Scheda informativa

La nuova legge sulla protezione dei dati dal 1° settembre 2023 – Gli aspetti salienti da considerare per le imprese artigianali

1. Situazione iniziale e panoramica

Con la nuova legge sulla protezione dei dati (LPD), che è stata adottata il 25 settembre 2020 dopo un'intensa consultazione del Consiglio nazionale e del Consiglio degli Stati ed entrerà in vigore il 1° settembre 2023 dopo un periodo di attuazione prolungato, la pressione e l'impegno per la conformità alla protezione dei dati aumentano notevolmente anche per le imprese artigianali. A ciò contribuisce la crescente consapevolezza della protezione dei dati. Con lo sviluppo digitale, la protezione della personalità e l'autodeterminazione informativa acquistano sempre più importanza in ampie categorie della popolazione.

Il Consiglio federale completa la LPD con l'ordinanza sulla protezione dei dati (OPDa) e l'ordinanza sulle certificazioni in materia di protezione dei dati (OCPD), entrambe del 31 agosto 2022.

È probabile che le imprese più grandi e quelle che hanno un legame con l'UE abbiano già ampliato la propria protezione dei dati con l'entrata in vigore del Regolamento europeo sulla protezione dei dati (GDPR). Questo perché il GDPR si applica anche a molte imprese svizzere (si veda la scheda informativa del 16 marzo 2018). La nuova LPD non è un'attuazione completa del GDPR. Tuttavia, molti regolamenti sono stati adottati in linea di principio per raggiungere un livello comparabile di protezione dei dati, il che facilita il traffico transfrontaliero di dati. Inoltre, la revisione della LPD consente anche la ratifica dell'estensione del la Convenzione europea 108 sulla protezione dei dati.

A livello territoriale, come nel caso del GDPR, si applica il principio degli effetti. La LPD si applica pertanto anche a tutte le circostanze che si verificano all'estero ma che hanno un effetto sulla protezione dei dati in Svizzera.

In linea di principio, il principio dell'applicazione delle norme in base al rischio si applica come prima. Quanto più i dati o un'operazione di trattamento sono sensibili in termini di lesione della personalità delle persone interessate, tanto più devono essere adottate precauzioni per garantire che la violazione non si verifichi. Questo per assicurare che la protezione dei dati sia già inclusa nella fase di pianificazione dei progetti digitali. Al contrario, le imprese (secondo la denominazione LPD «i titolari del trattamento») o gli organi di gestione responsabili devono anche chiedersi, nell'ambito della gestione del rischio, fino a che punto sono disposti ad accettare *consapevolmente* i rischi residui. È indiscutibile che la protezione dei dati, insieme alla sicurezza delle informazioni, stia diventando sempre più una questione strategica che rientra nell'agenda della direzione aziendale e del consiglio di amministrazione.

La legge sulla protezione dei dati interessa solo i dati relativi a una persona fisica identificata o identificabile, i cosiddetti dati personali. Tuttavia, come nel GDPR, la protezione dei dati sarà ora limitata ai dati delle persone *fisiche*. La protezione precedentemente esistente per le persone *giuridiche* non si applica più. Questo facilita le attività commerciali B2B. Tuttavia, la protezione delle persone giuridiche rimane come da art. 28 CC (protezione della personalità) o da art. 162 CP (segreto commerciale e di fabbricazione), nonché dalle disposizioni pertinenti della legge sui cartelli (LCart) e della legge contro la concorrenza sleale (LCSl). I dati personali delle imprese individuali sono comunque protetti dalla LPD. Anche i dati aziendali non personali devono essere adeguatamente protetti dalle imprese. La protezione dei dati e la sicurezza delle informazioni vanno quindi di pari passo e dovrebbero essere affrontate insieme, se non altro per ragioni di efficienza.

I dati personali *che richiedono particolare protezione*, il cui trattamento è soggetto a requisiti legali più elevati (ad esempio, il consenso deve essere dato *in modo esplicito*), hanno finora incluso le opinioni o le attività religiose, ideologiche, politiche o sindacali, la salute, la sfera privata e l'appartenenza a una razza, nonché le misure di assistenza sociale e i procedimenti e le sanzioni amministrative e penali.

A questi si aggiungono ora i dati genetici e biometrici. Inoltre, le conseguenze e i requisiti legali particolari non sono più legati alla fattispecie «profilo della personalità», bensì alla «profilazione» o al «rischio elevato», che riguarda il processo di trattamento automatizzato (valutazione dei profili della personalità). Tuttavia, alla luce dell'acceso dibattito parlamentare che ha accompagnato questo sviluppo, i cambiamenti pratici in questo senso sono marginali.

In pratica, si raccomanda alle imprese di redigere linee guida interne sulla protezione dei dati (può bastare un semplice insieme di regole), anche se non sono obbligatorie ai sensi della legge sulla protezione dei dati, una chiara regolamentazione delle responsabilità e della formazione e sensibilizzazione dei collaboratori. Oltre alle garanzie contrattuali (ad esempio nei confronti dei responsabili del trattamento), è importante documentare adeguatamente la protezione dei dati e la sicurezza delle informazioni, soprattutto per poter dimostrare la conformità in caso di incidente. Naturalmente, devono essere definiti anche i processi necessari all'interno dell'azienda e nei confronti di terzi (autorità di vigilanza, persone interessate, ecc.) per poter reagire efficacemente se necessario.

Di seguito, il numero 2 descrive in modo più dettagliato le regole essenziali per le imprese artigianali nell'ambito del trattamento dei dati personali e il numero 3 descrive i diritti delle persone interessate che devono essere rispettati. Nel numero 4 vengono delineate le conseguenze delle violazioni della protezione dei dati per la gestione del rischio. I riferimenti all'articolo (art.) e al capoverso (cpv.) si riferiscono alla nuova LPD.

2. Quali sono le regole che le imprese interessate sono tenute a prendere in considerazione quando trattano i dati personali?

Nell'ambito del trattamento dei dati personali, le imprese artigianali sono tenute a osservare le seguenti regole. Va notato che la legge si basa su un concetto globale di trattamento dei dati, che interessa praticamente tutti i trattamenti dei dati personali, dalla raccolta alla cancellazione.

- **Principio di liceità:** i dati personali devono essere trattati in modo lecito (art. 6 cpv. 1 LPD), ossia il trattamento è generalmente consentito a condizione che non venga effettuato violando una norma giuridica.

- **Principio di trasparenza:** deriva dal principio che il trattamento dei dati deve essere effettuato in buona fede (art. 6 cpv. 2 LPD). La raccolta e il trattamento dei dati devono sempre avvenire in modo che la persona interessata ne sia consapevole. In caso contrario, la persona interessata non può far valere i propri diritti.

- **Principio di proporzionalità:** in base a questo principio, possono essere raccolti solo i dati *necessari* e *appropriati* per la finalità corrispondente (art. 6 cpv. 2 LPD). Il principio di proporzionalità prevede anche che i dati possano essere conservati solo per il *tempo necessario* alla finalità.

- **Principio di finalità:** conformemente a tale principio, i dati 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 (art. 6 cpv. 3 LPD). I dati devono essere distrutti o resi anonimi non appena non sono più necessari alle finalità del trattamento (art. 6, cpv. 4 LPD).

- **Principio di esattezza:** chiunque tratti dati personali deve garantirne l'*esattezza* (art. 6 cpv. 4 LPD). Pertanto, adotterà tutte le misure ragionevoli per garantire che i dati inesatti o incompleti rispetto alle finalità per cui sono stati ottenuti o trattati siano rettificati o distrutti.

- **Principio di sicurezza dei dati:** richiede la protezione dei dati mediante *misure tecniche* e *organizzative* (art. 8 LPD), volte a garantire i vari obiettivi di protezione della *riservatezza*, della *disponibilità* e dell'*integrità* dei dati, nonché la *tracciabilità* del trattamento dei dati. Anche in questo caso si applica la proporzionalità e le misure devono corrispondere allo stato dell'arte. Quanto più sensibili

sono i dati, tanto più elevati sono i requisiti di sicurezza degli stessi. Poiché l'uomo è sempre l'anello debole della sicurezza dei dati, le misure organizzative, oltre a quelle tecniche, sono di grande importanza. Misure concrete possono essere: restrizioni dell'accesso, crittografia dei dati, registrazione, backup, tecniche di smaltimento sicure, controlli degli accessi e degli ingressi, regolamenti e direttive, formazione e sensibilizzazione, contratti per il trattamento dei dati e la riservatezza nonché controlli e miglioramenti periodici. Il principio della sicurezza dei dati è ulteriormente illustrato dal Consiglio federale nell'OPDa (artt. 1-6).

- **Protezione dei dati mediante la tecnologia (la cosiddetta privacy by design, art. 7 cpv. 1 e 2 LPD):** 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.

- **Impostazioni predefinite che favoriscono la protezione dei dati** (la cosiddetta privacy by default, art. 7 cpv. 3 LPD)**:** 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. In pratica, questa regola si applica in particolare all'accettazione dei cosiddetti cookie su Internet. Se si accettano le impostazioni predefinite, possono essere impostati solo i cookie strettamente necessari al servizio. Tuttavia, la persona interessata può accettare altri cookie nelle impostazioni del sito web.

- **Consenso e opposizione:** 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. Si presume invece una lesione della personalità ai sensi dell'art. 30 LPD qualora la persona interessata si opponga espressamente al trattamento dei dati. In questo caso, la lesione della personalità può essere giustificata solo da una base legale o dagli interessi preponderanti del titolare del trattamento ai sensi dell'art. 31 LPD (si veda anche la regola sulla lesione della personalità di seguito).

- **Obbligo di informazione:** l'estensione dell'obbligo di informazione ai sensi dell'art. 19 e segg. LPD è un aspetto importante nell'ambito del principio di trasparenza. La persona interessata deve sapere quali dati che la riguardano vengono raccolti e trattati e per quale finalità. In linea di principio, questo deve essere fatto *prima* di ottenere i dati. Se i dati non sono ottenuti direttamente presso la persona interessata, le informazioni devono essere fornite entro un mese dal ricevimento. Ai sensi dell'art. 13 OPDa, le informazioni devono essere fornite in forma precisa, trasparente, comprensibile e facilmente accessibile. A meno che non sussista un'eccezione motivata legalmente, l'obbligo di informazione si applica a ogni acquisizione programmata di dati personali. I dati personali raccolti solo incidentalmente o per caso sono esenti dall'obbligo di informazione. Sono altresì esenti i dati raccolti mediante acquisizione involontaria o accidentale.

  I clienti esistenti non devono essere informati dell'entrata in vigore della nuova LPD. Inoltre, la persona interessata non deve essere informata su ciò che già conosce. Si considera informata la persona che mette a disposizione del titolare del trattamento i propri dati personali senza l'intervento di quest'ultimo. Allo stesso modo, non è necessario informare circa le modifiche successive. Solo se la finalità dell'utilizzo dei dati cambia, è necessario fornire informazioni in merito. In termini di contenuto, devono essere comunicati l'identità e i dati di contatto del titolare del trattamento, le finalità del trattamento e, se del caso, i destinatari a cui i dati saranno divulgati. Se i dati vengono divulgati all'estero, devono essere indicati i Paesi interessati. L'obbligo di informazione è limitato o annullato da vari altri motivi legali di restrizione ed eccezioni, ad esempio se il trattamento dei dati è previsto dalla legge o se è in conflitto con gli interessi preponderanti di terzi. Se il titolare del trattamento può identificare la persona interessata solo con uno sforzo sproporzionato, non è necessario informarla in caso di raccolta indiretta dei dati. Nel caso specifico, è opportuno consultare le disposizioni di esenzione di cui all'art. 20 LPD. Se il trattamento porta a decisioni individuali automatizzate, i titolari

del trattamento sono tenuti ad adempiere all'ulteriore obbligo di informare la persona interessata e garantirle i diritti di audizione e di revisione (art. 21 LPD). Di norma, le imprese adempiono all'obbligo di informazione con l'informativa sulla privacy sul sito web o nelle condizioni generali. Tuttavia, non sussistono requisiti formali. Qualsiasi ambiguità sarà interpretata a favore della persona interessata o del cliente e a scapito del titolare del trattamento o dell'autore. Il GDPR (art. 12 e segg.) contiene obblighi di informazione che vanno oltre quelli della LPD e sono disciplinati in modo più dettagliato.

- **Trattamento da parte del responsabile del trattamento:** per mandato del trattamento si intende che il titolare del trattamento incarica un terzo (responsabile del trattamento) di eseguire il trattamento dei dati per suo conto. Il titolare del trattamento è tenuto a garantire contrattualmente la finalità e la sicurezza dei dati nei confronti del responsabile del trattamento (art. 9 LPD). Il responsabile del trattamento può trasferire il trattamento a terzi solo previo consenso del titolare del trattamento. La richiesta può essere di carattere generale o specifico (vedere anche art. 7 OPDa). Non è necessario alcun contratto nella misura in cui la legge prevede il mandato del trattamento. Anche in questo caso, tuttavia, è necessario garantire la finalità e la sicurezza dei dati.

- **Divulgazione dei dati all'estero:** Ai sensi dell'art. 16 e segg. LPD i dati personali possono essere comunicati a un destinatario all'estero (anche mediante accesso a un server in Svizzera) solo se il livello di protezione dei dati nel rispettivo Paese è altrettanto elevato che in Svizzera. A tal fine, l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT), successivamente all'entrata in vigore della nuova LPD del Consiglio federale, redige un elenco dei Paesi che, secondo la Svizzera, presentano un livello adeguato di protezione dei dati. Se un Paese terzo non ha un livello di protezione dei dati equivalente a quello della Svizzera, la divulgazione è comunque consentita qualora il titolare del trattamento disciplini contrattualmente con il destinatario estero dei dati l'osservanza degli standard svizzeri di protezione dei dati. Gli accordi più utilizzati nella pratica sono le clausole contrattuali standard della Commissione europea che esistono sia per i responsabili del trattamento che per i titolari del trattamento in qualità di destinatari. Anche l'IFPDT approva e pubblica tali clausole. Il Consiglio federale illustra ulteriormente la divulgazione dei dati all'estero nell'OPDa (artt. 8-12).

- **Registro delle attività di trattamento:** i titolari e i responsabili del trattamento dei dati delle imprese più grandi sono tenuti a redigere un registro di tutte le attività di trattamento dei dati (art. 12 LPD). Le imprese con meno di 250 collaboratori sono esenti, a meno che non trattino dati personali sensibili su larga scala o effettuino profilazione (art. 24 OPDa). Le informazioni richieste per legge devono essere registrate per ogni attività di trattamento. Queste ultime sono: 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. Poiché si tratta di un aspetto fondamentale per la protezione dei dati, è opportuno che anche le imprese più piccole tengano un elenco corrispondente, anche se non sono soggette all'obbligo di legge. Non sussistono requisiti formali, quindi sono sufficienti semplici documenti Word o Excel. Possono essere adottati i registri eventualmente creati in attuazione del GDPR. Le imprese non sono più obbligate a registrare le raccolte di dati, come invece accadeva con la precedente LPD, anche se nella pratica non avveniva quasi mai.

- **Valutazione d'impatto sulla protezione dei dati (VIPD):** se un trattamento dei dati previsto comporta un rischio elevato per la personalità e i diritti fondamentali delle persone interessate, il titolare del trattamento è tenuto a effettuare prima una VIPD (art. 22 LPD). Il rischio elevato deriva dalle tecnologie e dalla natura o dalle circostanze delle operazioni di trattamento dei dati (profilazione ad alto rischio, trattamento di dati che richiedono particolare protezione). L'attenzione non si concentra sulla possibile lesione della personalità, quanto sulla valutazione delle conseguenze del trattamento dei

dati per le persone interessate e sul modo in cui tali conseguenze possono essere prevenute se la probabilità che si verifichino è elevata. Il trattamento dei dati è particolarmente sensibile quando comporta un monitoraggio sistematico o il trattamento di dati personali riservati, o ancora quando comporta decisioni automatizzate che possono influenzare la conclusione di un contratto attraverso l'uso della tecnologia. Il titolare del trattamento dei dati è tenuto a conservare la VIPD per almeno due anni dopo la fine del trattamento dei dati (art. 14 OPDa). Se dopo la VIPD permane un rischio elevato, è necessario ottenere un parere dall'IFPDT. Quest'ultimo può sollevare obiezioni e proporre misure (art. 23 LPD). L'IFPDT può anche richiedere una VIPD. Se è disponibile un certificato o un codice di condotta o se è stato nominato un consulente per la protezione dei dati (vedere più avanti), si può rinunciare a una VIPD. Soprattutto alla luce del principio della privacy by design (protezione dei dati mediante la tecnologia), vale la pena di realizzare almeno una «piccola» VIPD in ogni progetto digitale.

- **Consulente per la protezione dei dati:** le imprese possono nominare volontariamente un consulente per la protezione dei dati (art. 10 LPD). Quest'ultimo può, ma non deve necessariamente avere un rapporto di lavoro con il titolare del trattamento. Oltre alla consulenza e alla formazione generale, il consulente per la protezione dei dati esamina i progetti di trattamento dei dati che presentano ancora un «rischio elevato» nonostante la VIPD sia stata effettuata e le misure siano state definite. Se la verifica viene effettuata dal consulente per la protezione dei dati, non è più necessario consultare l'IFPDT. A tal fine, il consulente per la protezione dei dati deve possedere le competenze adeguate. Allo stesso tempo, non deve essere coinvolto in prima persona nel trattamento dei dati personali in oggetto, in modo da poter mantenere la necessaria indipendenza, come specificato nell'art. 23 OPDa. Soprattutto per le imprese più piccole, è discutibile che questi requisiti rigorosi possano essere giustificati dal (solo) «vantaggio» di non dover consultare l'IFPDT. Le responsabilità per la protezione dei dati e la sicurezza delle informazioni possono e devono essere regolamentate in ogni azienda indipendentemente dalla nomina di un consulente per la protezione dei dati ai sensi dell'art. 10 LPD.

- **Codice di condotta:** le associazioni professionali, settoriali ed economiche possono elaborare i propri codici di condotta e sottoporli all'IFPDT (art. 11 LPD). Non sussiste alcun obbligo di presentare un codice, ma se presentato, l'IFPDT è tenuto a esprimere il proprio parere. I pareri dell'IFPDT sono pubblicati. I codici di condotta disciplinano gli aspetti della protezione dei dati per i membri dell'associazione. Se esiste un codice di condotta di questo tipo, l'obbligo di condurre una VIPD in relazione a questi aspetti non si applica (art. 22 cpv. 5 LPD). Il prerequisito è che il codice di condotta sia basato su una VIPD.

- **Certificazione:** anche se un titolare del trattamento dei dati utilizza un sistema o un programma di trattamento dei dati adeguatamente certificato (art. 13 LPD), ad esso non si applica l'obbligo di condurre una VIPD (art. 22 cpv. 5 LPD). La certificazione è espressione di una data «adeguatezza», ma non significa che in seguito non possano verificarsi violazioni della protezione o della sicurezza dei dati.

- **Lesione della personalità e motivi giustificativi:** chiunque tratti dati personali non deve ledere illecitamente la personalità delle persone interessate (art. 30 LPD). Si verifica una lesione della personalità in particolare (ma non limitatamente) se (a) vengono violati i principi del trattamento dei dati ai sensi degli artt. 6 e 8 LPD, (b) i dati personali vengono trattati in contrasto con l'espressa dichiarazione di volontà della persona interessata o (c) i dati personali che richiedono particolare protezione vengono divulgati a terzi.

  Una lesione della personalità non è illecita, ma ammissibile o «sanata» se esiste uno dei seguenti motivi giustificati (art. 31 cpv. 1 LPD): (a) consenso della persona interessata, (b) interesse pubblico o privato preponderante o (c) base legale.

In pratica, un importante motivo giustificato per le imprese, oltre al consenso, è l'interesse privato preponderante. Questo è ulteriormente illustrato nella legge. L'art. 31 cpv. 2 LPD contiene un catalogo non esaustivo di possibili interessi preponderanti del titolare del trattamento nei seguenti contesti: (a) svolgimento di un rapporto contrattuale, (b) tra persone in concorrenza economica, (c) verifica della solvibilità, (d) pubblicazione sui media, (e) personaggi pubblici e (f) ricerca, pianificazione e statistica.

In questo modo, vengono ulteriormente specificate le giustificazioni per contesto. Una giustificazione spesso invocata è la verifica della solvibilità. In questo ambito, la legge sulla protezione dei dati impone quattro restrizioni: In primo luogo, possono essere trattati solo dati di persone maggiorenni. In secondo luogo, i dati non devono essere più vecchi di dieci anni. Dopo dieci anni, ad esempio, le informazioni sul fallimento di una persona non possono più essere trattate. In terzo luogo, le verifiche della solvibilità non devono basarsi su profili ad alto rischio o su dati che richiedono particolare protezione. In quarto luogo, i dati sulla solvibilità possono essere comunicati a terzi solo se sono necessari a questi ultimi per la conclusione o l'esecuzione di un contratto con la persona interessata. È possibile continuare a utilizzare un sistema semaforico della capacità di pagamento.

Per ulteriori informazioni sulle rivendicazioni derivanti da una lesione ingiustificata della personalità ai danni di una persona interessate, vedere il numero 3.

- **Obbligo di notifica delle violazioni della sicurezza dei dati:** 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 dal titolare del trattamento all'IFPDT «il più presto possibile» (nel senso di tempestivamente) (art. 24 LPD). La conservazione dei dati per un periodo troppo lungo (principio di proporzionalità o della finalità) non costituisce una violazione della *sicurezza* dei dati, anche se è una violazione della *protezione* dei dati. La notifica è necessaria, ad esempio, in caso di perdita di dati non criptati dei collaboratori (file del personale con le qualifiche e i dati relativi agli stipendi). Il rischio che le persone interessate possano subire danni è elevato. Se i dati crittografati dei collaboratori vengono persi, la situazione deve essere valutata in modo diverso. I fatti, le possibili conseguenze e le misure adottate (ad esempio, l'informazione delle persone interessate) devono essere notificati. Le persone interessate saranno informate, se del caso, per la loro protezione o su richiesta dell'IFPDT. L'obbligo di notifica è ulteriormente illustrato nell'art. 15 OPDa. In particolare, stabilisce che la violazione della sicurezza dei dati oggetto dell'obbligo di notifica deve essere documentata. La documentazione deve essere conservata per due anni.

3. Quali (ulteriori) diritti hanno le persone interessate?

Le regole e gli obblighi dei titolari del trattamento descritti al numero 2 comportano naturalmente anche diritti corrispondenti per le persone interessate. Inoltre, la LPD contiene ulteriori diritti delle persone interessate, alcuni dei quali saranno ampliati dalla revisione. Questi ultimi sono:

- **Diritto d'accesso:** il diritto d'accesso delle persone interessate ai sensi dell'art. 25 LPD va oltre l'obbligo di informazione del titolare del trattamento. La persona interessata può venire a conoscenza di più di quanto il titolare del trattamento sia tenuto a rivelare in virtù del suo obbligo di informazione. 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). L'obiettivo è quindi quello di creare un'ampia trasparenza nel trattamento dei dati per una persona interessata che ne faccia richiesta. Di norma, le informazioni sono gratuite e devono essere fornite entro 30 giorni. La persona che chiede informazioni deve identificarsi chiaramente. L'art. 26 LPD disciplina le restrizioni al diritto d'accesso. Ad esempio, le domande querulose non devono essere

trattate. Una domanda può essere respinta anche a causa di interessi preponderanti di terzi. Sono previste ulteriori eccezioni, in particolare per i media (art. 27 LPD). Ulteriori regolazioni sul diritto d'accesso sono contenute nell'OPDa (artt. 16-19).

- **La portabilità dei dati** include ora il diritto i farsi consegnare dati o di esigerne la trasmissione a terzi (art. 28 LPD)**.** Le persone interessate possono chiedere di recuperare i dati che hanno comunicato al titolare del trattamento 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. A queste condizioni, può essere richiesto anche la trasmissione dei dati a terzi, qualora non comporti un onere sproporzionato. La portabilità dei dati può essere limitata per motivi analoghi a quelli del diritto d'accesso (art. 29 LPD). Ulteriori regolazioni sulla portabilità dei dati sono contenute nell'OPDa (artt. 20-22).

- **Diritto di rettifica:** ai sensi dell'art. 32 cpv. 1 LPD, la persona interessata può chiedere la rettifica dei dati personali inesatti; è probabile che ciò avvenga dopo aver esercitato il diritto d'accesso. Il titolare del trattamento può rifiutarsi di effettuare la rettifica qualora una disposizione di legge lo vieti (ad esempio, norme contabili e di conservazione). Se non è possibile stabilire né l'esattezza né l'inesattezza dei dati personali in oggetto, la persona interessata può chiedere che venga aggiunta una menzione del carattere contestato ai dati (art. 32 cpv. 3 LPD).

- **Diritto alla cancellazione dei dati («diritto all'oblio»):** come già menzionato, ai sensi dell'art. 30 LPD si verifica una lesione della personalità, tra l'altro, se i dati personali vengono trattati in contrasto con l'esplicita dichiarazione di volontà della persona interessata e non sussiste alcuna base legale né alcun interesse privato preponderante di terzi nel senso di una giustificazione ai sensi dell'art. 31 LPD. Ne consegue una limitazione del diritto alla cancellazione dei dati per la persona interessata.

- **Ulteriori rivendicazioni:** in caso di lesioni ingiustificate della personalità, le persone interessate possono avanzare ulteriori rivendicazioni civili. Ai sensi dell'art. 32 cpv. 2 LPD, si tratta (a) del divieto di determinati trattamenti di dati, (b) del divieto di determinate comunicazioni di dati personali a terzi e (c) anche della cancellazione o distruzione di dati personali. In base al riferimento dell'art. 32 cpv. 2 LPD al Codice civile, possono sussistere le seguenti ulteriori rivendicazioni: l'accertamento, l'omissione o l'eliminazione della lesione, nonché le richieste di risarcimento danni, di riparazione morale e di restituzione del profitto.

4. Quali sono le conseguenze delle violazioni della protezione dei dati?

- Come nella legge precedente, le violazioni degli obblighi di protezione dei dati ai sensi della nuova LPD possono avere ripercussioni legate sia al diritto di vigilanza (art. 49 e segg. LPD), che al diritto penale (art. 60 e segg. LPD) e al diritto civile (art. 30 e segg. LPD). Mentre nella legge precedente non era punibile la violazione di praticamente nessun obbligo legale, la parte relativa al diritto penale della LPD rivista è notevolmente ampliata e le possibili sanzioni sono considerevolmente più elevate. Anche la parte relativa al diritto di vigilanza sarà ampliata, conferendo all'IFPDT poteri più ampi. Al contrario, la parte relativa al diritto civile rimane praticamente invariata.

- L'IFPDT avvia un'indagine d'ufficio o su segnalazione se vi sono sufficienti indizi che un'operazione di trattamento dei dati possa violare le norme in materia di protezione dei dati (art. 49 LPD). In caso di violazioni minori, può astenersi da un'indagine (principio dell'opportunità). L'IFPDT dispone ora di ampi poteri investigativi sulle imprese, tra cui la perquisizione domiciliare e l'audizione di testimoni (art. 50 LPD). In caso di violazioni della protezione dei dati, l'IFPDT può ordinare l'adeguamento, l'interruzione o la cessazione totale o parziale del trattamento e la cancellazione o la distruzione dei dati personali (art. 51 LPD). I ricorsi contro le decisioni dell'IFPDT possono essere presentati al Tribunale amministrativo federale. Le sentenze del Tribunale amministrativo federale possono essere

impugnate davanti al Tribunale federale. Sono riservati anche i rimedi giuridici previsti dalla Convenzione europea dei diritti dell'uomo.

- A differenza delle autorità europee per la protezione dei dati, l'IFPDT non ha alcun potere sanzionatorio *relativo al diritto di vigilanza* (diretto) ai sensi della nuova legge. Le persone che hanno commesso l'infrazione vengono sanzionate dalle autorità cantonali preposte al perseguimento penale. L'IFPDT può solo sporgere denuncia penale ed esercitare i diritti di parte civile nel procedimento (art. 65 cpv. 2 LPD).

- Nella nuova LPD, i trasgressori sono soggetti a un sistema di sanzioni *penali* con multe fino a CHF 250 000 (art. 60 e segg. LPD). Sono punibili solo le azioni e le omissioni *intenzionali*, ma non la negligenza. Solo su richiesta della persona interessata, sono puniti l'inosservanza degli obblighi di informazione, divulgazione e comunicazione, nonché la violazione del segreto professionale e degli obblighi di diligenza in relazione alla sicurezza dei dati, alla divulgazione dei dati all'estero e al mandato del trattamento. D'altra parte, l'inosservanza delle decisioni dell'IFPDT è perseguita d'ufficio (potere sanzionatorio indiretto). Anche quest'ultimo può sporgere denuncia, ma non ha il diritto di sporgere una denuncia penale. Le autorità cantonali sono responsabili dell'esecuzione della sanzione attraverso i tradizionali canali di ricorso. Di norma, vengono multate le *persone fisiche* responsabili. Ciò potrebbe riguardare in primo luogo i membri responsabili degli organi decisionali, come la direzione aziendale e il consiglio di amministrazione, soprattutto nell'ambito del loro compito organizzativo strategico, ma anche i singoli collaboratori nell'ambito delle loro attività operative. L'impresa stessa può ora essere multata fino a CHF 50 000 se l'identificazione della persona fisica passibile di pena all'interno dell'impresa o dell'organizzazione comporterebbe uno sforzo investigativo sproporzionato.

  A differenza della LPD, le sanzioni previste dal GDPR sono rivolte esclusivamente alle persone *giuridiche*. Le autorità preposte alla protezione dei dati nell'UE possono comminare alle imprese inadempienti multe fino a 20 milioni di euro o corrispondenti al 4% del loro fatturato globale annuo.

- Per far valere le rivendicazioni civili derivanti da lesioni della personalità ai sensi dell'art. 32 LPD, le persone interessate devono rivolgersi ai tribunali civili.

- In relazione alle violazioni della protezione dei dati, è importante menzionare anche i rischi di reputazione e di fiducia, che possono superare di molte volte i rischi relativi al diritto di vigilanza e al diritto penale. In relazione agli incidenti legati alla protezione dei dati e alla sicurezza delle informazioni, le imprese sono talvolta tenute ad affrontare anche rischi esistenziali (continuità operativa, responsabilità, ecc.). Questo aspetto deve essere tenuto in debita considerazione nell'ambito della gestione del rischio.

5. Disclaimer

La presente scheda informativa ha uno scopo puramente informativo e non costituisce una lista di controllo completa, né può sostituire la consulenza legale. L'Unione svizzera delle arti e mestieri usam declina ogni responsabilità che possa derivare dall'applicazione o dall'omissione di qualsiasi azione di questa scheda informativa. Si consiglia inoltre di contattare l'organizzazione di settore competente, in grado di fornire ulteriori consigli.

6. Allegato: modelli di documenti

- Informativa sulla privacy (sito web)
- Informativa sulla privacy (interna)
- Registro di trattamento dei dati (struttura)

- Valutazione dell’impatto sulla protezione dei dati (struttura)
- Contratto di mandato del trattamento
- CG clausola di protezione dei dati

Ultimo aggiornamento: 6 dicembre 2022

Responsabile del dossier

Dieter Kläy, caposezione
Tel. 031 380 14 45, E-mail d.klaey@sgv-usam.ch