



PRIVACYDESK®
S U I S S E





ADEMPIMENTI OPERATIVI ai sensi della LPD





**Premessa LPD e Cybersecurity:
due facce della stessa medaglia**

**I rischi del non fare nulla e perché è
un'occasione per crescere?**

Passi concreti per mettersi in regola



Premessa LPD e cybersecurity: due facce della stessa medaglia

Protezione dei dati = protezione informatica

La LPD richiede che i dati siano **protetti “in modo adeguato”**. Questo significa **implementare misure tecniche e organizzative** → esattamente ciò che fa la **cybersecurity**.

Anche una PMI deve:

- Proteggere l'accesso ai dati digitali
- Evitare perdite, furti o accessi non autorizzati
- Essere in grado di dimostrare di aver preso misure adeguate



I rischi del non fare nulla

Attenzione a questi falsi miti

“Tanto siamo piccoli...”

“La legge è solo per i grandi”

“Nessuno ci controllerà mai”

“Ho parlato con le mie conoscenze e non hanno fatto niente”





Perché è un'occasione per crescere?

1

Fidelizzazione:

i clienti si fidano di chi protegge i loro dati

2

Vantaggio competitivo:

chi è conforme può lavorare con grandi aziende

3

Migliore organizzazione interna dei dati e dei processi

Meno rischi, più controllo



Passi concreti per mettersi in regola



1

Mappare i dati trattati

2

Formare il personale

3

Aggiornare informative privacy

4

Essere pronti alla gestione dei data breach

5

Rafforzare la sicurezza informatica

6

Mappare monitorare e verificare i fornitori che trattano dati

7

Redigere il registro dei trattamenti (se necessario)



Mappatura dei dati personali

Cosa significa "mappare" i dati personali?

Capire quali dati raccogliamo e perché:

Nomi, email, IBAN, CV, dati sanitari, ecc.

Dove li conserviamo?

Email, Excel, software, cloud, cartaceo?

Chi vi accede? Per quanto tempo?



Cos'è il Registro dei Trattamenti?

Un documento (digitale o cartaceo) **che descrive come vengono trattati i dati personali** all'interno dell'organizzazione.

Chi deve tenerlo?

Obbligatorio per imprese con 250+ collaboratori. Anche per PMI se:

Effettuano profilazioni su larga scala

Trattano dati sensibili su larga scala

Usano tecnologie ad alto rischio per i diritti delle persone

Cosa deve contenere? (*contenuto minimo*)

Finalità del trattamento

Categorie di dati trattati

Categorie di persone interessate

Destinatari dei dati (interni/esterni)

Durata di conservazione

Misure di sicurezza

Responsabile del trattamento

Eventuale trasferimento all'estero



Strumenti a supporto





L' informativa privacy

*Non serve un romanzo...
ma serve chiarezza...*

Cosa deve contenere:

- 1 L'identità del Titolare del trattamento
- 2 Quali dati vengono trattati
- 3 Perché li trattiamo (finalità)
- 4 Con chi li condividiamo (eventuali terzi)
- 5 Se i dati vengono comunicati all'estero, dove e in base a quale garanzia
- 6 Per quanto tempo li conserviamo
- 7 I diritti della persona (accesso, cancellazione, rettifica)

Usare un linguaggio semplice, evitare legalese

Mappare monitorare e verificare i fornitori che trattano dati

Il tuo fornitore tratta dati? Allora ti riguarda.

Sei responsabile anche per ciò che fanno **i tuoi fornitori**
(cloud, marketing, HR, IT...)

Obbligo di:

Verifica della conformità

Contratto scritto (es. "contratto di incarico")

Istruzioni documentate su cosa fare con i dati

Strumento pratico:

Checklist per valutare i fornitori

Modello base di accordo per i fornitori che trattano dati

GRAZIE !



[privacydesk.ch](https://www.privacydesk.ch)