema, di un'applicazione o di un prodotto devono essere configurate **di default sulle opzioni più sicure e che tutelano maggiormente i dati**.

09 PICCOLO SEGRETO PROFESSIONALE

Art. 62 I dati personali che sono stati trasmessi all'organizzazione devono essere trattati con riservatezza salvo quando diversamente comunicato alla persona interessata.

10 FORMAZIONE DEL PERSONALE

Il personale ha un ruolo molto importante ai fini dell'attuazione e del rispetto della protezione dei dati. Vi sono numerosi motivi per cui collaboratrici e collaboratori devono essere formati in materia di protezione dei dati.

Prevenzione delle sanzioni: le violazioni della legge sulla protezione dei dati possono comportare notevoli sanzioni personali fino a CHF 250'000.

Sicurezza dei dati: il personale appositamente formato è preparato meglio a riconoscere e prevenire i potenziali rischi per la sicurezza (come attacchi phishing, password deboli e altri problemi di sicurezza).

Fiducia della clientela: i clienti tendono a fidarsi maggiormente delle imprese che tutelano i loro dati. Una efficace pratica di protezione dei dati può contribuire alla soddisfazione della clientela.

Il presente documento rappresenta una sintesi informativa sulla nuova legge sulla protezione dei dati, comprende solo le indicazioni minime e non considera filiali, ulteriori ambiti di affari ecc. In quanto tale, non costituisce una consulenza legale.

impunix
einfach datenschutz

Autore: Impunix AG, Lagerhausstrasse 18, 8400 Winterthur; info@impunix.ch