La nuova legge federale sulla protezione dei dati (nLPD): implicazioni, opportunità e “to do” list

SVIT Sezione Ticino

Taverne e online, 7 marzo 2022

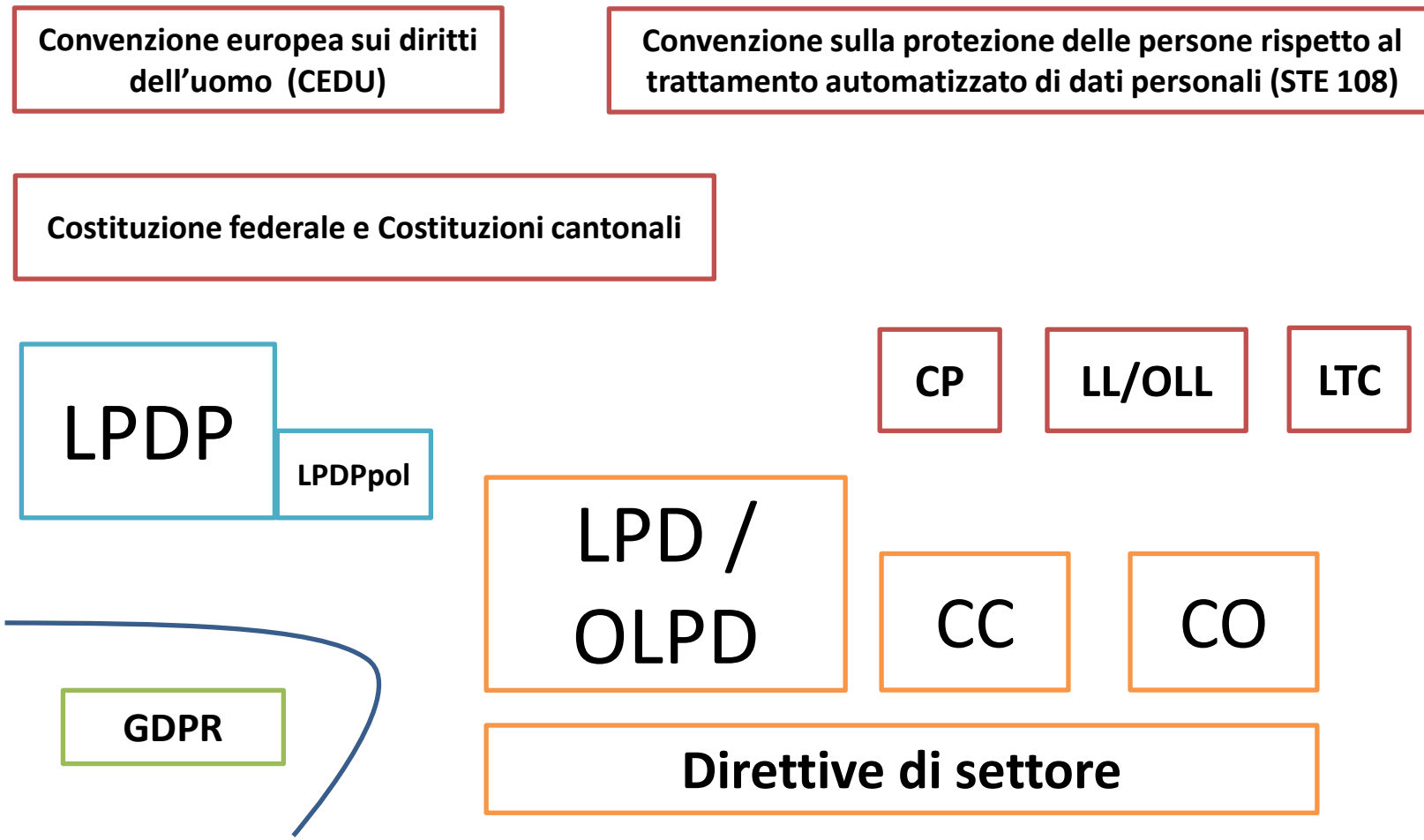
Avv. Gianni Cattaneo, Lugano

CBM Studio legale e notarile

www.cbm-lex.ch

gianni.cattaneo@cbm-lex.ch

Introduzione: quadro generale



Introduzione

REVISIONE (TOTALE) DELLA LEGGE SULLA PROTEZIONE DEI DATI PERSONALI (link)

- 01.04.2015: il CF decide di modificare la Legge federale sulla protezione dei dati (LPD)
- 15 settembre 2017: il Consiglio federale licenzia il **Messaggio concernente la revisione totale della legge sulla protezione dei dati (link) e il relativo Disegno di legge (link)**
- L'obiettivo generale è di modernizzare la LPD e di **adeguarla al diritto europeo**, affinché l'UE continui a riconoscere la Svizzera come uno Stato terzo con una protezione dei dati adeguata, in modo da consentire anche in futuro la comunicazione transfrontaliera di dati

Introduzione

- **nLPD**: adottata 25 settembre 2020 (testo finale: Link)

  Entrata in vigore: (**forse**) 1° gennaio 2023

- **pOLPD**: fase di consultazione (fino al 14 ottobre 2021)
  - Progetto posto in consultazione
  - Rapporto esplicativo
  - Tabella di concordanza
- **Nuovi poteri d'inchiesta e decisionali IFPD**
- **Sanzioni penali a carico dei manager (multe 250k)**
- **Promozione della fiducia dei mandanti**

Nuova Legge sulla protezione dei dati personali (nLPD)

Art. 1 Scopo

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

Art. 2 Campo d'applicazione personale e materiale

… si applica al trattamento di dati personali concernenti persone fisiche da parte di: a. **privati**; b. organi federali.

Non si applica al trattamento di dati personali da parte: …. di **persone fisiche per uso esclusivamente personale**

Nuova Legge sulla protezione dei dati personali (nLPD)

LPD disciplina le

«**attività di trattamento**»

= «qualsiasi operazione relativa a dati personali, indipendentemente dai mezzi e dalle procedure impiegati»

di

«**dati personali**»

= «tutte le informazioni concernenti una persona fisica identificata o identificabile»

- Dati ordinari
- Dati personali degni di particolare protezione

DIPENDENTI | CLIENTI | UTENTI WEB | VISITATORI | FORNITORI

Nuova Legge sulla protezione dei dati personali (nLPD)

Dati personali degni di particolare protezione:

- 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

Nuova Legge sulla protezione dei dati personali (nLPD)

- **violazione della sicurezza dei dati**: violazione 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 **(«CIA»)**
- **persona interessata**: la persona fisica i cui dati personali 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.

<u>Attenzione</u> alle traduzioni e ai malintesi!

Nuova Legge sulla protezione dei dati personali (nLPD) PRINCIPI GENERALI

- **Liceità = assenza di violazione della personalità**
- **Motivi giustificativi:** consenso (semplice o espresso); interesse preponderante pubblico o privato (es. adempimento contrattuale, ricerca, pianificazione, statistica, valutazione della solvibilità della controparte contrattuale) e legge (es. contabilità commerciale, dossier dipendente)
- Lesione della personalità (elenco non esaustivo): (i) trattamenti in violazione dei principi e della garanzia di sicurezza, (ii) trattamenti contro l'espressa volontà e (iii) comunicazione a terzi di dati degni di particolare protezione
- Di regola non vi è lesione della personalità se la persona interessata ha reso i suoi dati personali accessibili a chiunque e non si è opposta espressamente al trattamento

Nuova Legge sulla protezione dei dati personali (nLPD) PRINCIPI GENERALI

- **Buona fede (1)** e **Proporzionalità (2)**
  - (1) Divieto di inganni, sotterfugi e simili
  - (2) Minimizzare i dati raccolti e i trattamenti: solo quelli necessari per adempiere alle finalità; distruzione «asap»
  - Politica sulla conservazione dei dati personali
- **Sicurezza**
  - Approccio basato sul **rischio**
  - **Standard minimi** obbligatori (art. 1 – 4 D-OLPD)
  - Standard minimo TIC raccomandato da Confederazione

Nuova Legge sulla protezione dei dati personali (nLPD) PRINCIPI GENERALI

- **Finalità**: scopo del trattamento «determinato» e «riconoscibile»
- **Esattezza**: dati aggiornati, completi e veritieri
- Consenso **libero e informato** in riferimento a uno o più **trattamenti specifici**
  - Il consenso fornito dal dipendente o dell'inquilino è «libero»?
- **Privacy by design**: adozione fin dalla progettazione dei provvedimenti tecnici e organizzativi necessari affinché il trattamento sia conforme
- **Privacy by default**: tutela della privacy per impostazione predefinita

Nuova Legge sulla protezione dei dati personali (nLPD) OBBLIGHI PRINCIPALI (SALVO ECCEZIONI)

- Obbligo di **informazione** generalizzato 
- Cliente | Dipendente | Utente online | …
- Sussiste anche se i dati non sono raccolti presso la persona interessata
- Al momento della raccolta, il titolare del trattamento fornisce alla persona interessata almeno le informazioni seguenti:
  - l'identità e i dati di contatto del titolare del trattamento;
  - lo scopo del trattamento;
  - se del caso, i destinatari o le categorie di destinatari cui sono comunicati dati personali.

Nuova Legge sulla protezione dei dati personali (nLPD) OBBLIGHI PRINCIPALI (SALVO ECCEZIONI)

- Se i dati personali non sono raccolti presso la persona interessata: categorie di dati personali trattati.
- Se i dati personali sono comunicati all'estero: Stato destinatario e, se del caso, sulle garanzie di sicurezza.
- Se i dati personali non sono raccolti presso la persona interessata, il titolare del trattamento le fornisce le informazioni di cui ai capoversi 2–4 entro un mese dalla ricezione dei dati. Se comunica questi dati personali prima della scadenza di detto termine, il titolare del trattamento fornisce alla persona interessata tali informazioni al più tardi al momento della comunicazione dei dati.

Nuova Legge sulla protezione dei dati personali (nLPD) OBBLIGHI PRINCIPALI (SALVO ECCEZIONI)

Eccezioni:

- la persona interessata dispone già delle informazioni;
- il trattamento è previsto dalla **legge**;
- **segreto** fondato sulla legge;
- se i dati personali non sono raccolti presso la persona interessata: informazione impossibile o richiede un onere sproporzionato;
- interessi preponderanti di un terzo lo esigono;
- l'informazione pregiudica lo scopo del trattamento;
- è un privato e lo esigono i suoi interessi preponderanti e non comunica i dati personali a terzi (incluso intra-gruppo)

Nuova Legge sulla protezione dei dati personali (nLPD) OBBLIGHI PRINCIPALI (SALVO ECCEZIONI)

- **Delega** del trattamento a terzi: conforme alla legge 
- Non deve violare obbligo di **segretezza** legale o contrattuale
  - «Way out»: cifratura | funzione di ausiliario | consenso del cliente
- **Responsabilità** per l'intera filiera

Nuova Legge sulla protezione dei dati personali (nLPD)
OBBLIGHI PRINCIPALI (SALVO ECCEZIONI)

Contratto con il responsabile del trattamento?

Istruzioni di trattamento | Divieto di subappalto | Livelli di Sicurezza | Livelli di servizio (SLA) | Restituzione dei dati | Cancellazione | Localizzazione dei dati | Certificazioni | Riservatezza | Diritto applicabile e foro | Collaborazione per esercizio diritti interessati | Verifiche titolare | ecc.

Esiste un modello?

Modello danese approvato EDPB da modificare sulla base del diritto svizzero (link)

Nuova Legge sulla protezione dei dati personali (nLPD)

- Obbligo di dotarsi di un **registro delle attività di trattamento (**titolare e responsabile)
- **Eccezione**: persone fisiche o < 250 collaboratori e non sono trattati su vasta scala dati personali degni di particolare protezione e non viene eseguita una profilazione ad alto rischio (art. 26 D-OLPD)
- **Contenuto minimo**: identità, scopo del trattamento, descrizione delle categorie di persone interessate e delle categorie di dati personali trattati, categorie di destinatari, durata di conservazione o i criteri per determinarla, misure di sicurezza, Stati destinatari e garanzie
- **Esempio**: CNIL **UE** (link)

Nuova Legge sulla protezione dei dati personali (nLPD)

- Obbligo di svolgere **valutazioni d'impatto sulla protezione dei dati personali** (DPIA) in relazione ai trattamenti a «**rischio elevato**» (es. videosorveglianza, nuove tecnologie, dati sensibili, profilazione ecc.)
- **Eccezione**: trattamento è fondato su obbligo legale
- Obbligo di **consultazione preventiva** IFPDT (salvo DPO)
- **Esempio:** Governo olandese (**UE**) sull'uso di Teams in relazione a OneDrive, Sharepoint, Azure Active Directory (link)

Nuova Legge sulla protezione dei dati personali (nLPD)

- Obbligo di **notifica** all'IFPD delle **violazioni della sicurezza** dei dati in caso di probabile «rischio elevato»
- Obbligo di **comunicazione** delle **violazioni della sicurezza** dei dati alla persona interessata
  - Ordine dell'IFPD o
  - Necessario per proteggere la persona interessata
- **Piano in caso di emergenza**: team privacy competente e «allenato», politica di gestione delle violazioni della sicurezza, registro delle violazioni

Nuova Legge sulla protezione dei dati personali (nLPD)

- Divieto di **trasferire** i dati verso **Stati inadeguati** (ad es. USA) secondo accertamenti del Consiglio federale 
- Eccezioni (elenco non esaustivo):
  - DTA secondo SCC riconosciute da IFPD o
  - consenso espresso e informato della persona interessata o
  - adempimento contrattuale o
  - la persona ha reso i dati personali accessibili a chiunque e non si è opposta espressamente al loro trattamento
- **Cookie analitici USA**: Garante francese (link) e austriaco (link) sono intervenuti dichiarando illegale l'uso di Google Analytics
- **Gestori di newsletter USA**: Garante bavarese ha vietato l'uso da parte di una società tedesca (link)

Excursus: Privacy Shield CH - USA

Flussi transatlantici di dati personali

Sentenza 6 ottobre 2015: la Corte di Giustizia dell'Unione europea (CGUE) ha dichiarato invalida la decisione di adeguatezza della Commissione sulla protezione dei dati negli USA in regime "Safe Harbor"

Sentenza 16 luglio 2020: CJEU ha invalidato il «Privacy Shield» (link)

La Svizzera ha subito implementato la decisione della CGUE, depennando gli USA dall'elenco degli Stati dotati di una legislazione che garantisce una protezione adeguata.

Excursus: Privacy Shield CH - USA

Cosa fare?

- Parere **Settembre 2020** IFPD sulla trasmissione di dati personali negli Stati Uniti e in altri Stati che non garantiscono un livello di protezione dei dati adeguato conformemente all'articolo 6 capoverso 1 LPD (link)
  - BYOE – BYOK
  - Messo in dubbio validità delle Standard Contractual Clauses per il trasferimento di dati verso Stati inadeguati
- Guida **Giugno 2021** per l'esame dell'ammissibilità della comunicazione di dati all'estero (secondo art. 6 cpv. 2 lett. a LPD) (link)
- Guida **Agosto 2021** "The transfer of personal data to a country with an inadequate level of data protection based on recognized standard contractual clauses and model contracts" (link)

Nuova Legge sulla protezione dei dati personali (nLPD)

- **Diritti** degli interessati
  - Accesso ai dati: gratuità, 30 giorni, processo interno 
  - Aggiornamento
  - Cancellazione
  - Portabilità: trattamenti automatizzati fondati sul consenso
- **Contenuto minimo (diritto d'accesso):** identità e dati di contatto, dati personali trattati, scopo del trattamento, durata di conservazione dei dati o, se ciò non è possibile, i criteri per stabilirla, informazioni disponibili sulla provenienza dei dati, esistenza di una decisione individuale automatizzata e la logica su cui si fonda la decisione, destinatari o le categorie di destinatari, Stati destinatari e garanzie
- **Verifica identità: punto dolente!**

Nuova Legge sulla protezione dei dati personali (nLPD)

- **Consulente della protezione dei dati** (DPO)
  - Non obbligatorio nel settore privato
  - Requisiti precisi: competenze, indipendenza e autonomia (≠ manager)
  - Formazione, verifiche, consulenza
  - Pubblicazione dei dati di contatto
  - Comunicazione all'Incaricato
- **Vantaggio**: esenzione dall'obbligo di consultazione IFPDT in caso di DPIA a rischio elevato

Nuova Legge sulla protezione dei dati personali (nLPD)

- **Decisione basata esclusivamente su un trattamento di dati personali automatizzato** 

  che determina «effetti giuridici o conseguenze significative»

  es. esame automatizzato di solvibilità sito e-commerce

  – Obbligo di informazione (salvo eccezioni)
  – Diritto di esprimersi (su richiesta)
  – Diritto al riesame da parte di persona fisica

Diritto penale generale (CP)

Art. 29 CP Rapporti di rappresentanza

Se fonda o aggrava la punibilità, la violazione di un dovere particolare che incombe unicamente alla persona giuridica, alla società o alla ditta individuale è imputata a una persona fisica allorquando essa agisce:

a. in qualità di organo o membro di un organo di una persona giuridica;
b. in qualità di socio;
c. in qualità di collaboratore di una persona giuridica, di una società o di una ditta individuale nella quale esercita competenze decisionali autonome nel proprio settore di attività;
d. in qualità di dirigente effettivo senza essere organo, membro di un organo, socio o collaboratore.

Diritto penale speciale

Art. 60 Violazione degli obblighi di informare, di concedere l'accesso e di collaborare

Sono puniti, a querela di parte, con la multa fino a 250 000 franchi i privati che:

a. violano gli obblighi di cui agli articoli 19 [*informare*], 21 [*decisioni automatizzate*] e 25–27 [*accesso*], fornendo intenzionalmente informazioni inesatte o incomplete;

b. omettono intenzionalmente:

   1. di informare la persona interessata conformemente agli articoli 19 capoverso 1 e 21 capoverso 1, o

   2. di fornirle le informazioni di cui all'articolo 19 capoverso 2.

Sono puniti con la multa fino a 250 000 franchi i privati che in violazione dell'articolo 49 capoverso 3 forniscono intenzionalmente all'Incaricato, nel quadro di un'inchiesta, informazioni false o rifiutano intenzionalmente di collaborare.

Diritto penale speciale

Art. 61 Violazione degli obblighi di diligenza

Sono punite con la multa fino a 250 000 franchi i privati che intenzionalmente:

a. comunicano dati personali all'estero in violazione dell'articolo 16 capoversi 1 e 2 e senza che sussistano le condizioni di cui all'articolo 17;
b. affidano il trattamento di dati a un responsabile senza che sussistano le condizioni di cui all'articolo 9 capoversi 1 e 2;
c. non rispettano i requisiti minimi in materia di sicurezza dei dati emanati dal Consiglio federale secondo l'articolo 8 capoverso 3.

Diritto penale speciale

Art. 62 Violazione dell'obbligo del segreto

Chiunque rivela intenzionalmente dati personali segreti dei quali è venuto a conoscenza nell'esercizio di una professione che richiede la conoscenza di tali dati, è punito, a querela di parte, con una multa fino a 250 000 franchi.

È passibile della stessa pena chiunque intenzionalmente rivela dati personali segreti dei quali è venuto a conoscenza nell'ambito dell'attività svolta per conto della persona sottostante all'obbligo del segreto o in occasione della sua formazione presso tale persona.

La rivelazione di dati personali segreti è punibile anche dopo la cessazione dei rapporti di lavoro o di formazione.

Diritto penale speciale

Art. 63 Inosservanza di decisioni

È punito con la multa fino a 250 000 franchi il privato che intenzionalmente non ottempera a una decisione dell'Incaricato o a una decisione delle autorità di ricorso, notificatagli sotto comminatoria della pena prevista nel presente articolo.

Diritto penale speciale

Art. 64 Infrazioni commesse nell'azienda

Se la multa non supera i 50 000 franchi e se la determinazione delle persone punibili secondo l'articolo 6 DPA 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 (art. 7 DPA).

Action Plan: «what to do»

- **Sensibilizzazione CdA e Direzione**
  - Obblighi | Responsabilità
- **Nomina Leader + Formazione del Team**
  - Tecnico (informatica; sicurezza informatica)
  - Legale (specialista privacy e data protection)
  - Eventualmente: marketing, risorse umane, amministrazione
- **Identificazione del quadro normativo di riferimento per la tutela della privacy e la protezione dei dati personali**
  - LPD, GDPR ?, CC / CO / LL / LTC ecc. + normative di settore (es. settore immobiliare, attività fiduciaria, FINMA ecc.)
- **Definizione del Piano di valutazione («assessment»)**
  - Obiettivi | Tempistiche | Modalità di svolgimento | Budget | Criticità e settori sensibili | Priorità

Action Plan: «what to do»

- **«Mappare» i trattamenti di dati personali**, le **tecnologie**, **i soggetti coinvolti** e gli **Stati destinatari** (status quo)
- **Raccogliere i documenti rilevanti** (contratti con provider, politiche interne, contratti con clienti e dipendenti, informative esistenti ecc.)
- **Confrontare lo «status quo» con i requisiti legali applicabili** («gap analysis»)
- Stesura di una **relazione scritta** sulle lacune e sulle proposte per rimediarvi
- **Messa in conformità** («remediation»)

Action Plan: «what to do»

- **Rimedio alle lacune «secondo priorità»**
  - Reati penali (LL; requisiti minimi di sicurezza)
  - Visibilità «esterna» (sito; mandato con cliente)
  - Rischio accresciuto per gli interessati (es. videosorveglianza)
  - Dati degni di particolare protezione (HR)
  - Profilazione ad alto rischio (marketing)

Un esempio pratico

- **<u>«Home Office» → «lavorare da casa»</u>**

  = «sottocategoria» di «telelavoro» o «lavoro a distanza» → casa ≠ hotel, treno, bar ecc.

  - Gestione di dati e documenti aziendali da casa
  - Gestione e-mail aziendale da casa
  - Comunicazione a distanza con colleghi, clienti e fornitori
  - Collaborazione a distanza alle attività aziendali
- **Casa = «ufficio dislocato»**

Un esempio pratico

Portiamo

<u>la CASA in AZIENDA,</u>

<u>NON</u>

<u>l'AZIENDA in CASA</u>

Un esempio pratico

«Confessiamoci» (noi dipendenti): chi di voi non ha almeno una volta:

- inoltrato un'email aziendale al proprio indirizzo e-mail privato?
- trasmesso documenti aziendali tramite piattaforme di condivisione online?
- portato a casa dossier cartacei aziendali?
- condiviso una password personale con i colleghi d'ufficio?
- memorizzato su una chiavetta USB non cifrata un documento aziendale?

Un esempio pratico

- utilizzato un'App di messaggistica privata per inviare / ricevere documenti e/o informazioni aziendali?
- riciclato password con date di nascita e/o nomi dei figli e/o parole generiche per attivare servizi a distanza aziendali?
- lasciato incustoditi sul tavolo della cucina documenti aziendali?
- condiviso il computer usato per l'home office con famigliari?
- fatto una telefonata di lavoro in presenza di famigliari?
- usato servizi e piattaforme digitali per scopi lavorativi senza chiedere il consenso del datore di lavoro e consiglio al responsabile IT?

Un esempio pratico

«Confessate (imprese)»: chi di voi in questi anni ha:

- tollerato una delle attività precedenti?
- sensibilizzato il personale sui rischi legati al telelavoro?
- fornito un elenco di prodotti e servizi di verificata affidabilità e sicurezza per gestire il lavoro a distanza?
- fornito direttive e istruzioni ai dipendenti su come comportarsi durante il lavoro da casa?
- fornito indicazioni chiare per «securizzare» il perimetro casalingo (backup, password, cifratura dispositivi mobili, BYOD, clear desk, wi-fi, rete domestica ecc.)?

Una sentenza utile: videosorveglianza del locatore e privacy (LPD e art. 28 CC)

- DTF 142 III 263 (link) del 29 marzo 2016
- Tema: Valutazione dell'ammissibilità di un sistema di videosorveglianza in un immobile con appartamenti in locazione
- Fatti: 24 appartamenti; 12 telecamere (9 esterne e 3 interne); locali comuni (inclusa lavanderia e parti interne dell'entrata); consenso dei locatari salvo un inquilino (azione in rimozione); scopi dichiarati: prevenzione vandalismi e controllo degli accessi (misura anti intrusione)
- Diritto: LPD applicabile; principio di proporzionalità; ponderazione tra interessi proprietario vs inquilini

Una sentenza utile: videosorveglianza del locatore e privacy (LPD e art. 28 CC)

- Esito:
  - sorveglianza disproporzionata (e pertanto illecita) non giustificata: spazi comuni interni (pochi inquilini e rischio concreto di furti minimo data la natura dei locali)
  - sorveglianza giustificata: spazi esterni (inclusa l'entrata)
- Osservazioni:
  - Ponderazione **CASO PER CASO**
  - Regolamento sulla videosorveglianza: scopi, sicurezza, accessi
  - 24-72 ore conservazione (salvo esigenze giustificate)
  - Avvisi che sussiste un impianto di videosorveglianza
  - Se ripresi dipendenti: art. 328 e 328b CO; art. 26 OLL3 (divieto della sorveglianza pura del comportamento); coinvolgimento dei dipendenti

Per finire…


Il diritto alla protezione dei
dati è l'inizio di ogni libertà