Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
Préposé fédéral à la protection des données et à la transparence PFPDT
Incaricato federale della protezione dei dati e della trasparenza IFPDT
Incumbensà federal per la protecziun da datas e per la transparenza IFPDT

La nuova legge sulla protezione dei dati dal punto di vista dell'IFPDT

Indice

I. Introduzione

Nella sessione autunnale 2020 l'Assemblea federale ha adottato la revisione totale della legge sulla protezione dei dati (LPD) e altri atti normativi modificati riguardanti lo stesso argomento. Il 31 agosto 2022 il Consiglio federale ha deciso che metterà in vigore la nuova legge e le relative ordinanze il 1° settembre 2023.

Fino all'entrata in vigore l'economia privata e le autorità federali dovranno aver adeguato il trattamento dei dati personali alle nuove disposizioni. Per il momento l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) segnala le novità più importanti di cui tenere conto.

II. Genesi e scopo della revisione

La prima legge federale del 19 giugno 1992 sulla protezione dei dati è entrata in vigore nel 1993, quando Internet non era ancora usato a scopi commerciali e non era possibile prevedere una realtà digitale caratterizzata dall'onnipresenza degli *smartphone*. Dopo una revisione parziale nel 2008 che mirava a informare meglio la popolazione sul trattamento dei dati personali, si è presto rivelato necessario apportare ulteriori adeguamenti per stare al passo con il repentino sviluppo tecnologico. Nel frattempo per la maggior parte di noi è quasi impossibile immaginare una vita senza un ininterrotto accesso a Internet e senza apparecchi intelligenti dotati di schermi tattili. Si è dunque reso inevitabile modificare completamente la LPD al fine di garantire una protezione dei dati moderna alla popolazione che usa quotidianamente strumenti digitali quali il *cloud computing*, i big data, le reti sociali e l'Internet delle cose.

Nell'autunno del 2017 il Consiglio federale ha adottato il disegno di revisione totale della LPD e lo ha trasmesso alle Camere federali con il relativo messaggio. Lo scopo della revisione era di adeguare la protezione dei dati alle nuove evoluzioni tecnologiche e sociali. La nuova LPD deve dunque soddisfare l'esigenza di rafforzare e garantire il più a lungo possibile l'autodeterminazione informativa dei cittadini e la loro sfera privata.

Oltre a maggiori diritti delle persone interessate, il Consiglio federale rileva nel messaggio il cosiddetto approccio basato sui rischi quale elemento fondamentale della revisione: secondo tale approccio lo Stato e le imprese devono rilevare per tempo i rischi per la sfera privata e l'autodeterminazione informativa e contemplare le esigenze della protezione dei dati sin dalla pianificazione dei progetti digitali. I rischi elevati devono essere documentati insieme alle misure organizzative e tecniche prese per eliminarli o ridurli. Inoltre la LPD rivista promuove anche l'autoregolazione esonerando da determinati obblighi i membri di settori che emanano un codice di condotta vincolante. Ancora, la LPD rivista prevede alcune novità concepite per rafforzare le competenze di vigilanza dell'IFPDT.

All'inizio del 2018 il Parlamento ha deciso di suddividere la revisione in due fasi: al fine di rispettare termini di esecuzione risultanti da trattati internazionali, nella prima fase sono state adeguate le disposizioni relative al trattamento dei dati valide per organi federali, quali fedpol, che applicano la riveduta direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nel settore del diritto penale, dato che questa fa parte del cosiddetto *acquis* di Schengen. Questi lavori hanno portato alla legge sulla protezione dei dati in ambito Schengen (LPDS). La revisione della LPD nell'insieme è stata affrontata nella seconda fase.

1. Fase 1: parte Schengen

La LPDS è entrata in vigore il 1° marzo 2019 e si applica fino all'entrata in vigore della revisione totale della LPD. Oltre alla LPDS, sono stati adeguati altri atti normativi che rientrano nell'ambito della collaborazione di Schengen in materia penale.

2. Fase 2: intero atto legislativo

Nella sessione autunnale 2019 il Consiglio nazionale, in qualità di Camera prioritaria, ha esaminato la revisione totale dell'intera legge che le Camere federali hanno adottato il 25 settembre 2020 dopo la procedura di appianamento delle divergenze. Nello strutturare la nuova LPD il Consiglio federale e il Parlamento hanno tenuto conto della Convenzione STE 108[1] riveduta, firmata dalla Svizzera, e del regolamento europeo sulla protezione dei dati (RGPD)[2]. Trattandosi di un campo di applicazione extraterritoriale, il RGPD è già applicato da ampie cerchie dell'economia elvetica sin dalla sua entrata in vigore a maggio 2018. Nonostante la sua compatibilità con il diritto europeo, la nuova LPD segue la tradizione legislativa svizzera: presenta un elevato grado di astrazione ed è formulata in modo tecnologicamente neutro. Si differenzia dal RGPD non soltanto perché è più concisa, ma anche perché usa in parte una terminologia differente. In linea generale si presuppone che dopo la revisione delle normative sulla protezione dei dati la Svizzera e l'UE riconosceranno reciprocamente l'adeguatezza del rispettivo livello di protezione dei dati permettendo di continuare lo scambio informale di dati personali transfrontaliero.

III. Principali novità della revisione totale della legge sulla protezione dei dati

3. Soltanto dati di persone fisiche

La LPD rivista ha esclusivamente lo scopo di proteggere la personalità delle persone fisiche di cui vengono trattati i dati, mentre non tratta più i dati di persone giuridiche quali società commerciali, associazioni o fondazioni, rendendo così il suo ambito di applicazione conforme al RGPD. Le imprese possono continuare ad appellarsi alla protezione della personalità di cui all'articolo 28 CC, alla protezione del segreto di fabbrica o commerciale di cui all'articolo 162 CP e alle disposizioni pertinenti delle leggi federali contro la concorrenza sleale e sui cartelli.

4. Dati personali degni di particolare protezione

La nozione di «dati personali degni di particolare protezione» è estesa ai dati genetici e ai dati biometrici che identificano in modo univoco una persona fisica.

---

[1] Convenzione del 28 gennaio 1981 per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale, conclusa a Strasburgo il 28 gennaio 1981, approvata dall'Assemblea federale il 5 giugno 1997. L'ampliamento della Convenzione è stato approvato dalle Camere federali nell'estate del 2020. Il Consiglio federale potrà ratificarlo soltanto dopo l'entrata in vigore della nuova LPD.

[2] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

5. Privacy by design e privacy by default (nuovo: art. 7 LPD)

Nella LPD rivista sono stati introdotti i principi di «privacy by design» (protezione dei dati sin dalla progettazione) e di «privacy by default» (protezione dei dati per impostazione predefinita) che obbligano le autorità e le imprese ad attuare i principi di trattamento di cui alla LPD sin dalla fase di progettazione prendendo misure di protezione adeguate tanto tecniche quanto organizzative. La protezione dei dati sin dalla progettazione prevede che le autorità e le imprese impostino le loro applicazioni in modo che i dati siano cancellati o anonimizzati in maniera standardizzata. La protezione dei dati per impostazione predefinita ammette soltanto il trattamento dei dati direttamente necessari allo scopo e protegge così gli utenti di offerte online private che non esaminano le condizioni di utilizzazione né i diritti di opposizione che ne derivano; resta salva la facoltà dell'utente di autorizzare un trattamento più ampio se lo desidera. Al fine di garantire questo nuovo tipo di protezione, le imprese svizzere dovrebbero controllare per tempo la propria offerta ed eventualmente adeguarla mediante programmi favorevoli alla protezione dei dati e ai clienti.

6. Consulenti per la protezione dei dati (nuovo: art. 10 LPD)

Ai sensi dell'articolo 10 LPD rivista le imprese private possono designare un consulente per la protezione dei dati che può, ma non deve, essere legato all'impresa mediante un contratto di lavoro. In entrambi i casi l'attività di consulenza deve essere svolta in modo indipendente dalle altre mansioni dell'impresa. È anche opportuno che le attività dei consulenti per la protezione dei dati siano separate da quelle di consulenza di altro genere o di rappresentanza giuridica. Inoltre ai consulenti per la protezione dei dati occorre permettere di esprimere il proprio punto di vista in caso di divergenze d'opinione con la direzione aziendale (art. 23 lett. c OLPD). Contrariamente a quanto previsto nel RGPD europeo, per le imprese private la designazione del consulente per la protezione dei dati è sempre facoltativa – soltanto per gli organi federali è obbligatoria. Il consulente per la protezione dei dati non è soltanto il punto di riferimento all'interno dell'impresa, ma anche l'anello di congiunzione con l'autorità di protezione dei dati e la prima persona di contatto per l'IFPDT. Nelle sue mansioni rientra la consulenza generalizzata e la formazione dell'impresa nelle questioni che riguardano la protezione dei dati, la partecipazione all'emanazione e all'applicazione di condizioni di utilizzazione e disposizioni di protezione dei dati. Se la consulenza interna è svolta in modo tecnicamente e gerarchicamente indipendente e senza mansioni incompatibili con la funzione, dopo l'analisi d'impatto sulla protezione dei dati l'impresa può limitarsi alla consulenza interna senza dover consultare l'IFPDT, anche in caso di rischio permanentemente elevato (vedi in proposito «Valutazioni d'impatto sulla protezione dei dati»).

7. Valutazioni d'impatto sulla protezione dei dati (nuovo: art. 22s LPD)

Le valutazioni d'impatto sulla protezione dei dati non sono un elemento nuovo nel diritto svizzero della protezione dei dati: gli organi federali sono già oggi tenuti a svolgerle. Quando un trattamento può comportare un rischio elevato per la personalità o per i diritti fondamentali della persona interessata, anche i titolari privati del trattamento devono farlo precedere da una valutazione d'impatto sulla protezione dei dati. In particolare quando si usano nuove tecnologie, il rischio elevato risulta dal modo, dalla portata, dalle condizioni e dallo scopo del trattamento, soprattutto se è prevista una profilazione a rischio elevato o un ampio trattamento di dati personali degni di particolare protezione. Anche se è impostata in modo generale, la valutazione d'impatto sulla protezione dei dati non può dispensare da rischi riconoscibili che non vi sono menzionati. Se un prodotto, un sistema o un servizio è certificato ai sensi della legge sulla protezione dei dati o se si rispetta un codice di condotta basato su una valutazione d'impatto, si può prescindere dal redigerne un'altra. Se la valutazione d'impatto sulla

protezione dei dati lascia prevedere che il trattamento pianificato comporta un rischio elevato per la personalità o i diritti fondamentali della persona interessata nonostante le misure prese dal titolare, questi deve dapprima chiedere il parere dell'IFPDT. Quest'ultimo consiglia di precisarla o di completarla se ha obiezioni riguardo alla valutazione d'impatto perché il testo è redatto in maniera troppo generale e descrive gli eventuali rischi o le misure soltanto in modo insufficiente. Se tuttavia le obiezioni riguardanti la protezione dei dati si riferiscono al trattamento vero e proprio, l'IFPDT propone al titolare misure adeguate per modificarlo (vedi in proposito «Consulenze»). Contrariamente a quanto avviene per i codici di condotta, i pareri dell'IFPDT non sottostanno all'obbligo di pubblicazione. Tuttavia, in quanto documenti ufficiali, sottostanno alla legge federale sul principio di trasparenza dell'amministrazione. È possibile rinunciare a consultare l'IFPDT quando è già stato interpellato il consulente interno per la protezione dei dati (vedi in proposito «Consulenti per la protezione dei dati»).

8. Codice di condotta (nuovo: art. 11 LPD)

Per associazioni professionali, settoriali ed economiche la nuova LPD prevede all'articolo 11 incentivi a sviluppare codici di condotta propri e a sottoporli per parere all'IFPDT. I pareri sono pubblicati e possono contenere obiezioni e raccomandare relative modifiche o precisazioni. I pareri positivi dell'IFPDT fungono da base alla presunzione giuridica che la condotta riportata nel codice sia conforme alle disposizioni di protezione dei dati. I codici formulati in maniera generale non possono invece dispensare da ogni rischio che non sia citato con precisione nel testo. Accettando un codice di condotta, i membri delle associazioni possono rinunciare a elaborare supporti e indicazioni per l'applicazione della nuova LPD. Questa forma di autoregolamentazione presenta inoltre il vantaggio per queste associazioni di non dover svolgere valutazioni proprie d'impatto sulla protezione dei dati se è rispettato un codice di condotta basato su una valutazione d'impatto già svolta e ancora attuale, che preveda misure di protezione della personalità o dei diritti fondamentali e sia stata sottoposta all'attenzione dell'IFPDT.

9. Certificazioni (nuovo: art. 13 LPD)

Oltre ai sistemi di gestione e ai prodotti, ora sono certificabili servizi e processi. La certificazione permette alle imprese, ad esempio, di comprovare che rispettano il principio della protezione dei dati per impostazione predefinita e che dispongono di un sistema adeguato di gestione della protezione dei dati. Se un titolare privato del trattamento impiega un sistema, prodotto o servizio certificato, può rinunciare a svolgere una valutazione d'impatto sulla protezione dei dati. Il Consiglio federale ha disciplinato ulteriori disposizioni sulla procedura di certificazione e sul marchio di qualità mediante ordinanza (OCPD).

10. Registro delle attività di trattamento (nuovo: art. 12 LPD)

Secondo la nuova legge i titolari e i responsabili del trattamento devono tenere un registro di tutte le attività di trattamento; l'articolo elenca quelle fondamentali. Il registro deve sempre essere aggiornato. Nell'ordinanza il Consiglio federale ha previsto eccezioni per le imprese con meno di 250 collaboratori i cui trattamenti di dati personali comportano soltanto un rischio esiguo di violazione della personalità delle persone interessate (art. 24 OLPD). Gli organi federali devono notificare all'IFPDT i registri; per i responsabili privati del trattamento dei dati le nuove disposizioni non prevedono l'obbligo di notifica.

11. Comunicazione di dati personali all'estero (nuovo: art. 16 LPD)

La LPD rivista stabilisce all'articolo 16 che i dati personali possono essere comunicati all'estero soltanto se il Consiglio federale ha constatato che la legislazione dello Stato destinatario o

l'organismo internazionale garantisce una protezione adeguata dei dati. L'elenco tenuto sinora dall'IFPDT è ora parte dell'OLPD (allegato 1). Se lo Stato destinatario non figura nell'elenco del Consiglio federale, i dati possono comunque essergli comunicati, come avvenuto finora con il diritto vigente, se la protezione dei dati viene assicurata in modo adeguato con altri strumenti, ad esempio mediante un trattato di diritto internazionale, clausole contrattuali di protezione dei dati che devono essere precedentemente comunicate all'IFPDT o norme interne dell'impresa vincolanti, le cosiddette *Binding Corporate Rules*. Clausole standard della Commissione europea già autorizzate con il RGPD sono riconosciute dall'IFPDT.

Se si prevede di pubblicare i dati all'estero – anche in caso di memorizzazione su sistemi esteri (cloud) – devono essere indicati alle persone interessate i Paesi in questione, indipendentemente dal fatto che offrano o meno una protezione dei dati adeguata. In questo ambito la LPD è più severa del RGPD. È inoltre necessario indicare quali garanzie di protezione dei dati potrebbero eventualmente essere applicate (p. es. clausole contrattuali standard dell'UE) oppure a quali eccezioni si riferisce il titolare del trattamento; anche in questo caso la LPD differisce dal RGPD.

12. Ampi obblighi di informazione (nuovo: art. 19 segg. LPD)

In adempimento dell'obiettivo di trasparenza perseguito dalla revisione, la nuova LPD estende l'obbligo di informazione per le imprese. In linea di massima in futuro il titolare privato deve precedentemente informare in ogni caso e in modo adeguato la persona interessata sulla prevista raccolta di dati personali anche se i dati non sono raccolti presso di essa. La LPD vigente prescrive questo obbligo di informazione soltanto in caso di dati personali e profili della personalità degni di particolare protezione. Concretamente, devono essere resi noti l'identità e le coordinate di contatto del titolare del trattamento, lo scopo del trattamento ed eventualmente i destinatari o le categorie di destinatari cui sono stati comunicati i dati personali. Diversamente da quanto previsto nel RGPD, devono essere fornite informazioni anche sullo Stato destinatario e sulle eventuali garanzie di un adeguato livello di protezione di dati (vedi sopra, Comunicazione di dati personali all'estero). Le imprese devono dunque esaminare e tenere aggiornate le proprie dichiarazioni relative alla protezione dei dati. Sono esclusi dall'obbligo di informazione i dati personali rilevati soltanto incidentalmente o per caso. L'obbligo di informazione è inoltre limitato o abolito in presenza dei numerosi motivi di limitazione ed eccezione. Ciò si verifica, ad esempio, quando le persone interessate dispongono già delle informazioni o il trattamento dei dati è previsto per legge. Se il trattamento comporta decisioni individuali automatizzate, il titolare del trattamento deve rispettare nuovi obblighi di informazione nei confronti della persona interessata e accordarle i diritti di essere sentita e di riesaminare la decisione.

13. Diritto d'accesso della persona interessata (nuovo: art. 25 segg. LPD)

La nuova LPD estende il diritto della persona interessata di chiedere se dati personali che la concernono sono oggetto di trattamento. Il nuovo articolo 25 presenta un elenco più esteso delle informazioni che il titolare del trattamento deve comunicare, ad esempio, sulla durata di conservazione dei dati personali della persona interessata. Inoltre l'articolo sancisce che alla persona interessata devono essere messe a disposizione le informazioni necessarie affinché possa far valere i suoi diritti secondo la nuova LPD e sia garantito un trattamento trasparente dei dati. Come nel diritto vigente a determinate condizioni il titolare può rifiutare, limitare o differire l'informazione.

14. Obbligo di notifica di violazioni della sicurezza dei dati (nuovo: art. 24 LPD)

Conformemente all'articolo 24 della nuova LPD il titolare del trattamento deve notificare all'IFPDT ogni violazione della sicurezza dei dati che comporta un rischio elevato per la

personalità o i diritti fondamentali della persona interessata. La disposizione vale sia per i titolari privati sia per gli organi federali. La notifica deve pervenire quanto prima all'IFPDT, dopo che il titolare ha redatto una previsione delle possibili conseguenze della violazione e ha valutato se sussistono rischi, se la persona interessata debba essere informata della violazione e in che modo. Se il titolare ritiene che il rischio non sia elevato può comunque far pervenire all'IFPDT una notifica in merito. L'obbligo di notifica all'IFPDT sussiste soltanto in caso di violazione della personalità o dei diritti fondamentali, ma non di attacchi cibernetici respinti con successo o falliti. Anche il RGPD europeo prevede un obbligo di notifica corrispondente e indica scadenze concrete da rispettare presso le autorità di protezione dei dati dell'UE. Inoltre il diritto europeo prevede una soglia di notifica più bassa dato che presuppone soltanto un rischio semplice.

15. Diritto alla portabilità dei dati (nuovo: art. 28 LPD)

Il diritto di farsi consegnare dati o di esigerne la trasmissione a terzi, sancisce la possibilità della persona interessata di chiedere che i propri dati personali che ha reso noti a un titolare privato le siano consegnati in un formato elettronico usuale o siano trasmettessi a terzi. Questo presuppone che il titolare tratta i dati personali in modo automatizzato e che il trattamento sia effettuato con il consenso della persona interessata oppure in relazione diretta con un contratto. Il diritto può esser fatto valere in modo gratuito a meno che la consegna o la trasmissione richieda un onere sproporzionato come. ad esempio. nel caso di dati inerenti la comunicazione, per i quali si rende necessario un complicato smistamento tra le dichiarazioni proprie e quelle di terzi.

16. Inchiesta per violazione delle disposizioni sulla protezione dei dati (nuovo: art. 49 LPD)

In futuro l'IFPDT sarà tenuto a svolgere d'ufficio un'inchiesta in caso di violazioni della nuova LPD da parte di organi federali o di privati (art. 49 cpv. 1). Nella LPD vigente si applica ancora la limitazione secondo la quale l'IFPDT svolge di propria iniziativa un'inchiesta con accertamento dei fatti contro privati soltanto quando il metodo di trattamento può violare i diritti della personalità di un numero considerevole di persone. Questa soglia di intervento definita quale «errore di sistema» viene abolita. Tuttavia anche nella nuova LPD se la violazione delle disposizioni sulla protezione dei dati è di poca importanza, l'IFPDT può rinunciare ad aprire un'inchiesta (art. 49 cpv. 2). Inoltre, come avvenuto finora, può rinunciare a misure formali quando, dopo un primo scambio di informazioni, il titolare del trattamento riconosce la lacuna che gli è stata notificata e vi pone rimedio in tempo utile. Date le risorse limitate di cui dispone, si può prevedere che anche dopo l'entrata in vigore della nuova legge in generale l'IFPDT intenda determinare delle priorità nel trattamento di notifiche in base al principio dell'opportunità.

17. Provvedimenti amministrativi (nuovo: art. 51 LPD)

L'IFPDT potrà ora svolgere procedure secondo la legge federale sulla procedura amministrativa[3] e ordinare formalmente a organi federali o titolari privati di trattamenti di dati di adeguare, sospendere o cessare del tutto o in parte il trattamento nonché di cancellare o distruggere del tutto o in parte i dati personali. Può, ad esempio, ordinare che un'impresa informi la persona interessata della violazione notificata della sicurezza dei dati. Finora l'IFPDT

[3] Legge federale del 20 dicembre 1968 sulla procedura amministrativa (PA), RS 172.021.

aveva soltanto la competenza di emanare raccomandazioni e di adire il Tribunale amministrativo federale in caso di mancata ottemperanza.

Contro le decisioni dell'IFPDT è possibile opporre ricorso presso il Tribunale amministrativo federale e proseguire la causa presso il Tribunale federale. Anche l'IFPDT può impugnare presso il Tribunale federale le decisioni su ricorso pronunciate dal Tribunale amministrativo federale.

18. Consulenze

L'IFPDT non è né un'autorità di approvazione né un servizio di omologazione per applicazioni, prodotti, regolamentazioni e progetti. Tuttavia, la nuova legge prevede in svariati articoli che i titolari debbano consultare l'IFPDT prima della conclusione definitiva di lavori e la realizzazione di progetti. Devono dunque essergli sottoposti per parere codici di condotta nonché valutazioni d'impatto sulla protezione dei dati in caso di elevati rischi residui. Data la natura astratta di questi oggetti di consultazione, i pareri dell'IFPDT non avranno in genere un carattere vincolante e le misure e gli obblighi raccomandati non permetteranno il ricorso. Se non ottemperano ai pareri dell'IFPDT, i titolari del trattamento devono prendere tuttavia in considerazione la possibilità che trattamenti specifici di dati nell'ambito di raccomandazioni dell'IFPDT saranno in seguito oggetto di decisioni. Queste ultime potranno vietare completamente il trattamento di dati; i titolari potranno comunque avvalersi dei rimedi giuridici ordinari previsti dalla procedura amministrativa.

19. Pareri spontanei e informazione del pubblico

A parte i pareri nel quadro di consultazioni formali, l'IFPDT può continuare a esprimersi in modo spontaneo su nuove tecnologie, questioni di digitalizzazione o pratiche di trattamento di determinati settori e pubblicare la propria opinione e la propria valutazione. Inoltre, in caso di interesse generale l'IFPDT informa il pubblico, come secondo il diritto finora vigente, delle proprie constatazioni e misure. Ciò vale anche per gli accertamenti e i provvedimenti amministrativi scaturiti da indagini formali dell'IFPDT.

20. Emolumenti (nuovo: art. 59 LPD)

La legge disciplina le prestazioni dell'IFPDT per le quali i privati dovranno versare emolumenti: ad esempio, per un parere in merito a un codice di condotta o per una valutazione d'impatto sulla protezione dei dati o ancora per l'approvazione di clausole tipo di protezione dei dati e di norme interne d'impresa vincolanti. L'IFPDT potrà però riscuotere dai privati emolumenti anche per servizi di consulenza generale. I particolari sono determinati nell'ordinanza (OLPD).

21. Sanzioni (nuovo: art. 60 segg. LPD)

Nella nuova LPD sono previste multe per privati fino a 250 000 franchi. Sono punibili atti od omissioni intenzionali, ma non quelli colposi. Il mancato rispetto degli obblighi di informare, di concedere l'accesso e di collaborare nonché la violazione degli obblighi di diligenza e del segreto professionale sono punibili a querela di parte. Invece il mancato rispetto di provvedimenti amministrativi dell'IFPDT è perseguito d'ufficio. In linea di massima sono punibili con multa soltanto le persone fisiche, ma in futuro potranno esserlo anche le imprese stesse fino a 50 000 franchi, se la ricerca della persona fisica all'interno dell'impresa o dell'organizzazione esige un onere sproporzionato.

Contrariamente a quanto avviene nel caso delle autorità europee di protezione dei dati, nel regime previsto dalla nuova LPD l'IFPDT continuerà a non avere la facoltà di pronunciare sanzioni. Le persone che si sono rese colpevoli sono sanzionate dalle autorità di

perseguimento cantonali. L'IFPDT può sporgere denuncia e avvalersi nel procedimento dei diritti dell'accusatore privato, ma non ha il diritto di querela. Diversamente da quanto previsto nella nuova LPD, nel RGPD le sanzioni amministrative sono pronunciate soltanto contro persone giuridiche. Le autorità di protezione dei dati dell'UE possono emettere contro le imprese multe fino a 20 milioni di euro o fino al 4 per cento del loro fatturato annuo a livello mondiale.

IFPDT, 9 febbraio 2021 – aggiornato per l'ultima volta il 7 ottobre 2022