

CBM

CATTANEO  
BIONDA  
MAZZUCHELLI  
STUDIO LEGALE E NOTARILE

LA PROTEZIONE DEI DATI PERSONALI NEL SETTORE PUBBLICO

[WWW.CBM-LEX.CH](http://WWW.CBM-LEX.CH) | [GIANNI.CATTANEO@CBM-LEX.CH](mailto:GIANNI.CATTANEO@CBM-LEX.CH)

# INTRODUZIONE

- Digitalizzazione: **IMMENSE opportunità, NUOVI rischi**
  - 1 click
  - bisogno di sicurezza e di protezione delle INFORMAZIONI e dei MEZZI INFORMATICI
    - provvedimenti tecnici
    - provvedimenti organizzativi
  - responsabilizzazione dei «capi» → compito dirigenziale
  - sviluppo di competenze e sensibilità (dirigenti, collaboratori, utenti) → «anticorpi»
  - interconnessione, «effetto domino»
  - confidenzialità vs disponibilità: quale attributo è più importante?
  - divario digitale
  - costi (licenze, personale, software, cloud ecc.)
  - dipendenza

# OBBLIGO DI SEGNALAZIONE DEI CIBERATTACCHI ALLE INFRASTRUTTURE CRITICHE (LSIN)

- Ufficio federale della cibersicurezza (UFCS) (ex Centro nazionale per la cibersicurezza – CNCS)
- Cyber Security Hub (CSH)
- Ufficio federale della protezione della popolazione UFPP - Le infrastrutture critiche (homepage)
  - Comuni, organizzazioni di primo intervento, acqua potabile, acque di scarico, energia, rifiuti ecc.
  - ciberattacco: un evento provocato intenzionalmente che si verifica nell'utilizzo di mezzi informatici e che compromette la confidenzialità, la disponibilità o l'integrità delle informazioni o la tracciabilità del loro trattamento
  - condivisione tempestiva: entro **24 ore**
  - segnalazione **progressiva**
  - **sostegno gratuito** dell'UFCS
  - sanzione penale (1° ottobre 2025)
  - **PRONTEZZA: REGOLE / RUOLI / RESPONSABILITÀ / COMPETENZE / TEAM**

# OBBLIGO DI SEGNALAZIONE DEI CIBERATTACCHI ALLE INFRASTRUTTURE CRITICHE (LSIN)

## **Notifica obbligatoria** → **ciberattacchi alle infrastrutture critiche**

Dal 1° aprile 2025, le infrastrutture critiche dovranno comunicare all'OFCS gli incidenti informatici critici. I criteri per determinare se la vostra autorità o organizzazione è tenuta alla segnalazione sono disponibili sulla [piattaforma di pubblicazione del diritto federale](#). In una [guida passo passo](#), potete scoprire se il vostro incidente è da segnalare e come farlo correttamente.

## **Notifica volontaria** → **ciberincidenti involontari, cyberminacce, vulnerabilità, (altri) ciberattacchi**

Tramite il modulo online possiamo individuare possibili tendenze di pericoli su Internet e intervenire in modo mirato. [Dopo aver risposto ad alcune domande](#), riceverete una prima valutazione automatica del vostro caso con le misure da adottare e potrete quindi inoltrare il caso all'Ufficio federale della cbersicurezza UFCS per l'ulteriore elaborazione. [Segnali l'incidente qui](#).

# COMUNE TICINESE: LPD O LPDP?

## Qual è il campo d'applicazione della LPD?

... si applica al trattamento di dati personali concernenti **persone fisiche** da parte di:

a. **privati**

b. **organi federali**

→ Sentenza 9C\_650/2021 c. 5.3.2. nel settore LAMal: «*tâche publique de la Confédération*»

# COMUNE TICINESE: LPD O LPDP?

## Qual è il campo d'applicazione della LPDP / **pLPDP?**

### **Art. 2 Campo di applicazione – in generale**

2 Alla legge sottostanno il Cantone, i Comuni, le altre corporazioni e istituti di diritto pubblico e i loro organi. A questi sono parificate le persone fisiche e giuridiche di diritto privato, cui siano demandati / **delegati** compiti pubblici / **di diritto pubblico**.

3 La legge non si applica nella misura in cui uno di questi enti partecipa a una attività economica che non deriva da un potere sovrano. **Rimangono riservate le competenze di vigilanza dell'Incaricato cantonale della protezione dei dati ai sensi dell'articolo 37 lettera b e dell'articolo 38.**

# COMUNE TICINESE: LPD O LPDP?

- «**Rapporto**» con l'interessato: privato – orizzontale (LPD); pubblico – verticale (LPDP)
- Delega ai privati:
  - compiti stabiliti dal diritto pubblico
- Esempio: clinica psichiatrica privata inserita nella pianificazione ospedaliera pubblica cantonale: LPDP in relazione ai dati personali dei pazienti
- Messaggio LPDP riporta le seguenti esclusioni dal campo di applicazione della LPDP: «*gli istituti bancari cantonali, le assicurazioni immobiliari cantonali, le aziende industriali*»
- Ambiti di competenza legislativa materiale federale (ad es. cartella informatizzata del paziente)

# LA REVISIONE DELLA LPDP: COMMENTI ALLA CHECKLIST DI ADEGUAMENTO

- <https://www4.ti.ch/can/sgcds/pd/generalita/revisione-totale-lpdp>
- Rafforzamento delle competenze e del modo d'intervento dell'Incaricato cantonale della protezione dei dati (art. 38 pLPDP) (**inchiesta / raccomandazione / decisione**)
- Con la nuova LPDP vengono istituiti i seguenti nuovi obblighi:
  - informazione qualificata nei confronti della persona interessata riguardante la raccolta di dati personali (art. 10 pLPDP) → **TRASPARENZA / CONSAPEVOLEZZA**
    - SCHEDA
  - prova della protezione dei dati (art. 8 pLPDP) → **RESPONSABILIZZAZIONE / VERIFICABILITÀ**
    - SCHEDA

# LA REVISIONE DELLA LPDP: COMMENTI ALLA CHECKLIST DI ADEGUAMENTO

- valutazione d'impatto sulla protezione dei dati (art. 13 pLPDP) → **RIFLESSIONE / COLLABORAZIONE / MITIGAZIONE / CONSAPEVOLEZZA**
  - SCHEDA
  - Promemoria IFPDT
- segnalazione di incidenti che implicano un grave rischio per la protezione dei dati (art. 16 pLPDP) → **PREVENZIONE E (AUTO)PROTEZIONE**
  - SCHEDA
  - Rapporto con segnalazione LSIn?
    - Dati personali
    - Incidente intenzionale o volontario, anche senza mezzi informatici
  - Interessato?

# LA REVISIONE DELLA LPDP: COMMENTI ALLA CHECKLIST DI ADEGUAMENTO

## Checklist per l'adeguamento alla LPDP

---

Incaricato cantonale della protezione dei dati

6501 Bellinzona

[www.ti.ch/protezionedati](http://www.ti.ch/protezionedati)

- I. OBBLIGHI E INCOMBENZE **PREESISTENTI** ALLA REVISIONE TOTALE DELLA LPDP
  - II. OBBLIGHI **DERIVANTI** DALLA REVISIONE TOTALE DELLA LPDP
  - III. PIANIFICAZIONE E ESECUZIONE
- Periodo transitorio di «sospensione» degli obblighi suoi nuovi trattamenti?

[Checklist per l'adeguamento alla LPDP](#)

# SPUNTI PER LA DISCUSSIONE

- **IMPLEMENTAZIONE STRUMENTI BASATI SU IA GENERATIVA**
  - Valutazione d'impatto sulla protezione dei dati personali
  - Decisione organi preposti con strategia correlata (**non «dal basso»**)
- Assistente virtuale (chatbot) sito comunale
  - Sicurezza delle chat e dei documenti condivisi
  - DPA / fornitore affidabile / catena dei sub-fornitori
  - Termini e condizioni d'uso per l'utente (divieti, limitazione di responsabilità, obbligo di verifica)
  - Informativa sul trattamento dei dati personali (ad es. visibilità chat, fornitori ecc.)
- Ausilio al collaboratore
  - Elenco degli strumenti autorizzati con relative regole d'uso (impostazioni)
  - Direttive d'uso generali (ad es. divieto comunicazione dati segreti, dati personali e dati protetti dal diritto d'autore)
  - Workshop interni
- Decisioni individuali automatizzate (es. e-recruiting)
  - Base legale

# SPUNTI PER LA DISCUSSIONE

- **MS 365 / CLOUD**

- Valutazione d'impatto sulla protezione dei dati personali
- Impostazioni concrete e tecnologie di protezione della privacy («PET»)
- Contrattualistica adeguata (DPA, SLA e CGC)
- Rispetto delle raccomandazioni PRIVATIM
- *Privatim constate que l'utilisation de solutions SaaS internationales pour les organes publics est possible uniquement si les données sensibles ainsi que les données personnelles soumises à une obligation légale de garder le secret sont cryptées par l'organe responsable lui-même. Le fournisseur de services de cloud computing ne doit pas avoir accès à la clé.*

- **SITO WEB E GDPR / PRINCIPIO DI PROPORZIONALITÀ (MINIMIZZAZIONE)**

- Applicazione extra – territoriale del GDPR
- Cookies statistici e di profilazione, social media plug-in, widget
- Sorveglianza del comportamento di persone ubicate nell'UE
- Contenuti indirizzati all'estero (bandiere, prezzi in EUR, lingue europee ecc.)

# SPUNTI PER LA DISCUSSIONE

- **FORNITORI DI PRESTAZIONI INFORMATICHE CHE TRATTANO DATI PERSONALI**
  - Censire, istruire e verificare
  - Convenzione sulla protezione dei dati personali
- **Informazioni relative al consumo di acqua potabile**
  - Sentenza TF 1C\_273/2020 del 5 gennaio 2021
  - Dati personali
  - Particolarmente «invasivi»
  - Scopo: fatturazione (raccolta troppo frequente – violazione del principio di proporzionalità)
- **Poliziotto comunale (Zh) condivide informazioni con Amministrazione comunale / Controllo Abitanti concernenti attività di Polizia**
  - Sentenza TF 6B\_994/2024 del 30 aprile 2025
  - 4 e-mail
  - Condannato per violazione del segreto d'ufficio (art. 320 CP)

# SPUNTI PER LA DISCUSSIONE

- **DISCUSSIONE!**
- **Grazie per l'attenzione!**

[www.cbm-lex.ch](http://www.cbm-lex.ch) | [gianni.cattaneo@cbm-lex.ch](mailto:gianni.cattaneo@cbm-lex.ch)