



Direttiva sulla protezione dei dati

Generale

1. Introduzione

- 1.1. I dati disponibili in azienda sono di grande valore per l'impresa. Questi dati devono quindi essere protetti dall'accesso non autorizzato e da altre minacce.
- 1.2. I clienti, i partner e i dipendenti dell'azienda si aspettano che i dati affidati all'azienda siano particolarmente protetti e trattati con cura.
- 1.3. Per qualsiasi domanda sulla protezione dei dati o sul trattamento dei dati personali, è possibile contattare la Fédération romande des écoles de conduite.

2. Scopo della direttiva sulla protezione dei dati

- 2.1. Lo scopo della presente direttiva sulla protezione dei dati è quello di creare standard uniformi per la protezione dei dati all'interno dell'azienda.
- 2.2. Rispettando le norme stabilite nella presente politica di protezione dei dati, l'azienda adempie ai propri obblighi in materia di protezione dei dati e garantisce che gli interessi e i diritti degli interessati siano sufficientemente presi in considerazione.
- 2.3. L'osservanza della presente direttiva sulla protezione dei dati è un prerequisito per lo scambio sicuro di dati personali all'interno dell'azienda e con terzi.

3. Ambito di applicazione della direttiva sulla protezione dei dati

- 3.1. La presente direttiva sulla protezione dei dati si applica a tutti i trattamenti di dati personali, in particolare alla raccolta, alla registrazione, alla conservazione, all'uso, alla modifica, alla comunicazione, all'archiviazione, alla cancellazione o alla distruzione dei dati. Si applica a tutti i tipi di dati personali, compresi quelli relativi a dipendenti, clienti, fornitori e altri partner commerciali.
- 3.2. La direttiva sulla protezione dei dati descrive, specifica o integra anche le disposizioni legali, in particolare quelle della legge svizzera sulla protezione dei dati (LPD).

4. Definizioni

- 4.1. **Per dati personali** ai sensi delle presenti linee guida aziendali si intendono tutte le informazioni relative a una persona fisica identificata o identificabile.
- 4.2. **Gli interessati sono le persone** fisiche i cui dati personali sono trattati.
- 4.3. **Il responsabile del trattamento** è una persona fisica che, da sola o insieme ad altri, decide le finalità e i mezzi del trattamento.
- 4.4. **L'incaricato del trattamento** è un terzo che tratta i dati personali per conto del responsabile del trattamento.



Regole di base per l'elaborazione dei dati

5. La legalità

5.1 I dati personali devono essere trattati in modo lecito. Il trattamento è considerato lecito solo se è giustificato da (a) il consenso dell'interessato, (b) un interesse pubblico o privato prevalente o (c) la legge.

6. Trasparenza

6.1 In linea di principio, i dati devono essere trattati in modo tale che la persona interessata ne sia consapevole.

7. Principio di proporzionalità

7.1 Nel trattamento dei dati deve essere rispettato il principio di proporzionalità. In base a tale principio, possono essere raccolti solo i dati necessari e adeguati allo scopo perseguito.

7.2 Inoltre, i dati personali possono essere conservati solo per il tempo necessario a raggiungere lo scopo previsto (vedi sotto).

8. Scopo

8.1 I dati personali possono essere raccolti solo per una finalità specifica identificabile dall'interessato e possono essere trattati solo in modo compatibile con tale finalità.

8.2 Se i dati personali non sono più necessari ai fini del trattamento, devono essere distrutti o resi anonimi.

9. Precisione

9.1 Tutti i dipendenti devono garantire che i loro dati personali siano accurati e aggiornati.

9.2 Devono essere adottate tutte le misure ragionevoli per rettificare o distruggere i dati inaccurati o incompleti.

10. Sicurezza dei dati

10.1 Per l'azienda è molto importante che la sicurezza dei dati sia garantita in ogni momento. In questo contesto, i dati personali devono essere protetti da misure tecniche e organizzative, in particolare contro la perdita, l'accesso non autorizzato e altri pericoli.

10.2 Le misure di protezione specifiche devono essere documentate per le varie operazioni di trattamento dei dati e la loro adeguatezza deve essere verificata.

10.3 Il reparto IT può emanare direttive più severe nell'interesse della sicurezza dei dati, in particolare per quanto riguarda l'utilizzo dei sistemi informatici all'interno dell'azienda.

11. Consenso e obiezione

11.1 In linea di principio non è necessario il consenso dell'interessato al trattamento dei dati da parte di un'azienda, nemmeno per i dati personali sensibili.



11.2 D'altra parte, se l'interessato si oppone espressamente al trattamento dei dati, questo è giustificato solo se vi sono interessi prevalenti da parte del titolare del trattamento o una base giuridica.

12. Obbligo di informazione

12.1 Le persone interessate devono, per quanto possibile, essere informate in anticipo delle finalità per cui i dati personali che le riguardano vengono raccolti e trattati. Se i dati non vengono raccolti direttamente dall'interessato, quest'ultimo deve essere informato entro un mese dal ricevimento dei dati.

12.2 Se l'interessato rende accessibili al responsabile del trattamento i propri dati personali di propria iniziativa, si ritiene che sia stato informato.

12.3 Se lo scopo del trattamento dei dati cambia, le persone già informate devono essere nuovamente informate.

13. Subappalto

13.1 Quando i fornitori di servizi dell'azienda trattano i dati personali per suo conto (detti subappaltatori), occorre notare che gli stessi obblighi di diligenza che si applicano all'azienda responsabile si applicano anche al subappaltatore. In particolare, la limitazione delle finalità e la sicurezza dei dati devono essere garantite per contratto.

14. Trasferimento di dati personali all'estero :

14.1 La trasmissione di dati personali all'estero è consentita solo nei Paesi in cui il Consiglio federale ha stabilito che il livello di protezione dei dati è pari a quello svizzero. Il rispetto degli standard svizzeri di protezione dei dati può essere ottenuto, tra l'altro, anche attraverso la stipula di accordi contrattuali aggiuntivi.

Processi interni

15. Requisiti per i dipendenti

15.1 Tutti i dipendenti dell'azienda sono tenuti a rispettare la protezione dei dati. In particolare, sono informati che è vietato utilizzare i dati personali per scopi privati, trasmetterli a persone non autorizzate o renderli accessibili a persone non autorizzate. L'obbligo di rispettare la riservatezza si estende oltre la fine del contratto.

15.2 Anche all'interno dell'azienda, si deve fare attenzione a garantire che solo i dipendenti che hanno bisogno di accedere ai dati personali per svolgere le loro mansioni per l'azienda abbiano accesso ad essi.

15.3 Tutti i dipendenti devono essere formati e sensibilizzati sulle questioni relative alla protezione dei dati non appena vengono assunti e in seguito regolarmente.

16. Registro delle attività di trattamento

16.1 L'azienda deve tenere un registro delle attività di trattamento dei dati personali. Devono essere registrati: l'identità del responsabile del trattamento o dell'incaricato del trattamento, lo scopo del



trattamento, una descrizione delle categorie di soggetti e delle categorie di dati personali trattati, le categorie di destinatari, il periodo di conservazione o i criteri per determinarlo, se possibile una descrizione delle misure adottate per garantire la sicurezza dei dati e gli eventuali Paesi di destinazione se i dati sono inviati all'estero. Il registro deve essere sempre aggiornato e fornire una panoramica delle attività di protezione dei dati dell'azienda.

17. Protezione dei dati per progettazione, protezione dei dati per impostazione predefinita e valutazione dell'impatto sulla privacy

17.1 I sistemi utilizzati per il trattamento dei dati personali devono essere progettati fin dall'inizio in modo da rispettare la protezione dei dati. In particolare, le misure tecniche e organizzative devono essere adeguate allo stato dell'arte, alla natura e all'entità del trattamento dei dati e al rischio che il trattamento comporta per la personalità o i diritti fondamentali delle persone interessate (Privacy by Design).

17.2 I responsabili del trattamento dei dati devono scegliere le impostazioni predefinite del dispositivo o del software in modo che il trattamento dei dati personali sia limitato al minimo necessario per l'uso previsto, a meno che l'interessato non decida diversamente. Ciò vale, ad esempio, per l'accettazione dei cookie sul sito web.

17.3 Deve essere effettuata e documentata una valutazione d'impatto sulla protezione dei dati (DPIA), in particolare quando un'operazione di trattamento dei dati pianificata presenta un rischio elevato per la personalità e i diritti fondamentali degli interessati.

Diritti delle persone interessate

18. Diritto di accesso

18.1 Su richiesta, l'interessato deve essere informato se i dati personali che lo riguardano sono trattati dall'azienda. In tal caso, l'interessato ha il diritto di accedere ai dati personali in questione. Il diritto di accesso consiste nel sapere se i dati personali vengono trattati e, in caso affermativo, quali dati, in modo che l'interessato possa far valere i suoi altri diritti. Oltre ai dati personali trattati in quanto tali, ciò include informazioni sull'identità del titolare del trattamento, sulle finalità del trattamento, sul periodo di conservazione, sull'origine dei dati e, se del caso, informazioni sulle decisioni individuali automatizzate e sui destinatari (anche come categorie).

18.2 Nel fornire informazioni, è necessario assicurarsi che l'identità dell'interessato sia verificata. Si deve inoltre garantire che nel corso della fornitura di informazioni non vengano divulgati dati personali di terzi. Di norma, le informazioni devono essere fornite gratuitamente ed entro 30 giorni.

19. Portabilità dei dati / diritto alla comunicazione e alla trasmissione dei dati

19.1 Gli interessati possono richiedere il recupero dei dati che hanno fornito a un'azienda in un formato elettronico corrente, qualora i dati siano trattati con mezzi automatizzati e l'interessato abbia dato il proprio consenso al trattamento o il trattamento sia effettuato nel contesto di un contratto corrispondente.

20. Diritto di rettifica



20.1 Ai sensi dell'art. 32 cpv. 1 LPD, una persona interessata può richiedere la rettifica di dati personali inesatti.

21. Diritto alla cancellazione dei dati

21.1 Qualora i dati personali siano trattati in contrasto con l'espressa dichiarazione di volontà dell'interessato e non vi siano basi giuridiche o interessi privati prevalenti di terzi, l'interessato può richiedere la cancellazione dei propri dati personali.

Competenza

22. Responsabilità

22.1 La responsabilità dell'osservanza delle disposizioni della presente Direttiva sulla protezione dei dati spetta in primo luogo ai dipendenti responsabili del trattamento dei dati.

22.2 Tutti i dipendenti della Società devono garantire l'osservanza delle presenti Linee guida sulla protezione dei dati, contribuendo in tal modo alla definizione di standard uniformi ed elevati di protezione dei dati in tutta la Società.

22.3 In caso di violazione degli obblighi legali in materia di protezione dei dati, i trasgressori saranno esposti a conseguenze penali (multa fino a 250.000 franchi svizzeri) e l'azienda a conseguenze civili (che possono includere il risarcimento dei danni), nonché a danni alla sua reputazione. La responsabilità penale ricade in primo luogo sull'individuo, ossia sul dipendente colpevole. Le violazioni della protezione dei dati possono avere anche conseguenze disciplinari all'interno dell'azienda.

23. Segnalazione di violazioni e collaborazione con le autorità di vigilanza

23.1 I dipendenti devono riferire immediatamente al proprio responsabile o al Responsabile della protezione dei dati se vengono a conoscenza di una violazione della presente Politica di protezione dei dati o di qualsiasi disposizione di legge relativa alla protezione dei dati personali.

23.2 Le violazioni della sicurezza dei dati (ad es. divulgazione a persone non autorizzate, perdita di dati, attacchi informatici, ecc.) che comportano un rischio elevato per la personalità o i diritti fondamentali degli interessati devono essere segnalate dall'azienda all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) "il più presto possibile", ossia tempestivamente.

Altre disposizioni

24. Pubblicazione

24.1 La presente politica aziendale deve essere resa disponibile a tutti i dipendenti dell'azienda con mezzi adeguati (in particolare attraverso la rete Intranet).

24.2 Non è prevista la pubblicazione generale della presente direttiva sulla protezione dei dati.

25. Modifiche



- 25.1 L'azienda si riserva il diritto di modificare la presente politica di protezione dei dati se necessario. Le modifiche possono essere necessarie, in particolare, per conformarsi ai requisiti di legge, alle richieste delle autorità di vigilanza o alle procedure interne dell'azienda.
- 25.2 La misura in cui i cambiamenti tecnologici rendono necessario l'adeguamento di questa direttiva aziendale dovrebbe essere rivista a intervalli regolari.