La nostra direttiva sulla protezione dei dati.

Organizzazione:

Di cosa si tratta?

La presente direttiva regola la gestione dei dati personali* all'interno della nostra azienda ed è vincolante per tutti i collaboratori (comprese le persone integrate nell'azienda).

Emanato da/il/ a partire da:

Chi è responsabile di cosa in materia di protezione dei dati?

1. Ogni trattamento di dati nell'azienda ha una **persona responsabile (PR)**. La PR è la proprietaria della relativa attività aziendale (a meno che la direzione non abbia stabilito diversamente) nonché ogni persona che determina aspetti essenziali del trattamento dei dati. I superiori della PR sono responsabili della sua selezione, istruzione e supervisione. La PR riferisce loro di propria iniziativa in merito a eventi importanti.
2. Ogni PR deve garantire che le prescrizioni della legge sulla protezione dei dati (**LPD**) e in particolare le prescrizioni ai sensi della scheda seguente "nLPD: Cosa fare" (congiuntamente, le **prescrizioni LPD**) siano rispettate. Eccezioni devono essere motivate. Trattamenti di dati nuovi o modificati devono essere notificati alla DS.
3. Ogni PR deve garantire il rispetto delle disposizioni relative alla **conservazione** e alla **cancellazione** di documenti e dati personali.
4. **L'ufficio per la protezione dei dati (UPD)** designato dalla direzione cura l'attuazione e il rispetto delle prescrizioni LPD e offre consiglio alla PR. Non ha poteri decisionali, ma segnala alla direzione le violazioni sostanziali delle prescrizioni LPD.
5. Le regole sulla protezione dei dati stabilite dalla PR e le decisioni prese sono vincolanti per i **collaboratori**. Essi devono inoltre attenersi alle prescrizioni LPD e segnalare tempestivamente, in particolare, le violazioni della sicurezza dei dati nonché le richieste di terzi relative alla protezione dei dati (si veda il foglio seguente).
6. Tutti si attengono al **segreto professionale**. Divulgazione solo previa liberatoria.

Il mancato rispetto di tali responsabilità e direttive può comportare conseguenze disciplinari, civili e penali, fino al licenziamento.

Ci sono ulteriori disposizioni?

Per quanto va conservato cosa?

Principio: Tutto di cui non abbiamo più bisogno per l'attività quotidiana, lo archiviamo. Distruggiamo/cancelliamo per i seguenti termini & documentiamo:

Incarto personale	10 anni d. cessazione
Dati HR temp. rilevanti	3-5 anni (ad es. qualifiche, assenze)
Candidature	4 mesi d. rifiuto
Contratti	10 anni d. SD (20 anni per rischi di salute)
Contabilità	15 anni d. EF
Corrispondenza su un argomento	Analogo al tema (ad es. contratti)
Sinistri	20 anni

☐ Abbiamo una lista separata/ulteriore

Persona responsabile?

Trattamento dei dati	Chi?

Ufficio protezione:

Cosa vale per la sicurezza die dati?

Non condividiamo mai nostra password e non la usiamo per account (privati).

Non lasciamo mai incustoditi dati riservati o dispositivi contenenti tali dati.

Non memorizziamo dati aziendali su computer privati o in e-mail private.

Non clicchiamo su allegati e link da fonti sconosciute/non sicure.

Manteniamo i nostri dispositivi aggiornati, installiamo software con autorizzazione.

Non inseriamo dati riservati in servizi online non autorizzati a tale scopo.

Siamo discreti durante le conversazioni e il lavoro al computer con terzi vicini.

Non smaltiamo i dati personali altrui nel cestino, ma nel distruggidocumenti.

Evitiamo copie ombra dei dati.

Ci assicuriamo di dare dati personali solo a persone autorizzate e dove necessario.

Cosa facciamo con i dati dei dipendenti?

Raccogliamo i dati che ci fornite, nonché i dati provenienti da pubbl. registri, da autorità, da Internet, dai media e dalle registrazioni delle attività informatiche e delle e-mail.

Li trattiamo per l'interazione con loro, per eseguire il rapporto di lavoro (incluso l'utilizzo delle prestazioni lavorative), lo sviluppo del personale, a scopi di sicurezza e operativi, a fini di conformità, procedimenti, indagini, per eventi & marketing.

Li condividiamo con fornitori di servizi, autorità, clienti, altri partner commerciali, società del grup-po, media, l'opinione pubblica, altri datori di lavoro.

Inoltre si applica la nostra informativa sulla privacy.

☐ Esiste un'informativa separata per i dati personali

* I dati personali sono dati che si riferiscono a persone direttamente identificate (ad es. tramite nome, foto) o indirettamente identificabili con l'ausilio di fonti terze (ad es. In base alla qualifica professionale).

Abbreviazioni: Esercizio finanziario (**EF**), Scadenza (**SD**)

Versione 20.7.2023 – Aggiornamenti: www.rosenthal.ch

Autore: David Rosenthal, drosenthal@vischer.com

Tutti i diritti riservati. Può essere liberamente distribuito/utilizzato senza modifiche (tranne nei campi). Sono informazioni, non consulenza legale.

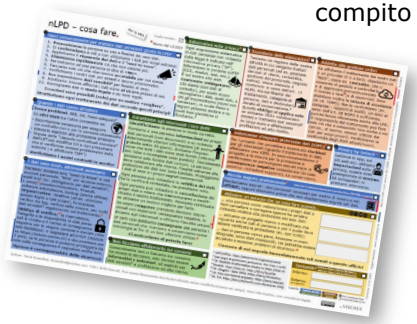
VISCHER SWISS LAW AND TAX

Una semplice direttiva generale sulla protezione dei dati per le PMI .

Verifichi gratuitamente la Sua conformità alla LPD su privacyscore.ch

La pagina precedente contiene una direttiva sulla protezione dei dati formulata in modo semplice ma esaustiva nei suoi punti essenziali, destinata alle piccole e medie imprese e conforme alla nuova legge sulla protezione dei dati (**LPD**), in vigore dal 1° settembre 2023.

La pagina precedente integra la nostra guida sintetica "Survival Guide" sulla LPD, che raissume anch'essa in un'unica pagina tutti i requisiti essenziali della LPD. Con la presente direttiva, la direzione aziendale può adottare tale documento di sintesi con valore vincolante, stabilendo al contempo le necessarie resopnsabilità operative. In base alla nostra esperienza, a quest'ultimo profilo viene spesso dedicata un'attenzione insufficiente; esso risulta tuttavia cruciale, in particolare alla luce dell'inasprimento delle norme penali introdotte dalla LPD (si veda al riguardo il nostro blog https://www.vischer.com/know-how/blog/wie-strafbarkeit-unter-dem-neuen-datenschutzgesetz-vermieden-wird/).



https://www.rosenthal.ch/downloads/VISCHER-revDSG-Survival-Guide.pdf

Per adottare la direttiva, compili innanzitutto i campi vuoti del primo foglio della direttiva (ovvero il modello sopra riportato). Indichi in alto il **nome della società**; in alto a destra è inoltre possibile inserire il logo aziendale.

Successivamente, completi la tabella con i **termini di conservazione**. Abbiamo già indicato alcuni termini di conservazione tipici; può aggiungerne altri nel modulo o in un elenco separato. Vale la regola fondamentale secondo cui i documenti e i dati personali devono essere distrutti o cancellati unicamente (ma in ogni caso) nel momento in cui scade un eventuale termine legale di conservazione e non sussiste alcun altro motivo di conservazione (ad es. qualora i documenti possano ancora servire come mezzi di prova finché decorrono i termini di prescrizione). Ciò non fa parte a rigore di una direttiva sulla protezione dei dati, ma poiché spesso manca, lo abbiamo integrato direttamente nel nostro modello come"bonus".

Occorre stabilire chi sia la **persona responsabile** di ciascun trattamento dei dati (la «**PR**«). Per ogni attività in cui vengono trattati dati personali, un soggetto deve essere responsabile del rispetto delle norme sulla protezione dei dati, ossia prendere le decisioni necessarie a tale scopo. Di norma, si tratta del "business owner" dell'attività in questione, poiché il trattamento dei dati viene effettuato per suo conto. Tale persona ne trae i benefici, ne sostiene i costi e deve pertanto disporre del relativo potere decisionale.

Nella pratica, indica ai collaboratori coinvolti nel trattamento di dati le istruzioni da seguire. Chi dirige ad esempio il dipartimento HR stabilisce per quanto tempo e quali documenti devono essere conservati, chi ha accesso, quali dati vengono trattati, dove vengono trattati, ecc. In un'azienda di dimensioni molto ridotte, tale compito spetterà alla direzione.

Questa persona (RP) deve fare in modo che le prescrizioni di protezione dei dati siano attuate come indicato sulla pagina riassuntiva – da lei stessa, dai collaboratori o mediante un supporto esterno. Deve quindi provvedere affinché esista un'informativa sulla protezione dei dati, siano rispettati i "dieci comandamenti", siano stipulati i contratti necessari con terzi, sia garantita la sicurezza dei dati e siano soddisfatti i diritti degli interessati in caso di richieste. Nella direttiva, la RP può essere indicata per singoli trattamenti di dati (ad es. con la sigla o con "DG").

Dovrebbe anche essere registrato chi sia il **servizio per la protezione dei dati** (nella misura in cui ne esista uno; nelle piccole aziende la RP assume questo ruolo). Tale servizio ha una funzione di coordinamento e di consulenza, non deve necessariamente essere uno specialista, ma deve sapere a chi rivolgersi per chiedere chiarimenti e occuparsi delle questioni operative. Il suo nome dovrebbe essere inserito anche nei campi liberi della pagina riassuntiva contenente le prescrizioni (ossia sotto il titolo "Abbiamo un servizio…" e alla voce "Domande?" in basso a destra).

Infine, vi è ancora spazio per ulteriori **indicazioni e direttive individuali** (ad es. per altri aspetti da osservare o documentazione). In alto a sinistra si può indicare chi ha **emanato** la direttiva, quando e a partire da quando si applica.

Avvertenza: Come ulteriore "bonus" abbiamo inserito anche una breve informativa sulla protezione dei dati per i collaboratori, questo poiché tale documento è raccomandabile ai sensi della LPD. Poiché tuttavia non vi è spazio per tutto e presumiamo che tutte le imprese dispongano anche di un'informativa sulla protezione dei dati "normale", per le informazioni mancanti rimandiamo semplicemente a quest'ultima.

Ha domande o necessita di modelli più dettagliati, materiale di formazione o altra assistenza? Scriva alla Sua persona di fiducia oppure a noi all'indirizzo dataprivacy@vischer.com.

VISCHER
SWISS LAW AND TAX