Osservazione introduttiva
L'esempio di politica di protezione dei dati riportato di seguito si concentra sugli elementi essenziali e fornisce una possibile struttura. È opportuno integrarlo o adattarlo in base alla specifica situazione aziendale. A tal fine, può essere utile consultare uno specialista.

Informativa sulla privacy

I. Generale

1. Introduzione

1.1. I dati disponibili in azienda hanno un grande valore per l'azienda. 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 [In caso di domande sulla protezione dei dati o sul trattamento dei dati personali, è possibile contattare il responsabile della protezione dei dati [nome, indirizzo e-mail/numero di telefono o simili]].
1.4 [...]

2. Obiettivo della direttiva sulla protezione dei dati

2.1 La presente politica di protezione dei dati ha lo scopo di creare standard uniformi per la protezione dei dati all'interno dell'azienda.
2.2 Aderendo agli standard definiti nella presente politica di protezione dei dati, l'azienda rispetta gli obblighi previsti dalla legge sulla protezione dei dati e garantisce che gli interessi e i diritti degli interessati siano tenuti in sufficiente considerazione.
2.3 L'osservanza della presente informativa sulla privacy è un prerequisito per lo scambio sicuro di dati personali all'interno dell'azienda e con terzi.
2.4 [...]

3. Ambito di applicazione della direttiva sulla protezione dei dati

3.1 La presente Informativa sulla privacy si applica a tutti i trattamenti di dati personali, compresi, a titolo esemplificativo, l'ottenimento, l'archiviazione, la conservazione, l'utilizzo, la modifica, la divulgazione, l'archiviazione, la cancellazione o la distruzione dei dati. Si applica a tutti i tipi di dati personali, in particolare a quelli di dipendenti, clienti, fornitori e altri partner commerciali.
3.2 Le linee guida per la protezione dei dati descrivono, motivano e integrano anche i requisiti legali, in particolare quelli della legge svizzera sulla protezione dei dati (LPD).
3.3 [...]

4. Definizioni

4.1 Ai fini della presente direttiva aziendale, per **dato personale** si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile.
4.2 **Gli interessati** sono le persone fisiche sulle quali vengono trattati i dati personali.
4.3 **Il titolare del trattamento** è un soggetto privato che, da solo o insieme ad altri, decide le finalità e i mezzi del trattamento.
4.4 **Un incaricato del trattamento** è un terzo che tratta i dati personali per conto del responsabile del trattamento.
[...]

II. Regole di base del trattamento 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, da (b) un interesse pubblico o privato prevalente o da (c) la legge.

6. Trasparenza

6.1 In linea di principio, il trattamento dei dati deve essere effettuato in modo che l'interessato ne sia consapevole.

7. Proporzionalità

7.1 Nel trattamento dei dati personali deve essere rispettato il principio di proporzionalità. In base a questo principio, possono essere raccolti solo i dati *necessari* e *appropriati per* lo scopo corrispondente.

7.2 Inoltre, i dati personali possono essere conservati solo per il tempo necessario allo scopo (cfr. sotto).

8. Stanziamento di fondi

8.1 I dati personali possono essere ottenuti solo per uno scopo specifico e identificabile per l'interessato e possono essere trattati solo in modo compatibile con tale scopo.

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

9. Correttezza

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

9.2 Devono essere adottate tutte le misure ragionevoli per correggere o distruggere i dati inesatti o incompleti.

10. Sicurezza dei dati

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

10.2 Per le singole operazioni di trattamento dei dati, le misure di protezione concrete devono essere documentate e controllate per verificarne l'adeguatezza.

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

11. Consenso e obiezione

11.1 Il consenso dell'interessato al trattamento dei dati da parte di un'azienda non è generalmente richiesto, nemmeno nel caso di dati personali particolarmente sensibili.

11.2 Se, invece, l'interessato si oppone espressamente al trattamento dei dati, questo sarà giustificato solo se esistono interessi prevalenti del titolare del trattamento o una base giuridica.

12. Obbligo di informazione

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

12.2 Se l'interessato mette di sua iniziativa i propri dati personali a disposizione del titolare del trattamento, 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. Elaborazione degli ordini

13.1 Se i fornitori di servizi dell'azienda trattano i dati personali per suo conto (i cosiddetti incaricati del trattamento degli ordini), si noti che gli stessi requisiti di diligenza previsti per l'azienda responsabile si applicano anche all'incaricato del trattamento degli ordini. In particolare, la limitazione delle finalità e la sicurezza dei dati devono essere garantite contrattualmente.

14. Trasferimento di dati personali all'estero

14.1 Il trasferimento di dati personali all'estero è consentito solo nei Paesi in cui il Consiglio federale ha stabilito che esiste un livello di protezione dei dati altrettanto elevato come in Svizzera. Il rispetto dello standard svizzero di protezione dei dati può essere ottenuto, tra l'altro, anche attraverso la stipula di accordi contrattuali aggiuntivi.

III. Processi interni

15. Requisiti per i dipendenti

15.1 Tutti i dipendenti dell'azienda sono impegnati nella protezione dei dati. In particolare, devono essere 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 mantenere la riservatezza vale anche dopo la fine del rapporto di lavoro.

15.2 Anche all'interno dell'azienda, occorre assicurarsi che solo i dipendenti abbiano accesso ai dati personali di cui hanno bisogno per svolgere le loro mansioni per l'azienda.

15.3 Tutti i dipendenti devono essere formati e sensibilizzati sui temi della protezione dei dati all'inizio del loro rapporto di lavoro e successivamente su base regolare.

16. Elenco delle attività di trattamento

16.1 L'azienda deve tenere un registro delle attività di trattamento dei dati personali. Tale registro deve contenere le seguenti informazioni: l'identità del titolare o del responsabile 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 determinare il periodo di conservazione, una descrizione delle misure di sicurezza dei dati, se possibile, e gli eventuali paesi di destinazione se i dati sono trasferiti all'estero. L'elenco deve essere sempre aggiornato e fornire una panoramica delle attività rilevanti per la protezione dei dati nell'azienda.

17. Protezione dei dati attraverso la tecnologia, le impostazioni predefinite favorevoli alla protezione dei dati e la valutazione dell'impatto sulla protezione dei dati.

17.1 I sistemi utilizzati per il trattamento dei dati personali devono essere progettati fin dall'inizio in modo tale da poter rispettare la protezione dei dati. In particolare, le misure tecniche e organizzative devono essere adeguate allo stato dell'arte, al tipo e alla portata del trattamento dei dati e al rischio che il trattamento comporta per la personalità o i diritti fondamentali degli interessati (privacy by design).

17.2 Il titolare del trattamento deve selezionare le impostazioni predefinite del dispositivo o del software in modo tale che il trattamento dei dati personali sia limitato al minimo necessario per lo scopo previsto, a meno che l'interessato non specifichi 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, in particolare se un trattamento dei dati previsto comporta un rischio elevato per la personalità e i diritti fondamentali delle persone interessate.

17.4 [...]

IV. Diritti degli interessati

18. Diritto all'informazione

18.1 Su richiesta, l'interessato viene informato se l'azienda sta trattando dati personali che lo riguardano. In tal caso, l'interessato ha il diritto di ricevere informazioni sui dati personali in questione. Il diritto all'informazione 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 ulteriori diritti. Oltre ai dati personali trattati in quanto tali, ciò include informazioni sull'identità del responsabile, 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 Quando si forniscono informazioni, si deve garantire che l'identità della persona interessata 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 al rilascio e al trasferimento dei dati

19.1 Gli interessati possono chiedere che i loro dati che hanno comunicato all'azienda vengano restituiti in un formato elettronico di uso comune se i dati sono trattati con mezzi automatizzati e l'interessato ha acconsentito al trattamento o il trattamento è effettuato in base a un contratto pertinente.

20. Diritto di rettifica

20.1 L'interessato può chiedere la rettifica di dati personali inesatti ai sensi dell'art. 32 capoverso 1 LPD.

21. Diritto alla cancellazione dei dati

21.1 Se i dati personali sono trattati in contrasto con l'espressa dichiarazione di intenti dell'interessato e non esiste una base giuridica né un interesse privato prevalente di terzi, l'interessato può richiedere la cancellazione dei propri dati personali.
[...]

V. Competenza

22. Responsabilità

22.1 I dipendenti incaricati del trattamento dei dati sono i principali responsabili dell'osservanza delle disposizioni della presente politica di protezione dei dati.

22.2 Tutti i dipendenti dell'azienda dovranno garantire l'osservanza della presente informativa sulla privacy, contribuendo in tal modo alla definizione di standard costantemente elevati di protezione dei dati in tutta l'azienda.

22.3 In caso di violazione degli obblighi legali previsti dalla legge sulla protezione dei dati, i trasgressori sono passibili di sanzioni penali (multe fino a 250.000 franchi svizzeri) e l'azienda di sanzioni civili (fino al risarcimento dei danni), nonché di danni alla reputazione. La persona fisica è la principale responsabile ai sensi del diritto penale, ossia il dipendente che commette intenzionalmente un reato. Le violazioni della protezione dei dati possono avere anche conseguenze disciplinari interne.

22.4 [...]

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

23.1 I dipendenti devono riferire immediatamente al supervisore o al responsabile della protezione dei dati, a dipendenza dei casi, se vengono a conoscenza di qualsiasi 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, attacco informatico, ecc.) che comportano un rischio elevato per la personalità o i diritti fondamentali degli interessati devono essere segnalate dall'azienda all'IFPDT "il più presto possibile", ossia tempestivamente.

23.3 [...]

VI. Ulteriori disposizioni

24. Pubblicità

24.1 La presente politica aziendale deve essere resa disponibile a tutti i dipendenti dell'azienda in modo appropriato, [in particolare attraverso l'intranet].

24.2 La pubblicazione generale della presente informativa sulla privacy non è prevista.

25. Modifiche

25.1 L'azienda si riserva il diritto di modificare la presente informativa sulla privacy secondo le necessità. In particolare, una modifica può essere necessaria per conformarsi ai requisiti legali, ai requisiti delle autorità di vigilanza o alle procedure aziendali interne.

25.2 La misura in cui i cambiamenti tecnologici richiedono un adeguamento della presente politica aziendale sarà inoltre riesaminata a intervalli regolari.

26. [...]