*Osservazione introduttiva*

*Il modello delle linee guida sulla protezione dei dati riportate di seguito si concentra sugli elementi essenziali e mostra una possibile struttura. È opportuno integrarlo o adattarlo in base alla situazione specifica dell’impresa. A questo scopo può essere utile consultare uno specialista.*

*\* \* \* \* \**

Linee guida sulla protezione dei dati

1. Informazioni generali
2. Introduzione
	1. I dati disponibili all’interno dell’impresa sono di grande valore per la stessa. Questi dati devono quindi essere protetti dall’accesso non autorizzato e da altre minacce.

1.2 I clienti, i partner e i collaboratori dell’impresa si aspettano che i dati affidati alla stessa siano scrupolosamente protetti e trattati con cura.

1.3 [In caso di domande sulla protezione dei dati o sul trattamento dei dati personali, è possibile contattare l’incaricato della protezione dei dati [nome e cognome, indirizzo e-mail/numero di telefono o simili.]

1.4 […]

2. Scopo delle linee guida sulla protezione dei dati

2.1 Le presenti linee guida sulla protezione dei dati hanno lo scopo di creare standard uniformi per la protezione dei dati all’interno dell’impresa.

2.2 Rispettando gli standard definiti nelle presenti linee guida sulla protezione dei dati, l’impresa adempie agli obblighi previsti dalla legge sulla protezione dei dati e garantisce che gli interessi e i diritti delle persone interessate siano adeguatamente presi in considerazione.

2.3 L’osservanza delle presenti linee guida sulla protezione dei dati è un prerequisito per lo scambio sicuro di dati personali all’interno dell’impresa e con terzi.

2.4 […]

3. Ambito di applicazione delle linee guida sulla protezione dei dati

3.1 Le presenti linee guida sulla protezione dei dati si applicano a qualsiasi trattamento di dati personali, in particolare all’acquisizione, alla memorizzazione, alla conservazione, all’utilizzo, alla modifica, alla divulgazione, all’archiviazione, alla cancellazione o alla distruzione dei dati. Si applica a tutti i tipi di dati personali, in particolare a quelli di collaboratori, clienti, fornitori e altri partner commerciali.

3.2 Le linee guida sulla protezione dei dati descrivono, motivano e completano anche i requisiti legali, in particolare quelli della legge svizzera sulla protezione dei dati (LPD).

3.3 […]

4. Definizioni

4.1 Ai fini delle presenti linee guida aziendali, per dati personali si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile.

4.2 Le persone interessate sono le persone fisiche i cui dati personali sono trattati.

4.3 Il titolare del trattamento è una persona privata che, da sola o insieme ad altre, decide le finalità e i mezzi del trattamento.

4.4 Il responsabile 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. Liceità

5.1 I dati personali devono essere trattati in modo lecito. Il trattamento è considerato lecito solo se giustificato (a) dal consenso della persona interessata, (b) da un interesse pubblico o privato preponderante o (c) dalla legge.

6. Trasparenza

6.1 In linea di principio, il trattamento dei dati deve avvenire in modo tale che la persona interessata 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 la finalità corrispondente.

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

8. Finalità

8.1 I dati personali possono essere ottenuti solo per una finalità specifica che sia evidente alla persona interessata 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. Esattezza

9.1 Tutti i collaboratori sono tenuti a garantire che i dati personali siano esatti 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’impresa è cruciale garantire la sicurezza dei dati in qualsiasi momento. In questo contesto, i dati personali devono essere protetti, tra l’altro, mediante misure tecniche e organizzative contro la perdita, l’accesso non autorizzato e altre minacce.

10.2 Le misure di protezione specifiche per le singole operazioni di trattamento dei dati devono essere documentate e controllate per verificarne l’adeguatezza.

10.3 Il dipartimento IT può stabilire requisiti più ampi nell’interesse della sicurezza dei dati, in particolare per quanto riguarda l’utilizzo dei sistemi informatici in azienda.

11. Consenso e opposizione

11.1 Il consenso della persona interessata al trattamento dei dati da parte di un’impresa non è richiesto in linea di principio, nemmeno nel caso di dati personali che richiedono particolare protezione.

11.2 Se, invece, la persona interessata si oppone espressamente al trattamento dei dati, questo è giustificato solo se sussistono interessi preponderanti del titolare del trattamento o una base legale.

12. Obbligo di informazione

12.1 Se possibile, le persone interessate devono essere informate in anticipo delle finalità per le quali i dati personali che le riguardano vengono raccolti e trattati. Se i dati non sono stati ottenuti direttamente dalla persona interessata, quest’ultima deve essere informata entro un mese dal ricevimento dei dati.

12.2 Se la persona interessata mette di sua iniziativa i propri dati personali a disposizione del titolare del trattamento, si ritiene informata.

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

13. Mandato del trattamento

13.1 Se i fornitori di prestazioni di servizi dell’impresa trattano i dati personali per conto della stessa (i cosiddetti responsabili del trattamento), ai responsabili del trattamento si applicano gli stessi requisiti di diligenza previsti per l’impresa responsabile. In particolare, la finalità e la sicurezza dei dati devono essere garantite contrattualmente.

14. Trasmissione di dati personali all’estero

14.1 La trasmissione di dati personali all’estero è consentita solo nei Paesi per i quali il Consiglio federale ha stabilito un livello di protezione dei dati di livello simile a quello in Svizzera. Per essere conformi allo standard svizzero di protezione dei dati, tra l’altro, è inoltre possibile concludere accordi contrattuali aggiuntivi.

IV. Processi aziendali interni

15. Requisiti per i collaboratori

15.1 Tutti i collaboratori dell’impresa sono impegnati nella protezione dei dati. In particolare, vengono informati del divieto di utilizzare i dati personali per finalità private, trasmetterli 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 collaboratori abbiano accesso ai dati personali di cui necessitano nell’ambito dello svolgimento delle loro mansioni aziendali.

15.3 Tutti i collaboratori devono essere formati e sensibilizzati sui temi della protezione dei dati all’inizio del rapporto di lavoro e in seguito regolarmente.

16. Registro delle attività di trattamento

16.1 L’impresa è tenuta a stilare un registro delle attività di trattamento dei dati personali che deve includere: l’identità del titolare o del responsabile del trattamento, la finalità del trattamento, la descrizione delle categorie di persone interessate, dei dati personali trattati e dei destinatari, il periodo di conservazione o i criteri per determinarlo, se possibile, la descrizione delle misure di sicurezza dei dati ed eventuali Paesi di destinazione se i dati devono essere trasferiti all’estero. Il registro deve essere sempre aggiornato e fornire una panoramica delle attività rilevanti per la protezione dei dati nell’impresa.

17. La protezione dei dati grazie alla tecnologia, le impostazioni predefinite che favoriscono la 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 sin dall’inizio in modo da garantire la protezione dei dati. Le misure tecniche e organizzative devono, in particolare, 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 delle persone interessate (privacy by design).

17.2 I titolari del trattamento selezionano le impostazioni standard del dispositivo o del software in modo tale che il trattamento dei dati personali sia limitato al minimo necessario per la finalità prevista, salvo diversamente specificato dalla persona interessata. Ciò riguarda, ad esempio, l’accettazione dei cookie sul sito web.

17.3 In particolare, se un trattamento dei dati previsto comporta un rischio elevato per la personalità e i diritti fondamentali delle persone interessate, è necessario effettuare e documentare una valutazione d’impatto sulla protezione dei dati (VIPD).

17.4 […]

Diritti delle persone interessate

18. Diritto d’accesso

18.1 Su richiesta, la persona interessata deve essere informata sull’eventuale trattamento di dati personali che la riguardano da parte dell’impresa. In tal caso, la persona interessata ha il diritto di accedere a detti dati personali. Il diritto d’accesso consiste nel sapere se i dati personali vengono trattati e, in caso affermativo, quali dati vengono trattati, in modo che la persona interessata possa far valere i suoi ulteriori 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 l’accesso, è necessario assicurarsi che l’identità della persona interessata sia stata verificata. Inoltre, è necessario garantire che non vengano divulgati dati personali di terzi nell’ambito della fornitura dell’accesso. Di norma, le informazioni sono gratuite e devono essere fornite entro 30 giorni.

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

19.1 Le persone interessate possono chiedere di recuperare i dati che hanno comunicato all’impresa in un formato elettronico di uso comune se i dati sono trattati con mezzi automatizzati e la persona interessata ha acconsentito al trattamento o se il trattamento è effettuato nell’ambito del rispettivo contratto.

20. Diritto di rettifica

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

21. Diritto alla cancellazione dei dati

21.1 Se i dati personali vengono trattati in contrasto con l’espressa dichiarazione di volontà della persona interessata e non sussiste alcuna base legale, né un interesse privato preponderante di terzi, la persona interessata può richiedere la cancellazione dei propri dati personali.

[…]

VI. Competenza

22. Responsabilità

22.1 I collaboratori incaricati del trattamento dei dati sono i principali responsabili dell’osservanza delle disposizioni delle presenti linee guida sulla protezione dei dati.

22.2 Tutti i collaboratori dell’impresa sono tenuti a garantire l’osservanza delle presenti linee guida sulla protezione dei dati e contribuire in tal modo alla definizione di standard di protezione dei dati uniformemente elevati in tutta l’impresa.

22.3 In caso di violazione degli obblighi legali in materia di protezione dei dati, i trasgressori possono essere soggetti a sanzioni penali (multe fino a CHF 250 000) e l’impresa può essere soggetta a sanzioni civili (fino al risarcimento dei danni) e a danni all’immagine. Il responsabile penale è innanzitutto la persona fisica, ossia il collaboratore che commette l’infrazione intenzionalmente. Le violazioni della protezione dei dati possono avere anche conseguenze disciplinari interne.

22.4 […]

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

23.1 Qualora ne vengano a conoscenza, i collaboratori sono tenuti a riferire immediatamente al supervisore o all’incaricato della protezione dei dati, a seconda dei casi, qualsiasi violazione delle presenti linee guida sulla protezione dei dati o di qualsiasi disposizione di legge relativa alla protezione dei dati personali.

23.2 Le violazioni della *sicurezza* dei dati (ad esempio divulgazione a persone non autorizzate, perdita di dati, attacco informatico, ecc.) che comportano un rischio elevato per la personalità o i diritti fondamentali delle persone interessate devono essere notificate dall’impresa all’IFPDT «il più presto possibile», ossia tempestivamente.

23.3 […]

VII. Ulteriori disposizioni

24. Informazione

24.1 Le presenti linee guida aziendali devono essere rese disponibili a tutti i collaboratori dell’azienda in maniera consona, [in particolare attraverso l’intranet].

24.2 Non è prevista la pubblicazione generale delle presenti linee guida sulla protezione dei dati.

25. Modifiche

25.1 L’impresa si riserva il diritto di modificare le presenti linee guida sulla protezione dei dati, se del caso. Una modifica può essere necessaria, in particolare, per conformarsi a requisiti legali, a requisiti delle autorità di vigilanza o a procedure aziendali interne.

25.2 A intervalli regolari, verrà inoltre verificato in che misura i cambiamenti tecnologici richiedano un adeguamento delle presenti linee guida aziendali.

26. […]