Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ
Direktionsbereich Öffentliches Recht

Revisione totale della legge sulla protezione dei dati
FAQ – Domande frequenti

Data: febbraio 2024

Riferimento: 212.9-754/50/4

La legge sulla protezione dei dati sottoposta a revisione totale (LPD; RS 235.1; entrata in vigore: 1° settembre 2023) conforma la protezione dei dati agli sviluppi tecnologici e agli standard europei. Questo documento raccoglie le risposte dell'Ufficio federale di giustizia (UFG) a svariate domande fondamentali in materia, al fine di rendere più comprensibile la nuova legge con le rispettive ordinanze, facilitando quindi l'applicazione da parte dei responsabili privati del trattamento e degli organi federali.

Le domande e le risposte seguono la struttura della legge sulla protezione dei dati. Le risposte si fondano sia sul messaggio del 15 settembre 2017 concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati sia sul rapporto esplicativo del 31 agosto 2022 riguardante l'ordinanza sulla protezione dei dati (OPDa; RS 235.11; entrata in vigore: 1° settembre 2023). L'accento è posto in particolare sulle disposizioni introdotte nel corso dei dibattimenti parlamentari e quindi non esaustivamente documentate nei lavori preliminari (p. es. per quanto riguarda il concetto di profilazione a rischio elevato o l'obbligo di rappresentanza per titolari privati domiciliati all'estero).

Questo documento, che sostituisce le «Domande frequenti diritto in materia di protezione dei dati» del 1° febbraio 2023 dell'UFG, sarà aggiornato e integrato costantemente.

Indice

1. Campo d’applicazione della legge sulla protezione dei dati (LPD) 4
1.1 Campo d’applicazione personale e materiale 4
1.2 Campo d’applicazione territoriale 5
2. Definizioni 6
2.1 Dati personali e dati personali degni di particolare protezione 6
2.2 Trattamento di dati 7
2.3 Profilazione 8
3. Principi applicabili (selezione) 10
3.1 Principio della trasparenza e delle riconoscibilità 10
3.2 Principio della finalità 11
3.3 Principio dell’esattezza 11
3.4 Consenso 11
3.5 Protezione dei dati fin dalla progettazione e per impostazione predefinita 13
3.6 Sicurezza dei dati 13
3.7 Consulenti per la protezione dei dati 17
3.8 Registro delle attività di trattamento 18
4. Obbligo di rappresentanza per titolari privati domiciliati all’estero 20
4.1 Condizioni 20
4.2 Compiti e obblighi del rappresentante 21
5. Comunicazione di dati personali all’estero 22
5.1 Panoramica 22
5.2 Valutazione dell'adeguatezza del Consiglio federale 22
5.3 Garanzie d'un livello di protezione dei dati appropriata 23
5.4 Eccezioni 25
6. Obblighi del titolare e del responsabile del trattamento 26
6.1 Obbligo del titolare di informare sulla raccolta di dati personali 26
6.2 Decisione individuale automatizzata 28
6.3 Valutazione d’impatto sulla protezione dei dati 30
6.4 Notifica di violazioni della sicurezza dei dati 31
7. Diritti dell’interessato 32
7.1 Panoramica 32
7.2 Diritto d’accesso 33
7.2.2 Domanda 33
7.3 Diritto alla consegna o alla trasmissione dei dati 34
8. Disposizioni speciali per il trattamento di dati da parte di privati 34
9. Disposizioni speciali per il trattamento di dati da parte di organi federali 35
10. Incaricato federale della protezione dei dati e della trasparenza (IFPDT) 35
11. Disposizioni penali 36
11.1 Panoramica 36
11.2 Destinatari delle disposizioni penali 36
11.3 Competenza in materia penale 37

12. Sviluppi internazionali in materia di protezione dei dati 37
12.1 Direttiva (UE) 2016/680 37
12.2 Regolamento generale dell'UE sulla protezione dei dati e valutazione dell'adeguatezza 37
12.3 Convenzione 108+ del Consiglio d'Europa sulla protezione dei dati 38

1. Campo d'applicazione della legge sulla protezione dei dati (LPD)

1.1 Campo d'applicazione personale e materiale

1.1.1 **Domanda**: *a chi si applica la LPD (campo d'applicazione personale)?*

La legge si applica a *privati* e *organi federali* che trattano dati personali (art. 2 cpv. 1 LPD). Sono organi federali le autorità o i servizi della Confederazione e le persone cui sono affidati compiti federali (art. 5 lett. i LPD). La legge non definisce per contro il concetto di «privati», che comprende in particolare le imprese e le persone fisiche (nella misura in cui non trattano dati in adempimento di un compito pubblico).

Il trattamento dei dati da parte di *autorità cantonali* (e *comunali*) non è retto dalla legge federale, ma da quelle cantonali; a prescindere dal fatto che i dati siano ottenuti direttamente oppure accedendo online a una banca dati della Confederazione. In linea di massima è retto dal diritto cantonale anche il trattamento di dati da parte di organi cantonali operanti in applicazione del diritto federale. In alcuni settori di competenza della Confederazione, come ad esempio quello delle assicurazioni sociali, esistono norme specifiche in materia di protezione dei dati, applicabili sia alle autorità federali competenti sia a quelle cantonali incaricate di applicare la legge federale. In questo contesto la Confederazione deve tuttavia tenere conto delle norme organizzative cantonali.

Rimandi: messaggio del 17 settembre 2017 concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati, FF 2017 5939, pag. 5951 e 6003 (qui di seguito: «messaggio LPD»); Scambio di dati personali tra autorità federali e cantonali. Rapporto del Consiglio federale del 22 dicembre 2010 in adempimento del postulato Lustenberger 07.3682 del 5 ottobre 2007 «Agevolazione dello scambio di dati tra autorità federali e cantonali», FF 2011 593.

1.1.2 **Domanda**: *quali sono i dati protetti dalla LPD (campo d'applicazione materiale)?*

Dopo la revisione totale della legge, il trattamento dei dati delle persone giuridiche non rientra più nel campo d'applicazione materiale: la LPD ormai si applica solo ai dati delle *persone fisiche* (= dati personali). Conferisce quindi diritti soltanto alle persone fisiche, non a quelle giuridiche (art. 2 cpv. 1 LPD e contrario).

Altre disposizioni dell'ordinamento giuridico svizzero continuano però a tutelare le persone giuridiche, la cui personalità è segnatamente protetta dal Codice civile (art. 28 segg. CC; RS 210), la legge federale contro la concorrenza sleale (LCSl; RS 241), la legge sul diritto d'autore (LDA; RS 231.1) o le disposizioni a tutela dei segreti professionali, d'affari e di fabbricazione. La sfera privata delle persone giuridiche è inoltre tutelata dall'articolo 13 della Costituzione federale (Cost; RS 101). Significa in particolare che gli organi federali possono trattare o comunicare i dati delle persone giuridiche soltanto se esiste una base legale sufficiente. Nel corso della revisione totale della LPD, sono pertanto state introdotte nuove disposizioni nella legge sull'organizzazione del Governo e dell'Amministrazione per disciplinare il trattamento dei dati di persone giuridiche da parte di organi federali (art. 57*r* segg. LOGA; RS 172.010). Infine, la disposizione transitoria dell'articolo 71 LPD previene eventuali lacune giuridiche per cinque anni.

La LPD non si applica ai dati materiali, e nemmeno a quelli anonimizzati, in quanto non sono più considerati personali una volta effettuata l'anonimizzazione.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6003 seg.; nota dell'UFG per l'elaborazione di basi legali per il trattamento dei dati da parte di organi federali: sinossi delle modifiche principali, ottobre 2022 (qui di seguito: «nota UFG/LPD»), pag. 26 segg.

1.1.3 **Domanda**: *quali deroghe prevede la LPD riguardo al campo d'applicazione personale e materiale?*

Stando all'articolo 2 capoverso 2, la LPD non si applica a dati personali trattati:

- da una persona fisica ad uso esclusivamente personale (lett. a);
- dalle Camere federali e dalle commissioni parlamentari nell'ambito delle loro deliberazioni (lett. b);
- da beneficiari istituzionali di cui all'articolo 2 capoverso 1 della legge sullo Stato ospite (RS 192.12) che godono dell'immunità di giurisdizione in Svizzera (lett. c).

  Esempio: CICR

Per i *procedimenti civili, penali e di assistenza giudiziaria internazionale, come pure per quelli di diritto pubblico e di diritto amministrativo* (esclusi quelli amministrativi di primo grado), l'articolo 2 capoverso 3 LPD disciplina il rapporto tra il diritto processuale e quello in materia di protezione dei dati: in presenza di un nesso diretto con un procedimento giudiziario, le modalità di trattamento dei dati personali e i diritti degli interessati in sede processuale sono retti dal diritto procedurale applicabile, che tutela la personalità e i diritti fondamentali di tutte le persone coinvolte. Per le deroghe alla vigilanza dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) cfr. l'articolo 4 capoverso 2 lettere c–e LPD.

I *registri pubblici relativi ai rapporti di diritto privato* tenuti da *autorità federali* sono disciplinati dalle disposizioni speciali del diritto federale applicabile (art. 2 cpv. 4 LPD), in particolare per quanto riguarda l'accesso a tali registri e i diritti degli interessati. In assenza di disposizioni speciali si applica la LPD. La legge riveduta affida all'IFPDT la vigilanza sui registri (art. 4 cpv. 1 LPD), ossia sul registro informatizzato dello Stato civile, su Zefix, sul registro aeronautico dell'Ufficio federale dell'aviazione civile e sui registri dell'Istituto federale della proprietà intellettuale (in particolare quelli dei marchi, dei brevetti e del design).

I registri pubblici di diritto privato di competenza dei *Cantoni* sono invece disciplinati dal diritto cantonale sulla protezione dei dati (cfr. in merito la domanda 1.1.1), anche nel caso in cui i dati personali siano trattati in esecuzione del diritto federale. Tuttavia il diritto cantonale non può impedire l'applicazione corretta e uniforme del diritto privato federale e in particolare il principio della pubblicità dei registri. Dei registri cantonali fanno parte il registro fondiario, il registro del naviglio, i registri cantonali di commercio, i registri sulle esecuzioni e sul fallimento nonché il registro pubblico sulle riserve di proprietà.

Rimandi: messaggio LPD, FF 2017 5939 pag. 6004 segg.

1.2 Campo d'applicazione territoriale

Domanda: *qual è il campo d'applicazione territoriale della LPD?*

Nel quadro della revisione totale della LPD, il Parlamento ha inserito nell'articolo 3 una disposizione esplicita riguardo al campo d'applicazione territoriale. In merito va fatta la seguente distinzione.

- Per le *disposizioni a protezione dei dati applicabili al diritto privato* e *a quello penale*, l'articolo 3 capoverso 2 LPD rimanda in forma dichiarativa alle norme di conflitto contemplate nella legge federale sul diritto internazionale privato (art. 139 LDIP; RS 291) e nel Codice penale (art. 3 segg. CP; RS 311.0).

- Per le *disposizioni a protezione dei dati applicabili al diritto pubblico*, comprendenti anche la vigilanza da parte dell'IFPDT, l'articolo 3 capoverso 1 LPD stabilisce l'applicazione della legge alle fattispecie che generano effetti in Svizzera, anche se si verificano all'estero. Di per sé non è una novità: secondo la giurisprudenza, in presenza di un forte nesso con la Svizzera le disposizioni a protezione dei dati nel diritto pubblico si applicano già oggi alle fattispecie internazionali; si tratta quindi di una codificazione della prassi giudiziaria riguardante il principio della territorialità e degli effetti nel diritto pubblico.

Rimandi: DTF 138 II 346 consid. 3.3.

2. Definizioni

2.1 Dati personali e dati personali degni di particolare protezione

2.1.1 **Domanda**: *cosa sono i dati personali?*

I dati personali comprendono tutte le informazioni relative a una persona identificata o identificabile (art. 5 lett. a LPD). Per contro, la nuova LPD non copre più i dati delle persone giuridiche (cfr. in merito la domanda 1.1.2).

Per il resto il concetto di «dati personali» riflette comunque quanto valevole finora. Una persona fisica è identificabile se può essere identificata direttamente o indirettamente, ad esempio grazie alle informazioni risultanti dalle circostanze o dal contesto (numero d'identificazione, dati relativi alla sua ubicazione, elementi specifici riguardanti le sue caratteristiche fisiche, fisiologiche, genetiche, psichiche, economiche, culturali o sociali). L'identificazione può basarsi su un solo elemento (numero di telefono, numero dell'immobile, numero AVS, impronte digitali) o sulla combinazione di varie informazioni (indirizzo, data di nascita e stato civile). La mera possibilità teorica che qualcuno possa essere identificato non è sufficiente per supporre che sia identificabile. Non si può parlare di identificabilità se l'identificazione richiede mezzi tali da rendere improbabile, per esperienza generale, che qualcuno vorrà farsene carico. Occorre invece tenere conto, in ogni singolo caso, di tutti i mezzi che possono essere ragionevolmente impiegati per identificare una persona. La ragionevolezza dei mezzi a disposizione deve essere valutata in relazione a tutte le circostanze, quali il dispendio di tempo e l'onere finanziario necessari per impiegarli, tenendo conto delle tecnologie disponibili al momento del trattamento e della loro evoluzione.

Rimandi: messaggio LPD, FF 2017 5939 pag. 6011; DTF 136 II 508.

2.1.2 **Domanda**: *cosa sono i dati personali degni di particolare protezione?*

Il concetto di dati personali degni di particolare protezione è definito in modo esaustivo nell'articolo 5 lettera c LPD. Come finora comprende i dati concernenti le opinioni o attività religiose, filosofiche, politiche o sindacali (n. 1), i dati concernenti la salute, la sfera intima o l'appartenenza a una razza (n. 2), i dati concernenti perseguimenti e sanzioni amministrativi e penali (n. 5) e i dati concernenti le misure d'assistenza sociale (n. 6).

La LPD sottoposta a revisione totale vi aggiunge le seguenti categorie di dati degni di particolare protezione.

- *Dati concernenti l'appartenenza a un'etnia (art. 5 lett. c n. 2 LPD):* stando alla giurisprudenza del Tribunale federale in merito all'articolo 261bis CP, un'etnia è un aggregato sociale che considera sé stesso come un gruppo ben distinto e come tale è percepito dal

resto della popolazione. Deve condividere una storia e un sistema coerente di mentalità e comportamenti (tradizioni, usi e costumi, lingua ecc.) che servono a distinguerlo[1].

Esempi: Albanesi del Kosovo, Arabi, Palestinesi o nomadi.[2]

- *Dati genetici (art. 5 cpv. c n. 3 LPD):* sono informazioni sul patrimonio genetico di una persona ottenute attraverso un esame genetico. La definizione riprende quella dell'articolo 3 lettera k della legge federale concernente gli esami genetici sull'essere umano (LEGU; RS 810.12).

  Esempio: profilo del DNA.

- *Dati biometrici che identificano in modo univoco una persona fisica (art. 5 lett. c n. 4 LPD):* sono quelli relativi a caratteristiche fisiche, fisiologiche o comportamentali ottenuti grazie a un processo tecnico specifico e atti a identificare univocamente una persona fisica o a confermarne l'identificazione. A differenza di quanto vale per i dati genetici, nel caso dei dati biometrici il processo tecnico che permette d'identificare univocamente la persona è parte integrante della loro qualifica come dati personali degni di particolare protezione. Senza questa precisazione anche le semplici fotografie o registrazioni audio godrebbero di protezione particolare.

  Esempi: immagine del viso trattata con un software di riconoscimento facciale, scansione di un'impronta digitale, dell'iride o della retina.

Non è vietato trattare dati personali degni di particolare protezione, ma le regole per il trattamento sono più severe che in altri casi: ad esempio requisiti più elevati in materia di consenso (art. 6 cpv. 7 lett. a LPD), una base legale in una legge formale per gli organi federali (art. 34 cpv. 2 lett. a e 36 cpv. 1 LPD) o l'obbligo generalizzato di valutare l'impatto sulla protezione dei dati nel caso di trattamenti su grande scala (art. 22 cpv. 2 lett. a LPD).

Rimandi: messaggio LPD, FF 2017 5939 pag. 6011; nota UFG/LPD, pag. 10 seg.

2.1.3 **Domanda**: *tutti i dati genetici sono dati personali degni di particolare protezione?*

Come il diritto previgente, anche la LPD sottoposta a revisione totale contempla soltanto i dati riferiti a una persona fisica identificata o identificabile (art. 5 lett. a LPD; cfr. domanda 2.1.1). Significa che i dati genetici sono degni di particolare protezione soltanto se contengono informazioni che permettono d'identificare l'interessato senza sforzi particolari, altrimenti non rientrano nel campo d'applicazione della LPD. La legge non si applica nemmeno ai dati anonimizzati se non consentono a terzi di risalire agli interessati.

Rimandi: Boll. uff. 2019 N 1787 (intervento del Capodipartimento DFGP nel dibattito del 24 settembre 2019 sulla revisione totale della LPD al Consiglio nazionale).

2.2 Trattamento di dati

2.2.1 **Domanda**: *cosa s'intende per «trattamento» di dati personali?*

Secondo l'articolo 5 lettera d LPD, il «trattamento» comprende qualsiasi operazione relativa a dati personali, indipendentemente dai mezzi e dalle procedure impiegati, segnatamente la raccolta, la registrazione, la conservazione, l'utilizzazione, la modificazione, la comunicazione,

[1] DTF 143 IV 193 consid. 2.3.

[2] Esempi tratti da FABIENNE ZANNOL, L'applicazione della norma penale contro la discriminazione razziale (studio commissionato dalla CFR), Berna 2007.

l'archiviazione, la cancellazione o la distruzione di dati. Il termine, tecnologicamente neutro, comprende sia il trattamento automatizzato dei dati sia quello non automatizzato (manuale).

Rimandi: messaggio LPD, FF 2017 5939 pag. 6012.

2.2.2 **Domanda**: *cosa s'intende per trattamento «automatizzato» dei dati?*

Il concetto non è definito nella legge, ma figura esplicitamente in svariate disposizioni della LPD e dell'OPDa (p. es. art. 5 lett. f LPD [profilazione], art. 28 [diritto alla consegna o trasmissione dei dati], art. 35 LPD [sistemi pilota], art. 4 cpv. 1 e 2 OPDa [verbalizzazione], art. 5 e 6 OPDa [regolamento per il trattamento]). In tali contesti il trattamento automatizzato si contrappone a quello manuale (ossia analogico) dei dati (p. es. appunti scritti a mano nel corso di un colloquio di assunzione) e comprende ogni trattamento effettuato in via elettronica (p. es. con l'ausilio di computer, smartphone, tablet o camere). Non occorre per contro che il trattamento sia completamente automatizzato – ovvero non richieda alcun intervento umano – come prevede il concetto di decisione individuale automatizzata dell'articolo 21 LPD (cfr. in merito la domanda 6.2.1).

2.3 Profilazione

2.3.1 **Domanda***: cosa s'intende per «profilazione»?*

La LPD sottoposta a revisione totale introduce il concetto di «profilazione» (art. 5 lett. f LPD) in sostituzione di quello di «profilo della personalità» (art. 3 lett. d vLPD). Anche se sono simili, le due nozioni non coincidono. Il profilo della personalità è il risultato di un trattamento (= elenco di dati che traccia un quadro degli aspetti [parziali] fondamentali di una persona), riflettendo quindi una situazione statica. La profilazione è invece un metodo di trattamento dei dati (= valutazione automatizzata di determinati aspetti di una persona) e pertanto costituisce un processo dinamico.

Secondo la definizione dell'articolo 5 lettera f LPD, la profilazione racchiude qualsiasi trattamento automatizzato di dati personali consistente nell'utilizzarli per valutare determinati aspetti individuali di una persona fisica. Significa analizzarne o prevederne il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, i luoghi di permanenza e gli spostamenti. In poche parole, la profilazione è un metodo per inquadrare o valutare una persona, ad esempio analizzando le sue caratteristiche personali, ma anche anticipandone comportamenti e peculiarità.

L'accertamento oggettivo dei fatti non costituisce profilazione. Anche classificare le persone in funzione di caratteristiche note come età, sesso e altezza non costituisce profilazione purché non vengano formulate previsioni o tratte conclusioni in merito a determinati individui.

Nella profilazione il trattamento dei dati, e in particolare il processo di valutazione, è automatizzato. Tuttavia, a differenza della decisione individuale automatizzata (cfr. domanda 6.2.1), la profilazione non implica per forza un trattamento del tutto automatizzato. L'intervento di una persona fisica non esclude che si tratti di una profilazione, a condizione che la parte essenziale del trattamento dei dati sia automatizzata.

Esempi[3]

- *Analisi della situazione economica o del merito creditizio*: il *credit scoring* è un metodo statistico per valutare il merito creditizio (solvibilità e affidabilità nei pagamenti) di una persona; prende ad esempio in considerazione informazioni riguardanti esecuzioni, attestati carenza beni, carte bancarie o di credito bloccate per morosità,

[3] Esempi tratti da Olivier Heuberger, Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz, diss. Lucerna, 2020 (n. marg. 157 segg.).

domande di credito, procedure di pagamento e d'incasso o esperienze fatte nelle relazioni d'affari precedenti. Alla persona valutata è assegnato un punteggio, utilizzato ad esempio per decidere sulla concessione di un prestito o le modalità di pagamento (acquisto dietro fattura). Il *credit scoring* automatizzato (e non manuale) costituisce profilazione.

- *Analisi dello stato di salute*: se un tracker di attività si limita a contare i passi, in linea di massima non si ha ancora un'analisi dello stato di salute di una persona e quindi non si tratta di profilazione. Se però ai passi contati vanno ad aggiungersi altri dati, come ad esempio altezza, peso, sesso, comportamento alimentare, ritmo del sonno o dati GPS, è possibile trarre conclusioni sullo stato di salute. Una tale analisi (automatizzata) dello stato di salute costituisce profilazione.

Rimandi: messaggio LPD, FF 2017 5939 pag. 6013 seg.; nota UFG/LPD, pag. 12 segg.

2.3.2 **Domanda**: *quando si ha una «profilazione a rischio elevato»?*

Il concetto è stato introdotto durante i dibattimenti parlamentari sulla revisione totale della LPD. Il Parlamento ha optato per un approccio basato sul rischio, imponendo ai titolari privati del trattamento di dati regole più severe soltanto per la «profilazione a rischio elevato» e non per ogni profilazione. La distinzione tra profilazione «ordinaria» e profilazione a rischio elevato è meno rilevante invece per gli organi federali (cfr. in merito la domanda 2.3.3)

È considerata «profilazione a rischio elevato» secondo l'articolo 5 lettera g LPD quella che «comporta un rischio elevato per la personalità o i diritti fondamentali della persona interessata, poiché collega dati in modo tale da permettere di valutare aspetti essenziali della personalità di una persona fisica». La definizione di rischio elevato dell'articolo 5 lettera g LPD s'ispira all'attuale concetto di «profilo della personalità» secondo l'articolo 3 lettera d vLPD. Resta pertanto determinante anche la giurisprudenza riguardo ai profili della personalità (in particolare la sentenza di principio del Tribunale amministrativo federale A-4232/2015 del 18 aprile 2017).

In altre parole, si è in presenza di una profilazione a rischio elevato se ne risulta un profilo della personalità ai sensi della precedente legge sulla protezione dei dati, ottenuto appunto combinando metodo (profilazione) e risultato (profilo della personalità) del trattamento dei dati. Tale definizione legale tiene conto del fatto che dal collegamento di una moltitudine di dati (anche non particolarmente degni di protezione) risulta un'immagine complessiva dell'interessato che implica di per sé un rischio elevato per la personalità e i diritti fondamentali. Spesso l'interessato non ha alcun influsso su questa immagine e non può controllarne né l'esattezza né l'uso.

Esempi

- Il GPS integrato consente in linea di massima di localizzare ogni smartphone con una precisione di pochi metri. È poi possibile analizzare in automatico questi dati sugli spostamenti per trarre conclusioni in merito al detentore. Se l'analisi si limita a un periodo circoscritto e a un luogo determinato (p. es. breve sosta in una stazione ferroviaria), si ha di norma e regola soltanto una profilazione «ordinaria». Se invece i dati sugli spostamenti sono analizzati per periodi prolungati e uno spazio geografico più ampio, è possibile dedurre informazioni in merito a svariati ambiti della vita di una persona, come ad esempio il luogo di lavoro, la situazione abitativa, le abitudini alimentari, le relazioni personali, eventuali visite mediche e le abitudini di consumo. Ne risulta un'immagine individuale che richiede particolare protezione. Si tratta verosimilmente di una profilazione a rischio elevato.
- Una profilazione per verificare il merito creditizio che non considera soltanto la situazione economica o la solvibilità di una persona, ma anche altri aspetti (come la situazione abitativa o personale) è da considerarsi a rischio elevato (cfr. nel diritto previgente la sentenza TAF A-4232/2015 del 18 aprile 2017).

All'atto pratico una profilazione può compromettere gravemente la personalità o i diritti fondamentali degli interessati anche per altri motivi, ad esempio se la profilazione verte su minorenni o altre persone vulnerabili o se rischia di precludere una prestazione importante. Di

tali rischi va ad esempio tenuto conto anche nel valutare l'impatto sulla protezione dei dati secondo l'articolo 22 LPD (cfr. domanda 6.3.2).

Rimandi: nota UFG/LPD, pag. 15 seg.

2.3.3 **Domanda**: *quali sono le regole applicabili alla profilazione (a rischio elevato)?*

Rispetto ad altri trattamenti di dati, la profilazione a rischio elevato impone regole più severe ai responsabili privati, tenuti ad esempio ad applicare requisiti più elevati per il consenso (art. 6 cpv. 7 lett. b LPD) e a valutare sempre l'impatto sulla protezione dei dati (cfr. art. 22 cpv. 1 e 2 LPD; domanda 6.3.2). Agli organi federali invece si applicano regole più severe anche per la profilazione «ordinaria»: in linea di massima sono autorizzati a effettuare una profilazione soltanto se lo prevede una base legale formale (art. 34 cpv. 2 lett. b LPD).

2.3.4 **Domanda**: *i responsabili privati necessitano sempre di un consenso per procedere a una profilazione? E cosa vale per gli organi federali?*

Alla stregua di ogni altro trattamento di dati, la profilazione da parte di *responsabili privati* è in linea di massima consentita, purché non leda illecitamente la personalità degli interessati (art. 30 cpv. 1 LPD). La profilazione non fa infatti parte dei trattamenti che la legge definisce di per sé lesivi della personalità (art. 30 cpv. 2 LPD e contrario). Se, però, nel caso specifico la profilazione lede la personalità, in quanto pregiudica con una certa intensità i diritti della personalità dell'interessato, la lesione può essere giustificata dal consenso, da un interesse preponderante privato o pubblico oppure dalla legge (art. 31 cpv. 1 LPD). Pertanto anche una profilazione lesiva della personalità non richiede sempre il consenso, ma può giustificarsi per uno degli altri motivi citati. È considerato un motivo giustificativo in particolare anche un interesse preponderante privato o pubblico (cfr. anche l'art. 31 cpv. 2 LPD). Si potrebbe, ad esempio, addurre la lotta antifrode come legittimo interesse, se nello specifico prevale sugli interessi contrapposti dell'interessato.

Il consenso dell'interessato a giustificazione di una profilazione lesiva della personalità deve adempire i requisiti dell'articolo 6 capoverso LPD oppure, in presenza di un rischio elevato, quelli dell'articolo 6 capoverso 7 (cfr. in merito la domanda 3.4.2).

A differenza dei privati, gli *organi federali*, vincolati al principio della legalità, possono trattare dati personali soltanto se esiste una base legale (art. 34 cpv. 1 LPD), che per una profilazione deve addirittura figurare in una legge formale (art. 34 cpv. 2 lett. b LPD). In assenza di una base legale per il trattamento dei dati o la profilazione, la LPD prevede una serie di deroghe, tra cui anche il consenso dell'interessato per il caso specifico (art. 34 cpv. 4 lett. b LPD). Per il trattamento dei dati da parte di organi federali il consenso è quindi nettamente meno rilevante rispetto al settore privato. Se infatti il trattamento è frequente o continuo, il consenso dell'interessato non è un motivo giustificativo sufficiente, ma occorre piuttosto creare le necessarie basi legali.

3. Principi applicabili (selezione)

3.1 Principio della trasparenza e delle riconoscibilità

Domanda: *cosa s'intende per principio della trasparenza e della riconoscibilità?*

Il principio della trasparenza e della riconoscibilità si evince dall'articolo 6 capoverso 3 LPD. La disposizione, seppur leggermente riformulata rispetto alla versione precedente (art. 4 cpv. 4 vLPD), non introduce nessuna modifica materiale, come illustra il messaggio del Consiglio federale sulla revisione totale della LPD. La raccolta di dati personali e in particolare lo scopo

del trattamento devono essere riconoscibili per l'interessato, il che è in linea di principio il caso quando l'interessato viene informato o quando il trattamento è previsto da una legge o chiaramente evincibile dalle circostanze.

Rimandi: messaggio LPD, FF 2017 5939 pag. 6016 seg.

3.2 Principio della finalità

Domanda: *cosa s'intende per principio della finalità?*

L'articolo 6 capoverso 3 LPD contiene una formulazione leggermente diversa rispetto al diritto precedente (art. 4 cpv. 3 vLPD), esplicitando in particolare che i dati personali possono essere trattati soltanto in modo compatibile con lo scopo iniziale per il quale sono stati raccolti. Il nuovo tenore non implica tuttavia modifiche sostanziali: come nel diritto vigente, un ulteriore trattamento viola il principio della finalità se l'interessato può legittimamente considerarlo inatteso, inappropriato o contestabile.

Esempi

- Non è conforme allo scopo iniziale utilizzare a fini pubblicitari indirizzi ottenuti in occasione della raccolta di firme per una campagna politica.
- Per contro, se l'interessato trasmette il suo indirizzo a un'impresa per ottenere una carta cliente o per ordinare qualcosa, l'ulteriore utilizzazione dell'indirizzo a fini commerciali da parte dell'impresa stessa va considerata una finalità inizialmente riconoscibile e quindi compatibile con le finalità iniziali[4].

È ammesso modificare lo scopo iniziale se previsto dalla legge, richiesto da una modifica legislativa o legittimato da un altro motivo giustificativo (p. es. il consenso dell'interessato).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6017.

3.3 Principio dell'esattezza

Domanda: *cosa implica il principio dell'esattezza dei dati?*

Chiunque tratti dati personali deve accertarsi della loro esattezza (art. 6 cpv. 5 primo periodo LPD). Deve prendere tutte le misure necessarie per rettificare, cancellare o distruggere i dati inesatti o incompleti rispetto alle finalità per le quali sono stati raccolti o trattati (art. 6 cpv. 5 secondo periodo LPD). Nell'articolo 6 capoverso 5 terzo periodo LPD il Parlamento ha tenuto a precisare che l'adeguatezza delle misure dipende segnatamente dal tipo e dall'entità del trattamento dei dati come pure dai rischi che ne derivano per la personalità o i diritti fondamentali dell'interessato. L'aggiunta sancisce esplicitamente nella legge la dottrina e la prassi (in particolare del Tribunale amministrativo federale) in materia di esattezza dei dati personali, pur non comportando cambiamenti in termini materiali.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6016 seg.

3.4 Consenso

3.4.1 **Domanda**: *occorre il consenso dell'interessato per trattare dati personali?*

In linea di massima i *responsabili privati* possono trattare dati personali senza il consenso dell'interessato. Il consenso è necessario soltanto se serve a giustificare un trattamento di dati lesivo della personalità (art. 30 seg. LPD), ad esempio per la comunicazione a terzi di dati

[4] Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Berna 2011, N 731.

personali degni di particolare protezione (p. es. relativi alla salute; cfr. domanda 2.1.2; art. 30 cpv. 2 lett. c LPD). L'eventuale consenso deve soddisfare i requisiti dell'articolo 6 capoversi 6 e 7 LPD (cfr. domanda 3.4.2). Se il consenso dell'interessato non può essere chiesto, non è valido o viene revocato, il trattamento lesivo della personalità non è automaticamente illecito. È infatti possibile far valere gli altri motivi giustificativi, ossia una base legale oppure un interesse preponderante privato o pubblico.

Il consenso riveste un'importanza minore per il trattamento di dati da parte di *organi pubblici* rispetto al trattamento da parte di privati. Nel settore pubblico importa soprattutto il requisito della base legale (art. 34 segg. LPD), mentre il consenso è utilizzato soltanto a titolo eccezionale e in casi specifici (art. 34 cpv. 4 lett. b e 36 cpv. 2 lett. b LPD).

In merito all'importanza del consenso per la profilazione cfr. domanda 2.3.4.

3.4.2 **Domanda**: *quali sono i requisiti relativi al consenso?*

Se il trattamento di dati personali è subordinato al consenso dell'interessato (cfr. in merito la domanda 3.4.1), il consenso è valido soltanto se, dopo debita informazione, è espresso liberamente e in modo inequivocabile in riferimento a uno o più trattamenti specifici (art. 6 cpv. 6 LPD). Lo stralcio da parte del Parlamento della «inequivocabilità» del consenso, prevista nel disegno del Consiglio federale, non implica alcun cambiamento materiale, dal momento che i principi generali stessi dell'ordinamento giuridico svizzero richiedono che un consenso sia sufficientemente definito.

L'articolo 6 capoverso 7 LPD disciplina le situazioni in cui il consenso – sempre che sia necessario – deve soddisfare requisiti più elevati: in sostanza occorre un «espresso» consenso per trattare dati personali degni di particolare protezione (lett. a) e per effettuare una profilazione a rischio elevato da parte di privati (lett. b) o una profilazione da parte di un organo federale (lett. c). In linea di massima l'espresso consenso è quello attivo e non soltanto tacito o concludente: deve fare immediata chiarezza sulla volontà dell'interessato.

Esempi

- Il consenso espresso comprende ad esempio le dichiarazioni orali o scritte, ma anche espliciti cenni col capo o con la mano oppure, nel contesto di Internet, la spunta attiva di una casella.
- Non è per contro considerato espresso un consenso concludente, come ad esempio continuare a utilizzare un servizio dopo che sono state modificate – avvisando il cliente – le condizioni generali.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6019 seg.

3.4.3 **Domanda**: *la nuova legge sulla protezione dei dati prevede un divieto di pratiche di vendita aggregata?*

L'UE ha sancito il cosiddetto «divieto di pratiche di vendita aggregata» nell'articolo 7 paragrafo 4 del Regolamento generale sulla protezione dei dati (cfr. domanda 12.2.1). Significa che: se un contratto è subordinato al consenso a un trattamento di dati non necessario per il suo adempimento, il consenso è in linea di massima considerato imposto e quindi nullo.

A differenza della normativa europea, la LPD non contempla un esplicito divieto di pratiche di vendita aggregate. Anche il diritto svizzero in materia di protezione dei dati impone tuttavia che il consenso sia «dato in modo libero». Il consenso è considerato imposto in particolare quando il rifiuto comporta svantaggi sproporzionati non correlati allo scopo del trattamento, il che di per sé è in linea con l'orientamento strategico del divieto di pratiche di vendita aggregate. Anche in

Svizzera le relative fattispecie vanno esaminate con particolare cura e rigore quando si tratta di giudicare il carattere volontario di un consenso.

Rimandi: DTF 138 I 331 consid. 7.4.1.

3.5 Protezione dei dati fin dalla progettazione e per impostazione predefinita

Domanda: *cosa s'intende per protezione dei dati fin dalla progettazione e per impostazione predefinita (risp. «privacy by design» e «privacy by default»)?*

La protezione dei dati fin dalla progettazione («*privacy by design*»; art. 7 cpv. 1 e 2 LPD) impone al titolare d'impostare il trattamento dei dati sin dalla progettazione in modo che sia conforme alle disposizioni sulla protezione dei dati. In altre parole: sul piano tecnico i requisiti per un trattamento dei dati conforme alla legge sono implementati in modo tale da ridurre o escludere il rischio di violazioni delle disposizioni in materia.

Esempio: un'applicazione è impostata in modo da eliminare periodicamente i dati o da anonimizzarli di default.

I titolari sono inoltre tenuti a garantire, mediante appropriate impostazioni predefinite («*privacy by default*»; art. 7 cpv. 3 LPD), che il trattamento di dati personali sia circoscritto al minimo indispensabile per lo scopo perseguito, salvo che l'interessato disponga altrimenti.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6019 segg.

3.6 Sicurezza dei dati

3.6.1 Aspetti generali

3.6.1.1 **Domanda**: *cosa s'intende per violazione della sicurezza dei dati?*

L'articolo 8 capoverso 1 LPD impone al titolare e al responsabile del trattamento di garantire, mediante appropriati provvedimenti tecnici e organizzativi, che la sicurezza dei dati personali sia adeguata al rischio. I provvedimenti devono permettere di evitare violazioni della sicurezza dei dati (art. 8 cpv. 2 LPD).

Il concetto di violazione della sicurezza dei dati è definito all'articolo 5 lettera h LPD: consiste in una «violazione della sicurezza in seguito alla quale, in modo accidentale o illecito, dati personali vengono persi, cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate». Ai fini della violazione è determinante solo e soltanto la presenza di una tale lacuna di sicurezza; è del tutto irrilevante che fosse semplicemente possibile divulgare i dati o renderli accessibili a persone non autorizzate o che ciò sia effettivamente accaduto.

In merito all'obbligo di notificare le violazioni della sicurezza dei dati cfr. le domande al numero 6.4.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6014 seg. e 6021.

3.6.1.2 **Domanda**: *cosa devono fare il titolare e il responsabile del trattamento per garantire un'adeguata sicurezza dei dati?*

Fondandosi sull'articolo 8 capoverso 3 LPD, il Consiglio federale ha fissato nell'ordinanza i requisiti minimi in materia di sicurezza dei dati (art. 1–6 OPDa):

In linea di massima il titolare e il responsabile del trattamento devono garantire un'adeguata sicurezza dei dati, definendo la *necessità di protezione dei dati personali* e stabilendo *provvedimenti tecnici e organizzativi* adeguati in considerazione del *rischio* (art. 1 cpv. 1 OPDa).

- Per determinare la *necessità di protezione*, vanno valutati il tipo di dati trattati, nonché scopo, tipo, portata e circostanze del trattamento (art. 1 cpv. 2 OPDa).
- Per determinare il *rischio per la personalità o i diritti fondamentali degli interessati*, vanno considerati le cause del rischio, il pericolo sostanziale, i provvedimenti adottati o previsti nonché la probabilità e la gravità di una violazione della sicurezza dei dati nonostante i provvedimenti adottati o previsti (art. 1 cpv. 3 OPDa).
- Nello *stabilire i provvedimenti tecnici e organizzativi* da adottare va inoltre tenuto conto dello stato della tecnica e delle spese d'implementazione (art. 1 cpv. 4 OPDa).

L'articolo 2 OPDa indica gli obiettivi perseguiti con i provvedimenti tecnici e organizzativi a garanzia della sicurezza dei dati. In funzione della necessità di protezione, i dati trattati dal titolare e dal responsabile devono essere:

- accessibili solo alle persone autorizzate (*confidenzialità*);
- disponibili quando necessario (*disponibilità*);
- non modificabili indebitamente o inavvertitamente (*integrità*); nonché
- trattati in modo tracciabile (*tracciabilità*).

L'articolo 3 OPDa elenca una serie di misure tese a realizzare gli obiettivi dell'articolo 2 OPDa.

In merito alla verbalizzazione di cui all'articolo 4 OPDa, cfr. le domande al numero 3.6.2.

In merito al regolamento sul trattamento di cui all'articolo 5 OPDa, cfr. le domande al numero 3.6.3.

Rimandi: rapporto esplicativo del 31 agosto 2022 dell'Ufficio federale di giustizia in merito all'ordinanza sulla protezione dei dati (qui di seguito: «rapporto esplicativo alla OPDa»), pag. 17 segg.

3.6.2 Verbalizzazione

3.6.2.1 **Domanda**: *qual è lo scopo dell'obbligo di verbalizzazione?*

La verbalizzazione è un provvedimento per garantire la sicurezza dei dati ai sensi dell'articolo 3 OPDa. Costituisce inoltre uno strumento preventivo classico per salvaguardare la cibersicurezza.

Lo scopo è permettere la verifica a posteriori del trattamento di dati personali. In altre parole, dev'essere possibile constatare in un secondo tempo se sono stati smarriti, cancellati, distrutti, modificati, comunicati o resi accessibili dati personali. La verbalizzazione può inoltre fornire indicazioni sulla conformità allo scopo e servire a individuare e chiarire violazioni della sicurezza dei dati (cfr. domanda 3.6.1.1). *Non* mira invece a sorvegliare gli utenti che trattano dati personali.

Rimandi: rapporto esplicativo alla OPDa, pag. 25 segg.

3.6.2.2 **Domanda**: *in quali casi i privati devono verbalizzare i trattamenti effettuati?*

I privati titolari e responsabili del trattamento devono verbalizzare almeno la registrazione, modificazione, lettura, comunicazione, cancellazione e distruzione dei dati quando trattano dati

personali degni di particolare protezione (cfr. domanda 2.1.2) su grande scala (cfr. domanda 3.6.2.3) in automatico (cfr. domanda 2.2.2) oppure effettuano una profilazione a rischio elevato (cfr. domanda 2.3.2) e i provvedimenti preventivi non possono garantire la protezione dei dati (art. 4 cpv. 1 primo periodo OPDa). La verbalizzazione è imperativa in particolare quando non è possibile stabilire a posteriori se i dati sono stati trattati ai fini per i quali sono stati raccolti o comunicati (art. 4 cpv. 1 secondo periodo LPD).

Rimandi: rapporto esplicativo alla OPDa, pag. 25.

3.6.2.3 **Domanda**: *cosa s'intende per trattamento «su grande scala» di dati personali degni di particolare protezione?*

L'espressione «su grande scala» dell'articolo 4 capoverso 1 OPDa (e in altre disposizioni come p. es. l'art. 22 cpv. 2 lett. a LPD [Valutazione d'impatto sulla protezione dei dati] o l'art. 5 cpv. 1 lett. a OPDa [Regolamento dei privati sul trattamento] e l'art. 24 lett. a OPDa [Eccezione all'obbligo di tenere un registro delle attività di trattamento]) si riferisce alle situazioni in cui i dati personali degni di particolare protezione non sono trattati solo sporadicamente. Rientra ad esempio in tale definizione il trattamento di dati dei pazienti da parte di uno studio medico o di un ospedale, ma non il trattamento sporadico, da parte di un'impresa, dei dati riguardanti le assenze per malattia dei collaboratori. Il trattamento di dati personali degni di particolare protezione è considerato su grande scala in particolare se costituisce l'attività principale della persona o del servizio che tratta i dati.

3.6.2.4 **Domanda**: *in quali casi gli organi federali devono verbalizzare i trattamenti effettuati?*

Gli organi federali titolari e responsabili del trattamento verbalizzano almeno la registrazione, modificazione, lettura, comunicazione, cancellazione e distruzione dei dati (art. 4 cpv. 2 OPDa) quando trattano dati personali in automatico (cfr. domanda 2.2.2). Sono le stesse operazioni che devono essere verbalizzate anche dai titolari privati del trattamento (cfr. domanda 3.6.2.2). Il campo d'applicazione è però più ampio: l'obbligo di verbalizzazione si applica a prescindere dall'oggetto del trattamento, non importa quindi se i dati personali sono o no degni di particolare protezione o se la profilazione è a rischio elevato o meno. In questo modo si tiene conto dei requisiti dell'articolo 25 del Regolamento generale sulla protezione dei dati (cfr. domanda 12.1). Per i trattamenti di dati che non rientrano nel campo d'applicazione della direttiva (UE) 2016/680, l'articolo 46 capoverso 1 OPDa prevede un periodo transitorio di tre anni dall'entrata in vigore dell'ordinanza o al più tardi alla fine del ciclo di vita del sistema. Durante il periodo di transizione si applicano le regole per titolari privati dell'articolo 4 capoverso 1 OPDa.

Rimandi: rapporto esplicativo alla OPDa, pag. 26 e 57.

3.6.2.5 **Domanda**: *quali regole si applicano ai dati personali accessibili al pubblico in modo generalizzato?*

Per i dati personali accessibili al pubblico in modo generalizzato, l'articolo 4 capoverso 3 OPDa prevede che siano verbalizzati almeno la registrazione, modificazione, cancellazione e distruzione dei dati, ma *non* la lettura e la comunicazione.

Esempio: la consultazione o lettura dell'Annuario federale, pubblicamente accessibile, non va per forza verbalizzata.

Rimandi: rapporto esplicativo alla OPDa, pag. 26.

3.6.2.6 **Domanda**: *cosa va verbalizzato?*

I verbali devono riportare informazioni sull'identità della persona che ha effettuato il trattamento, sul tipo, la data e l'ora del trattamento nonché, all'occorrenza, sull'identità del destinatario dei dati (art. 4 cpv. 4 OPDa).

Rimandi: rapporto esplicativo alla OPDa, pag. 26.

3.6.2.7 **Domanda**: *per quanto e in che modo vanno conservati i verbali?*

Vanno conservati per almeno un anno separatamente dal sistema in cui i dati personali sono trattati (art. 4 cpv. 5 primo periodo OPDa). Sono fatte salve disposizioni di legge speciali (p. es. l'art. 4 cpv. 1 lett. b dell'ordinanza sul trattamento di dati personali derivanti dall'utilizzazione dell'infrastruttura elettronica della Confederazione; RS 172.010.442). La durata di conservazione deve sempre essere proporzionata agli obiettivi della sicurezza dei dati. La conservazione separata dal sistema è necessaria per evitare la manipolazione o la criptazione dei verbali in caso di ciberattacco.

Possono inoltre accedere ai verbali soltanto gli organi e gli individui incaricati di verificare l'applicazione delle disposizioni in materia di protezione dei dati o di salvaguardare o ripristinare la confidenzialità, l'integrità, la disponibilità e la tracciabilità dei dati (ne fanno p. es. parte anche gli addetti alla sicurezza e gli amministratori di sistema se sospettano una falla nella sicurezza). I verbali possono essere utilizzati esclusivamente a tale fine (art. 4 cpv. 5 secondo periodo OPDa); non è ammesso servirsene per sorvegliare gli utenti. È fatto salvo l'utilizzo per scopi previsti da leggi speciali, ad esempio in un procedimento penale.

Rimandi: rapporto esplicativo alla OPDa, pag. 26 seg.

3.6.3 Regolamento per il trattamento

3.6.3.1 **Domanda**: *quando i privati titolari o responsabili del trattamento devono stilare un regolamento?*

L'articolo 5 capoverso 1 OPDa prevede che il privato titolare o responsabile stabilisca un regolamento per i trattamenti automatizzati se tratta dati personali degni di particolare protezione su grande scala (cfr. domanda 3.6.2.3) o esegue una profilazione a rischio elevato (cfr. domanda 2.3.2).

Rimandi: rapporto esplicativo alla OPDa, pag. 27 seg.

3.6.3.2 **Domanda**: *quando gli organi federali devono stilare un regolamento per il trattamento?*

Secondo l'articolo 6 capoverso 1 OPDa, l'organo federale titolare del trattamento e il suo responsabile sono tenuti a stabilire un regolamento per i trattamenti automatizzati se trattano dati personali degni di particolare protezione (lett. a; cfr. domanda 2.1.2); effettuano una profilazione (lett. b; cfr. domanda 2.3.1); lo scopo o il tipo di trattamento può comportare una grave ingerenza nei diritti fondamentali dell'interessato (lett. c); concedono l'accesso a dati personali a Cantoni, autorità estere, organizzazioni internazionali o privati (lett. d); connettono tra loro raccolte di dati (lett. e) oppure gestiscono insieme ad altri organi federali un sistema d'informazione o raccolte di dati (lett. f).

Rimandi: rapporto esplicativo alla OPDa, pag. 28 seg.

3.6.3.3 **Domanda**: *cosa deve contenere il regolamento per il trattamento?*

Deve illustrare in particolare l'organizzazione interna (p. es. descrizione dell'architettura di sistema), la procedura di trattamento e di controllo dei dati (p. es. per la minimizzazione dei dati, la comunicazione dei dati e l'esercizio del diritto d'accesso e del diritto alla consegna o alla trasmissione dei dati) nonché i provvedimenti per garantire la sicurezza dei dati (art. 5 cpv. 2 e 6 cpv. 2 OPDa). Il regolamento va aggiornato a intervalli regolari e messo a disposizione del consulente per la protezione dei dati (nel settore privato: se ne è stato designato uno; art. 5 cpv. 3 e 6 cpv. 3 OPDa; cfr. le domande al n. 3.7).

Il regolamento va impostato come finora sotto forma di documentazione o di manuale.

Rimandi: rapporto esplicativo alla OPDa, pag. 27 segg.

3.6.3.4 **Domanda**: *qual è la differenza tra il regolamento di cui all'articolo 5 seg. OPDa e il registro delle attività di trattamento di cui all'articolo 12 LPD?*

Cfr. in merito la domanda 3.8.2.

3.7 Consulenti per la protezione dei dati

3.7.1 **Domanda**: *chi deve nominare un consulente per la protezione dei dati?*

I *titolari privati del trattamento* non sono tenuti a nominare un consulente per la protezione dei dati, ma possono farlo a titolo volontario (art. 10 cpv. 1 LPD), beneficiando – a determinate condizioni (cfr. in merito la domanda 3.7.3) – di un'agevolazione nel valutare l'impatto sulla protezione dei dati (esonero dal consultare l'IFPDT [cfr. in merito la domanda 6.3.3]; art. 10 cpv. 3 in combinato disposto con l'art. 23 cpv. 4 LPD).

Gli *organi federali* sono invece tenuti a nominare un consulente per la protezione dei dati (art. 10 cpv. 4 LPD in combinato disposto con l'art. 25 OPDa). Tuttavia, diversi organi federali possono designare un consulente congiunto; questo per permettere agli organi federali meno grandi o ai dipartimenti più centralizzati di sfruttare le sinergie ed economizzare le risorse.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6023 segg.; rapporto esplicativo alla OPDa, pag. 48.

3.7.2 **Domanda**: *quali sono i compiti del consulente per la protezione dei dati?*

I consulenti per la protezione dei dati contribuiscono all'applicazione delle norme in materia verificando, tra le altre cose, il trattamento di dati personali e raccomandando provvedimenti correttivi se constatano una violazione delle prescrizioni pertinenti. Formano e consigliano i collaboratori in materia di protezione dei dati (p. es. a valutare l'impatto sulla protezione dei dati; cfr. domanda 6.3.1). Inoltre fungono da interlocutori per le persone interessate da un trattamento di dati e le autorità competenti in materia (in particolare l'IFPDT; cfr. in merito per i privati l'art. 10 cpv. 2 LPD e per gli organi federali l'art. 10 cpv. 4 LPD in combinato disposto con gli art. 26 cpv. 2 e 28 OPDa). Il trattamento conforme alle norme di protezione dei dati non rientra nella responsabilità del consulente, ma esclusivamente in quella del titolare del trattamento.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6023 segg.; rapporto esplicativo alla OPDa, pag. 48 segg.

3.7.3 **Domanda**: *quali sono i requisiti richiesti a un consulente per la protezione dei dati?*

Nel caso degli *organi federali*, il consulente per la protezione dei dati deve disporre delle conoscenze tecniche necessarie ed esercitare la sua funzione in modo indipendente dall'organo

federale e senza ricevere da questi istruzioni (art. 26 cpv. 1 OPDa). Va insomma garantito che il consulente possa formulare liberamente le proprie raccomandazioni senza dover temere ripercussioni. Per tutelarne l'indipendenza vanno innanzitutto adottate misure organizzative affinché, tra le altre cose, l'attività di consulente non pregiudichi la valutazione annuale.

Se un *titolare privato del trattamento* desidera avvalersi di una valutazione d'impatto agevolata (esonero dal consultare l'IFPDT [cfr. in merito la domanda 6.3.3; art. 10 cpv. 3 in combinato disposto con l'art. 23 cpv. 4 LPD]), il suo consulente deve soddisfare gli stessi requisiti applicabili agli organi federali (art. 10 cpv. 3 lett. a e c LPD). Al consulente sono inoltre espressamente vietate attività inconciliabili con i suoi compiti (art. 10 cpv. 3 lett. b LPD), come ad esempio fare parte della direzione, esercitare funzioni di conduzione del personale o di gestione dei sistemi informatici oppure lavorare per un'unità che tratta dati personali degni di particolare protezione. È invece ipotizzabile affidare alla stessa persona le funzioni di consulente per la protezione dei dati e incaricato della sicurezza delle informazioni. I dati di contatto del consulente devono essere pubblicati e comunicati all'IFPDT (art. 10 cpv. 3 lett. d LPD).

Rimandi: messaggio LPD, FF 2017 5939, 6023 segg.; rapporto esplicativo alla OPDa, pag. 48 segg.

3.7.4 **Domanda**: *quali sono gli obblighi dei titolari del trattamento nei confronti dei consulenti per la protezione dei dati?*

Il consulente deve ricevere dagli *organi federali* tutti gli accessi alle informazioni, ai documenti, ai registri delle attività di trattamento (cfr. in merito la domanda 3.8.1) e ai dati personali di cui necessita per adempire i suoi compiti (art. 27 cpv. 1 lett. a OPDa). Sono fatte salve le disposizioni di leggi speciali contrarie a tale accesso. Gli organi federali devono inoltre provvedere – p. es. mediante istruzioni – a che il consulente sia informato di qualsiasi violazione della sicurezza dei dati (art. 27 cpv. 1 lett. b OPDa; cfr. in merito la domanda 3.6.1.1). Tale obbligo non comprende soltanto le violazioni da notificare all'IFPDT in base all'articolo 24 LPD, ma tutte le violazioni della sicurezza dei dati. Il consulente per la protezione dei dati consiglia l'organo federale per determinare se la violazione va notificata sensi dell'articolo 24 LPD (cfr. in merito le domande 6.4.2 e 6.4.5). La notifica stessa rientra tuttavia nella responsabilità dell'organo federale o delle persone che agiscono per suo conto: sono loro a decidere se e – casomai – quali violazioni notificare all'IFPDT. Infine l'organo federale deve pubblicare in Internet i dati di contatto del consulente e comunicarli all'IFPDT (art. 27 cpv. 2 OPDa). Per la pubblicazione in Internet è sufficiente segnalare l'indirizzo mail del servizio competente; non occorre indicare il consulente per nome.

Anche per i *titolari privati del trattamento* l'articolo 23 OPDa prevede vari obblighi: devono mettere a disposizione del consulente le risorse necessarie (lett. a); concedergli l'accesso a qualsiasi informazione, documento, registro delle attività di trattamento (cfr. in merito la domanda 3.8.1) e ai dati personali di cui necessita per adempire i suoi compiti (lett. b) e infine concedergli il diritto di informare i massimi organi dirigenti o amministrativi in casi importanti (lett. c).

Rimandi: rapporto esplicativo alla OPDa, pag. 46 e 49.

3.8 Registro delle attività di trattamento

3.8.1 **Domanda**: *cos'è il registro delle attività di trattamento?*

L'articolo 12 capoverso 1 LPD impone ai titolari e ai responsabili di tenere ognuno un registro delle rispettive attività di trattamento, contenente le informazioni essenziali in merito ai dati da loro trattati. Il registro, in poche parole, fornisce una panoramica delle attività di trattamento,

permettendo di ricavare informazioni importanti sulla conformità di un trattamento con i principi della protezione dei dati. *Non* è per contro un diario in cui trascrivere singoli dati o attività come fosse un verbale.

L'obbligo di tenere un registro delle attività di trattamento sostituisce il vecchio obbligo di notificare raccolte dati (art. 11*a* vLPD).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6026 segg.

3.8.2 **Domanda**: *qual è la differenza tra il registro delle attività di trattamento di cui all'articolo 12 LPD e il regolamento di cui all'articolo 5 seg. OPDa?*

Il regolamento per il trattamento (teso a garantire la sicurezza dei dati secondo l'art. 5 seg. OPDa; cfr. in merito le domande al n. 3.6.3) va distinto dal registro delle attività (art. 12 LPD). Mentre quest'ultimo è un elenco generale che offre una panoramica dei trattamenti di dati effettuati da un privato o un organo federale, il regolamento disciplina l'organizzazione interna (come p. es. l'architettura e la gestione dei sistemi d'informazione o la garanzia dei diritti degli interessati), le procedure di trattamento e di controllo dei dati (come p. es. i diritti d'accesso) e i provvedimenti (tecnici e organizzativi) per garantire la sicurezza dei dati (cfr. in merito la domanda 3.6.3.3).

3.8.3 **Domanda**: *cosa va inserito nel registro delle attività di trattamento?*

L'articolo 12 capoverso 2 LPD elenca le indicazioni minime richieste per il registro del titolare.

Ne fanno parte innanzitutto l'identità (nome o ditta e indirizzo) del titolare del trattamento (lett. a) e lo scopo del trattamento (lett. b). Vanno poi indicati per categoria gli interessati (p. es. «consumatori» o «lavoratori») e i dati trattati (p. es. «recapiti» o «dati per il pagamento»), oltre che i destinatari cui sono resi noti i dati personali (risp. lett. c e d). Anche in quest'ultimo caso s'intendono gruppi tipici con caratteristiche comuni, ad esempio le «autorità di sorveglianza», i «fornitori» oppure i «fornitori di servizi informatici». Per i destinatari all'estero la lettera g impone d'indicare anche i relativi Stati e le eventuali garanzie secondo l'articolo 16 capoverso 2 LPD (p. es. clausole contrattuali standard; cfr. domanda 5.3.2). Il registro deve contenere la durata di conservazione dei dati personali o almeno i criteri che ne determinano la durata se non sono possibili indicazioni precise (lett. e). La lettera f infine prevede che nel registro vadano descritti i provvedimenti tesi a garantire la sicurezza dei dati secondo l'articolo 8 LPD (cfr. in merito le domande al n. 3.6.) L'espressione «se possibile» chiarisce che la descrizione è richiesta soltanto se i provvedimenti possono essere illustrati in modo sufficientemente chiaro.

L'articolo 12 capoverso 3 LPD elenca le indicazioni minime richieste per il registro del responsabile del trattamento.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6026 segg.

3.8.4 **Domanda**: *il registro delle attività di trattamento va notificato all'IFPDT?*

Secondo l'articolo 12 capoverso 4, gli organi federali devono notificare i loro registri all'IFPDT, che gestisce un portale di notifica o tiene un registro pubblico delle attività di trattamento (art. 56 LPD; <https://datareg.edoeb.admin.ch/search>).

A differenza di quanto valeva finora, l'obbligo di notificare l'IFPDT non si applica ai *titolari privati* che, in ottemperanza del loro obbligo di collaborare nel quadro di un'inchiesta, sono tuttavia tenuti a presentare i registri su richiesta per permettere all'IFPDT di controllare il rispetto del diritto in materia di protezione dei dati (cfr. art. 49 cpv. 3 e 50 cpv. 1 lett. a LPD).

3.8.5 **Domanda**: *la videosorveglianza da parte di un organo federale è un'attività di trattamento da inserire nel registro e notificare all'IFPDT?*

L'obbligo di tenere un registro secondo l'articolo 12 LPD comprende tutte le attività di trattamento di un titolare o responsabile. Se pertanto le riprese permettono di riconoscere persone identificate o identificabili, anche la videosorveglianza da parte di organi federali rientra nel campo di applicazione della LPD ed è quindi soggetta alle norme sul registro delle attività di trattamento (fatte salve le deroghe previste da leggi speciali). Significa che all'IFPDT vanno ad esempio notificate le telecamere installate per sorvegliare l'entrata di un edificio federale.

3.8.6 **Domanda**: *esistono deroghe all'obbligo di tenere un registro delle attività di trattamento?*

L'articolo 12 capoverso 5 LPD in combinato disposto con l'articolo 24 OPDa prevede una deroga per le persone fisiche nonché le imprese e altre organizzazioni di diritto privato che al 1° gennaio di un anno impiegano meno di 250 collaboratori (a prescindere dal tasso di occupazione), esentandole dall'obbligo di tenere un registro delle attività di trattamento. Tale deroga non si applica però nei casi in cui (a) trattano dati personali degni di particolare protezione su grande scala (p. es. dati sulla salute; cfr. in merito la domanda 2.1.2) oppure (b) eseguono una profilazione a rischio elevato (cfr. in merito la domanda 2.3.2): per questi (e solo per questi) trattamenti va tenuto un registro delle attività.

In merito alla definizione di trattamento su grande scala di dati personali degni di particolare protezione cfr. n. 3.6.2.3.

I privati esentati dall'obbligo di tenere un registro delle attività sono ovviamente liberi di allestirne uno. È uno strumento utile e semplice che permette a chi tratta regolarmente dati personali di mantenere la visione d'insieme sulle attività di trattamento e di rispettare anche altri obblighi, come quello d'informare sulla raccolta di dati personali (cfr. domanda 6.1.1).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6026; rapporto esplicativo alla OPDa, pag. 48.

4. Obbligo di rappresentanza per titolari privati domiciliati all'estero

4.1 Condizioni

4.1.1 **Domanda**: *quali titolari stranieri devono designare un rappresentante in Svizzera?*

L'articolo 14 capoverso 1 LPD impone a taluni titolari stranieri di designare un rappresentante in Svizzera. Sono soggetti a tale obbligo i titolari privati domiciliati all'estero che trattano dati personali di persone in Svizzera (periodo introduttivo) effettuando trattamenti che presentano – tutte – le seguenti caratteristiche.

- Il trattamento è legato a un'*offerta di merci o prestazioni* o è finalizzato a *osservare il comportamento di persone in Svizzera* (lett. a): un esempio classico consiste nel commercio online quando il titolare propone la sua offerta in franchi svizzeri o prevede una consegna in Svizzera; non basta però che un sito o un indirizzo elettronico sia accessibile dalla Svizzera. Il comportamento di una persona in Svizzera risulta, ad esempio, osservato quando il titolare ne monitora l'attività in Internet; i destinatari di questa norma sono in particolare le reti sociali.
- È un *trattamento su grande scala* (lett. b; cfr. in merito la domanda 3.6.2.3).
- È un *trattamento periodico* (lett. c): rientra nella categoria, ad esempio, il commercio elettronico. Il trattamento è periodico anche quando i dati personali costituiscono per così dire

la «materia prima» di un'attività – come ad esempio nelle reti sociali. Non si ha invece trattamento periodico se i dati sono trattati soltanto occasionalmente o per periodi limitati.

- Il trattamento comporta *un rischio elevato per la personalità degli interessati* (lett. d): va accertato caso per caso se sussiste un tale rischio, che può risultare in particolare da quantità e tipo dei dati trattati (p. es. dati degni di particolare protezione), scopo e modalità del trattamento (p. es. nuove tecnologie), un'eventuale comunicazione dei dati all'estero e i diritti d'accesso (p. es. accesso conferito a un numero cospicuo se non addirittura illimitato di persone).

Verosimilmente l'obbligo di designare un rappresentante in Svizzera si applicherà in particolare alle grandi piattaforme Internet e alle reti sociali domiciliate all'estero.

Secondo l'articolo 14 capoverso 3 LPD il titolare straniero è tenuto a pubblicare nome e indirizzo del suo rappresentante, ad esempio sul proprio sito.

4.1.2 **Domanda**: *cosa succede se un titolare straniero non designa un rappresentante in Svizzera?*

L'IFPDT può disporre che un titolare straniero rientrante nei criteri dell'articolo 14 capoverso 1 LPD designi un rappresentante in Svizzera (art. 51 cpv. 4 LPD). Trattandosi di un documento ufficiale, la decisione dell'IFPDT va notificata per via diplomatica (a meno che un accordo internazionale preveda la notifica diretta). Insieme alla sua decisione, l'IFPDT può notificare al titolare straniero anche una comminatoria di pena per inosservanza (art. 63 LPD). L'eventuale multa disposta in seguito può essere eseguita soltanto in via rogatoria ossia tramite richiesta per canali diplomatici di assistenza all'esecuzione.

4.2 Compiti e obblighi del rappresentante

Domanda: *quali sono i compiti e gli obblighi del rappresentante in Svizzera?*

Il rappresentante funge da interlocutore svizzero per gli interessati e l'IFPDT (art. 14 cpv. 2 LPD), ma non è responsabile di eventuali violazioni della protezione dei dati da parte del responsabile del trattamento.

L'articolo 15 LPD prevede tre obblighi per il rappresentante:

- tiene un registro delle attività di trattamento del titolare (cpv. 1); il registro deve contenere le stesse indicazioni previste all'articolo 12 capoverso 2 LPD (cfr. domanda 3.8.3), essenzialmente una descrizione generale delle attività di trattamento. Il registro non contiene per contro dati personali;

- su richiesta, trasmette all'IFPDT tutte le indicazioni contenute nel registro (cpv. 2); l'IFPDT non può però chiedere al rappresentante informazioni o dati personali che si trovano all'estero, in quanto sarebbe problematico per la sovranità dello Stato estero. Se necessita di tali informazioni, l'IFPDT deve procurarsele attraverso i canali dell'assistenza giudiziaria;

- su richiesta, informa gli interessati su come esercitare i loro diritti (cpv. 3), fornendo ad esempio i recapiti del titolare o del suo consulente per la protezione dei dati. Sebbene il rappresentante funga da interlocutore per gli interessati, è il titolare a essere obbligato per legge a informarli sulla raccolta di dati personali (cfr. domanda 6.1.1). Anche il diritto d'accesso (cfr. domanda 7.2.1) può essere fatto valere unicamente nei confronti del titolare e non del suo rappresentante.

5. Comunicazione di dati personali all'estero

5.1 Panoramica

Domanda: *quando è ammesso comunicare dati personali all'estero?*

L'articolo 16 capoverso 1 LPD permette di comunicare dati personali all'estero se il Consiglio federale ha constatato che la legislazione dello Stato destinatario o dell'organo internazionale garantisce una protezione adeguata dei dati (cfr. n. 5.2).

In assenza di una valutazione dell' adeguatezza del Consiglio federale, i dati personali possono essere comunicati all'estero soltanto nei casi previsti dall'articolo 16 capoversi 2 e 3 LPD (elenco di garanzie per una protezione appropriata dei dati; cfr. n. 5.3) oppure dall'articolo 17 LPD (eccezioni; cfr. n. 5.4) .

Garantiscono una protezione appropriata dei dati:

- i trattati internazionali (art. 16 cpv. 2 lett. a LPD);
- le clausole contrattuali a protezione dei dati tra il titolare o il responsabile del trattamento e l'altro contraente, previamente comunicate all'IFPDT (art. 16 cpv. 2 lett. a LPD);
- le garanzie specifiche stabilite dall'organo federale competente, previamente comunicate all'IFPDT (art. 16 cpv. 2 lett. c LPD);
- le clausole tipo a protezione dei dati previamente approvate, stabilite o riconosciute dall'IFPDT (art. 16 cpv. 2 lett. d LPD);
- le norme aziendali vincolanti in materia di protezione dei dati («*Binding Corporate Rules*»), previamente approvate dall'IFPDT o da un'autorità competente in materia appartenente a uno Stato che garantisce una protezione adeguata (art. 16 cpv. 2 lett. e LPD);
- i codici di condotta e le certificazioni (art. 16 cpv. 3 LPD in combinato disposto con l'art. 12 OPDa).

Per la comunicazione di dati personali all'estero si vedano anche le informazioni e i documenti dell'IFPDT: <https://www.edoeb.admin.ch/edoeb/it/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html>.

5.2 Valutazione dell'adeguatezza del Consiglio federale

5.2.1 **Domanda**: *dove trovo gli Stati e gli organismi internazionali che garantiscono un'adeguata protezione dei dati?*

In virtù della nuova legge non sarà (più) l'IFPDT, ma il Consiglio federale a determinare gli Stati e gli organismi internazionali che garantiscono una protezione adeguata dei dati.

Stati, territori, determinati settori di uno Stato e organismi internazionali che il Consiglio federale ritiene dotati di una protezione adeguata dei dati sono elencati nell'allegato 1 all'OPDa e consultabili sul sito dell'UFG: <https://www.bj.admin.ch/bj/it/home/staat/datenschutz/internationales/anerkennung-staaten.html>.

5.2.2 **Domanda***: in base a quali criteri il Consiglio federale valuta se uno Stato o un organismo internazionale garantisce un'adeguata protezione dei dati?*

L'articolo 8 capoverso 2 OPDa stabilisce svariati criteri di cui il Consiglio federale deve tener particolare conto nel valutare l'adeguatezza, ossia:

- gli impegni internazionali dello Stato o dell'organismo internazionale, in particolare in materia di protezione dei dati (lett. a);
- lo Stato di diritto e il rispetto dei diritti dell'uomo (lett. b);
- la legislazione vigente in particolare in materia di protezione dei dati, la sua attuazione e la giurisprudenza pertinente (lett. c);
- l'effettiva garanzia dei diritti delle persone interessate e della tutela giurisdizionale (lett. d);
- l'effettivo funzionamento di una o più autorità indipendenti responsabili della protezione dei dati nello Stato in questione o preposte a un organismo internazionale e dotate di poteri e competenze sufficienti (lett. e).

L'IFPDT è consultato al momento di ogni valutazione. Inoltre possono essere presi in considerazione i pareri di organismi internazionali o autorità estere competenti per la protezione dei dati (art. 8 cpv. 3 OPDa).

L'adeguatezza della protezione dei dati è periodicamente oggetto di una nuova valutazione (art. 8 cpv. 4 LPD). Le valutazioni sono pubblicate (art. 8 cpv. 5 LPD) all'indirizzo seguente: <https://www.bj.admin.ch/bj/it/home/staat/datenschutz/internationales.html>.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6028 seg.; rapporto esplicativo alla OPDa, pag. 30 segg.

5.3 Garanzie d'un livello di protezione dei dati appropriata

5.3.1 **Domanda**: *quali sono i requisiti per le clausole contrattuali a protezione dei dati (art. 16 cpv. 2 lett. b LPD) e le garanzie specifiche (art. 16 cpv. 2 lett. c LPD)?*

In assenza di una valutazione dell'adeguatezza da parte del Consiglio federale (cfr. n. 5.2), la protezione appropriata dei dati nel settore privato può essere garantita da *clausole contrattuali a protezione dei dati* tra il titolare o il suo responsabile e l'altro contraente (art. 16 cpv. 2 lett. b LPD). L'analogia nel settore pubblico consiste nelle *garanzie specifiche* stabilite dall'organo federale competente (art. 16 cpv. 2 lett. c LPD).

A differenza delle clausole tipo a protezione dei dati (cfr. domanda 5.3.2), quelle contrattuali valgono solo per le comunicazioni di dati previste da tale contratto.

L'articolo 9 capoverso 1 OPDa definisce il contenuto minimo di tali clausole contrattuali e garanzie specifiche come segue:

- l'applicazione dei principi della liceità, della buona fede, della proporzionalità, della trasparenza, della finalità e dell'esattezza (lett. a);
- le categorie dei dati personali comunicati e degli interessati (lett. b);
- il tipo e lo scopo della comunicazione dei dati personali (lett. c);
- all'occorrenza, il nome degli Stati o degli organismi internazionali cui sono comunicati dati personali nonché i requisiti della comunicazione (lett. d);
- i requisiti della conservazione, della cancellazione e della distruzione di dati personali (lett. e);
- i destinatari o le categorie dei destinatari (lett. f);
- provvedimenti per garantire la sicurezza dei dati (lett. g; cfr. le domande al n. 3.6);
- l'obbligo di comunicare le violazioni della sicurezza dei dati (lett. h; cfr. le domande al n. 6.4);

- se i destinatari sono titolari del trattamento, l'obbligo di informare gli interessati (lett. i; cfr. le domande al n. 6.1);
- i diritti dell'interessato, segnatamente il diritto d'accesso e quello alla consegna o alla trasmissione dei dati, il diritto di opporsi alla comunicazione dei dati, il diritto di chiedere la rettifica, la cancellazione o la distruzione dei dati che la concernono, nonché il diritto di chiedere tutela giurisdizionale a un'autorità indipendente (lett. j; cfr. le domande al n. 7).

A differenza delle clausole tipo a protezione dei dati (cfr. domanda 5.3.2) o delle norme aziendali vincolanti in materia (cfr. domanda 5.3.3), le clausole contrattuali e le garanzie specifiche non vanno approvate dall'IFPDT. È sufficiente informarlo (prima di comunicare i dati; art. 16 cpv. 2 lett. b e c LPD e art. 9 cpv. 3 OPDa).

Il titolare del trattamento e (nel caso di clausole contrattuali) anche il suo responsabile devono adottare misure adeguate per garantire che il destinatario rispetti le clausole o le garanzie specifiche (art. 9 cpv. 2 OPDa).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6029 seg.; rapporto esplicativo alla OPDa, pag. 32 segg.

5.3.2 **Domanda**: *quali sono i requisiti per le clausole tipo a protezione dei dati (art. 16 cpv. 2 lett. d LPD)?*

In assenza di una valutazione dell'adeguatezza da parte del Consiglio federale (cfr. n. 5.2), la protezione appropriata dei dati può essere garantita da *clausole tipo* (art. 16 cpv. 2 lett. d LPD).

Le clausole tipo a protezione dei dati possono essere stabilite da privati, gruppi di interesse oppure organi federali, previa approvazione dell'IFPDT. È vietato comunicare dati all'estero prima che l'IFPDT abbia deciso in merito alle clausole, a meno che si applichino altre garanzie secondo l'articolo 16 capoverso 2 LPD (cfr. le domande 5.3.1 e 5.3.3) oppure un'eccezione secondo l'articolo 17 LPD (cfr. la domanda 5.4). L'IFPDT decide entro 90 giorni (art. 10 cpv. 2 OPDa).

L'IFPDT stesso può emanare o riconoscere clausole tipo. Pubblica l'elenco all'indirizzo <https://https://www.edoeb.admin.ch/edoeb/it/home/deredoeb/infothek/infothek-ds.html>.

Esempio: l'IFPDT ha riconosciuto le clausole contrattuali tipo della Commissione europea (decisione di esecuzione [UE] 2021/914 del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso Paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio).

Se comunica dati personali all'estero fondandosi su clausole tipo di protezione dei dati, il titolare o il responsabile del trattamento adotta provvedimenti adeguati per garantire che il destinatario le rispetti (art. 10 cpv. 1 OPDa).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6030 seg.; rapporto esplicativo alla OPDa, pag. 34.

5.3.3 **Domanda**: *quali sono i requisiti per le norme aziendali vincolanti in materia di protezione dei dati (art. 16 cpv. 2 lett. e LPD)?*

In assenza di una valutazione dell'adeguatezza da parte del Consiglio federale (cfr. n. 5.2), è possibile comunicare dati personali a un'impresa estera appartenente allo stesso gruppo (cfr. art. 11 cpv. 1 OPDa) attenendosi alle *norme aziendali vincolanti a protezione dei dati* (art. 16 cpv. 2 lett. e LPD).

Tali norme, note come «*Binding Corporate Rules*» (BCR), vanno previamente approvate dall'IFPDT o dalla competente autorità di uno Stato che garantisce una protezione adeguata

dei dati. I dati personali non possono essere comunicati prima che l'IFPDT abbia deciso in merito alle BCR; i risultati del relativo esame sono comunicati entro 90 giorni (art. 11 cpv. 3 OPDa). L'approvazione esplicita dell'IFPDT non è necessaria se le BRC sono già state approvate dalla competente autorità di uno Stato che garantisce una protezione adeguata dei dati.

Il contenuto minimo delle BCR è disciplinato all'articolo 11 OPDa: devono comprendere almeno le informazioni richieste per le clausole contrattuali e le garanzie specifiche secondo l'articolo 9 capoverso 1 OPDa (cfr. in merito la domanda 5.3.1), come pure le seguenti indicazioni (art. 11 cpv. 2 OPDa):

- l'organizzazione e i dati di contatto del gruppo e delle sue imprese;
- le misure adottate in seno al gruppo per garantire il rispetto delle norme aziendali vincolanti in materia di protezione dei dati.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6031 seg.; rapporto esplicativo alla OPDa, pag. 34 seg.

5.3.4 **Domanda**: *esistono altre garanzie ai fini di una protezione appropriata dei dati all'estero e della loro comunicazione all'estero?*

Sì. L'articolo 16 capoverso 3 LPD in combinato disposto con l'articolo 12 capoverso 1 OPDa consente la comunicazione dei dati personali all'estero se la loro adeguata protezione è garantita da un *codice di condotta* o da una *certificazione*. Il codice di condotta va previamente sottoposto all'IFPDT per approvazione (art. 12 cpv. 2 OPDa). In aggiunta occorre l'impegno vincolante ed esecutorio del titolare o del responsabile del trattamento nello Stato terzo di adottare le misure contenutevi (art. 12 cpv. 3 OPDa).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6032; rapporto esplicativo alla OPDa, pag. 34 seg..

5.4 Eccezioni

Domanda: *a titolo eccezionale è possibile comunicare all'estero dati personali senza una valutazione dell'adeguatezza del Consiglio federale o garanzia di una protezione appropriata dei dati?*

Sì. L'articolo 17 capoverso 1 LPD consente la comunicazione eccezionale dei dati all'estero, ossia senza valutazione dell'adeguatezza (cfr. n. 5.2) o particolari garanzie (cfr. n. 5.3), nei casi elencati qui di seguito.

- L'interessato ha dato il suo espresso consenso alla comunicazione (lett. a).
- La comunicazione è chiaramente riconducibile alla conclusione o all'esecuzione di un contratto tra il titolare del trattamento e l'interessato oppure tra il titolare e un altro contraente nell'interesse dell'interessato (lett. b). In quest'ultimo caso l'IFPDT va informato su richiesta (art. 17 cpv. 2 LPD).
- La comunicazione è necessaria per tutelare un interesse pubblico preponderante o per accertare, esercitare o far valere un diritto dinanzi a un giudice o a un'altra autorità estera competente (lett. c). L'IFPDT ne va informato su richiesta (art. 17 cpv. 2 LPD).
- La comunicazione è necessaria per proteggere la vita o l'integrità fisica dell'interessato o di un terzo e non è possibile ottenere il consenso dell'interessato entro un termine ragionevole (lett. d). L'IFPDT ne va informato su richiesta (art. 17 cpv. 2 LPD).
- L'interessato ha reso i dati personali accessibili a chiunque e non si è opposto espressamente al loro trattamento (lett. e).

- I dati provengono da un registro previsto dalla legge accessibile al pubblico o alle persone con un interesse degno di protezione, sempreché nel caso specifico siano adempiute le condizioni legali per la consultazione (lett. f).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6032 seg.

6. Obblighi del titolare e del responsabile del trattamento

6.1 Obbligo del titolare di informare sulla raccolta di dati personali

6.1.1 **Domanda**: *cosa s'intende per obbligo del titolare di informare sulla raccolta di dati personali?*

Secondo l'articolo 19 capoverso 1, il titolare del trattamento deve informare in modo adeguato l'interessato sulla raccolta di dati personali. È un principio fondamentale del diritto in materia di protezione dei dati, perché soltanto chi sa che qualcuno sta trattando i suoi dati può decidere come vadano gestiti.

Il nuovo testo di legge estende l'obbligo di informare alla raccolta di tutti i tipi di dati personali (art. 19 cpv. 1 LPD). Per gli organi federali non è una novità; e infatti la modifica riguarda in primo luogo i titolari privati del trattamento, cui la legge precedente imponeva solo d'informare in merito alla raccolta di dati personali degni di particolare protezione o di profili della personalità. Il trattamento dei dati risulterà più trasparente e l'autodeterminazione informativa dei cittadini ne esce rafforzata.

Come finora l'obbligo sussiste anche se i dati non sono raccolti presso l'interessato (art. 19 cpv. 1 secondo periodo subordinato LPD).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6039 seg.

6.1.2 **Domanda**: *sono previste eccezioni all'obbligo di informare sulla raccolta di dati personali?*

Sì. L'articolo 20 LPD prevede deroghe e restrizioni, ossia situazioni in cui non sussiste obbligo d'informare (cpv. 1 e 2) o in cui occorre ponderare gli interessi (cpv. 3 e 4).

Si ha una *deroga* all'obbligo d'informare se, tra le altre cose:

- l'interessato dispone già delle pertinenti informazioni (art. 20 cpv. 1 lett. a LPD);

  Esempio: l'interessato ha già dato il suo consenso al trattamento dei dati.

- il trattamento dei dati personali è previsto dalla legge (art. 20 cpv. 1 lett. b LPD);

  Possono rientrare in questa fattispecie i trattamenti di dati da parte sia di organi federali che di titolari privati, nel qual caso l'interessato può evincere le grandi linee del trattamento dalla base legale.

- i dati personali sono raccolti presso terzi e informare l'interessato non è possibile o richiede un onere sproporzionato (art. 20 cpv. 2 LPD).

Il titolare del trattamento può limitare o differire l'informazione oppure rinunciarvi se

- interessi preponderanti di un terzo lo esigono (art. 20 cpv. 3 lett. a LPD);
- interessi preponderanti del titolare privato lo esigono ed egli non comunica i dati personali a terzi (esterni a un gruppo aziendale; cfr. art. 20 cpv. 3 e 4 LPD);

- nel caso di organi federali, lo esige un interesse pubblico preponderante, in particolare la salvaguardia della sicurezza interna o esterna della Svizzera (art. 20 cpv. 3 lett. d n. 1 LPD).

L'informazione andrebbe limitata soltanto per quanto assolutamente necessario e il motivo della limitazione deve essere messo in relazione con la trasparenza del trattamento. In linea di massima va scelta la soluzione che sia più favorevole per l'interessato e garantisca un trattamento possibilmente trasparente dei dati.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6041 segg.

6.1.3 **Domanda**: *quali informazioni deve fornire all'interessato il titolare del trattamento?*

Ai sensi dell'articolo 19 capoverso 2 periodo introduttivo LPD, all'interessato vanno in linea di massima comunicate tutte le informazioni necessarie per permettergli di far valere i diritti riconosciutigli dalla legge e per garantire un trattamento trasparente dei dati. L'articolo 19 capoversi 2 lettere a–c, 3 e 4 LPD precisa tale principio indicando svariate informazioni minime da comunicare all'interessato, il che consente di gestire l'obbligo di informare con flessibilità e in funzione dei rischi. L'informazione dovrà essere più o meno dettagliata a seconda del tipo di dati trattati nonché della natura e della portata del trattamento.

Rientrano nelle informazioni minime: l'identità (ossia nome o ditta) e i dati di contatto del titolare (art. 19 cpv. 2 lett. a LPD), lo scopo del trattamento (art. 19 cpv. 2 lett. b LPD) e, se del caso, i destinatari o le categorie di destinatari cui sono comunicati dati personali (art. 19 cpv. 2 lett. c). Sono considerati destinatari a sensi di questa disposizione anche i responsabili del trattamento. Quando raccoglie dati personali, il titolare deve quindi segnalare agli interessati che i dati saranno comunicati a un responsabile. Se i dati non sono raccolti presso l'interessato, ma presso un terzo, il titolare lo informa inoltre sulle categorie di dati personali trattati (art. 19 cpv. 3 LPD). Se comunica all'estero i dati personali (art. 19 cpv. 4 LPD), lo informa infine sullo Stato o l'organismo internazionale destinatario e, se del caso, sulle garanzie di cui all'articolo 16 capoverso 2 LPD (cfr. in merito le domande al n. 5.3) oppure sull'applicazione di un'eccezione secondo l'articolo 17 LPD (cfr. in merito le domande al n. 5.4).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6040 seg.

6.1.4 **Domanda**: *in che modo l'interessato dev'essere informato della raccolta dei suoi dati personali? È sufficiente pubblicare le informazioni necessarie su un sito?*

La legge non specifica le modalità dell'informazione. L'articolo 19 capoverso 1 LPD si limita a prescrivere un'informazione «adeguata». L'articolo 13 OPDa specifica che il titolare del trattamento informa l'interessato in forma precisa, trasparente, comprensibile e facilmente accessibile.

Né la legge né l'ordinanza prevedono prescrizioni formali in merito, per cui sono ipotizzabili, ad esempio, informative sulla privacy, condizioni generali, apposite lettere o pittogrammi. Il titolare del trattamento deve tuttavia provvedere affinché l'interessato possa effettivamente prendere atto dell'informazione in modo facilmente accessibile, in particolare nel caso in cui i dati sono raccolti presso terzi. In tal caso la semplice pubblicazione dell'informazione può non essere sufficiente perché l'interessato deve sapere che può informarsi accedendo a un determinato sito e ne va attivamente messo a conoscenza.

Nel caso di una telefonata, le informazioni possono essere date a voce, eventualmente indicando il link a un sito. Nel caso di informazioni registrate, l'interessato deve avere la possibilità di ascoltare spiegazioni più dettagliate. Le persone filmate da un drone o un impianto di

videosorveglianza vanno rese attente a tale fatto ad esempio con un cartello o una campagna d'informazione.

Nello scegliere lo strumento di comunicazione, il titolare deve garantire che l'interessato riceva sempre al primo colpo le informazioni principali sulla raccolta dei dati che lo riguardano. Se opta ad esempio per la pubblicazione sul suo sito, una buona prassi può consistere nel riunire le informazioni essenziali in una panoramica strutturata, che l'interessato può espandere con un clic per accedere agli approfondimenti del caso.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6039 seg.; rapporto esplicativo alla OPDa, pag. 35.

6.2 Decisione individuale automatizzata

6.2.1 **Domanda***: cosa s'intende per decisione individuale automatizzata?*

Si parla di decisione individuale automatizzata quando la decisione si basa esclusivamente su un trattamento automatizzato di dati personali e ha effetti giuridici o conseguenze significative per l'interessato (art. 21 cpv. 1 LPD).

- *Automatizzazione integrale*: nel caso di una decisione individuale automatizzata sia la valutazione materiale di un fatto sia la decisione che ne risulta è opera di una macchina, ossia di un algoritmo, senza l'intervento di una persona fisica. Per contro è irrilevante se l'algoritmo è stato programmato da un umano. È considerata automatizzata anche la decisione individuale comunicata da una persona fisica che non l'abbia adottata o che si è limitata a sottoporla a un controllo formale. Non è per contro automatizzata la decisione individuale preparata da una macchina, ma adottata da un umano.

- *Complessità*: la decisione individuale automatizzata ai sensi della nuova legge sulla protezione dei dati deve presentare una certa complessità. Lo scopo tutelare delle pertinenti disposizioni (segnatamente art. 21, 25 cpv. 2 lett. f nonché 34 cpv. 2 lett. c LPD) sembra porre l'accento sui processi decisionali che risultano incomprensibili agli interessati. Ecco perché, a titolo di riduzione teleologica dell'articolo 21 capoverso 1 LPD, non dovrebbero rientrare nel concetto di decisione individuale automatizzata né le banali decisioni conseguenziali (se – allora) né le semplici domande cui rispondere sì o no in base a criteri oggettivi evidenti per l'interessato.

  Esempi: non sono decisioni individuali automatizzate ai sensi dell'articolo 21 capoverso 1 LPD il prelievo di denaro al bancomat o il controllo degli accessi tramite badge ed elenchi predefiniti di persone autorizzate, e nemmeno le banali operazioni matematiche (come p. es. una semplice addizione), troppo poco complesse per rientrare nella definizione.

- *Effetto*: nel concetto di decisione individuale automatizzata secondo l'articolo 21 capoverso 1 LPD rientrano soltanto quelle che hanno effetti giuridici o conseguenze significative per l'interessato.

  Ha *effetti giuridici* una decisione che espone l'interessato a conseguenze dirette previste per legge. Nel diritto privato gli effetti giuridici sono legati alla conclusione o alla risoluzione di un contratto: la mancata stipula di un contratto non esplica in linea di massima effetti giuridici (sussiste però una situazione peculiare nel caso dell'obbligo di contrarre). Un contratto non concluso può comunque avere conseguenze significative (seconda eventualità; cfr. qui di seguito). Nel settore pubblico si hanno effetti giuridici in particolare quando una decisione amministrativa è adottata in modalità completamente automatizzata.

Si possono presumere *conseguenze significative* per l'interessato se questi subisce pregiudizi economici o personali durevoli. Una semplice inconveniente non è sufficiente. Tutto dipende dalle circostanze concrete del caso. Occorre in particolare tenere conto dell'importanza del bene in questione per l'interessato, della durata degli effetti della decisione e delle eventuali alternative a disposizione. Se si tratta di un bene importante (p. es. abitazione o posto di lavoro), l'eventuale presenza di alternative va interpretata in modo restrittivo.

Esempio: si possono avere conseguenze significative nel caso di prestazioni mediche effettuate sulla base di una decisione individuale automatizzata.

La decisione individuale automatizzata va distinta dalla profilazione, anche se le due operazioni possono coincidere: il trattamento dei dati alla base della decisione individuale automatizzata può, ma non deve, costituire una profilazione, mentre una profilazione può, ma non deve, sfociare in una decisione individuale automatizzata (p. es. nel caso di un semplice esame preliminare in vista di una decisione adottata da un umano). Sebbene il Parlamento abbia stralciato l'inciso «inclusa la profilazione» nell'articolo 19 capoverso 1 del disegno del Consiglio federale, nulla cambia in termini materiali, come esposto dal Capodipartimento DFGP nel Consiglio degli Stati il 18 dicembre 2019. Infatti la profilazione non rivestiva alcuna rilevanza in tale disposizione in quanto, esplicitata o no, rientra nel campo di applicazione dell'articolo 21 capoverso 1 LPD se porta a una decisione individuale automatizzata.

Rimandi: messaggio LPD, FF 2017 5939 pag. 6045 segg.; nota UFG/LPD, pag. 20 segg.; Boll. uff. 2019 S 1241 (intervento del Capodipartimento DFGP nel dibattito del 18 dicembre 2019 sulla revisione totale della LPD nel Consiglio degli Stati).

6.2.2 **Domanda**: *quali sono i diritti dell'interessato nel caso di una decisione individuale automatizzata?*

La nuova legge impone che la persona i cui dati sono trattati vada informata in merito a una decisione individuale automatizzata (art. 21 cpv. 1 LPD). Se la decisione individuale automatizzata è presa da un organo federale, questi la deve designare come tale (art. 21 cpv. 4 primo periodo LPD). Inoltre la persona in questione ha il diritto, su sua richiesta, di esprimere un parere e di esigere che la decisione vada riesaminata da una persona fisica (art. 21 cpv. 2 LPD).

Secondo l'articolo 21 capoverso 3 LPD, l'obbligo del titolare d'informare e sentire l'interessato non si applica se la decisione individuale automatizzata è in relazione diretta con la conclusione o l'esecuzione di un contratto tra il titolare e l'interessato e la richiesta di quest'ultimo è soddisfatta (lett. a) o se l'interessato ha dato il suo espresso consenso all'adozione automatizzata della decisione (lett. b; in merito ai requisiti posti al consenso cfr. la domanda 3.4.2). Inoltre l'articolo 21 capoverso 2 LPD riguardo al diritto dell'interessato di essere sentito non si applica agli organi federali se non sono tenuti a sentirlo secondo l'articolo 30 capoverso 2 PA (legge sulla procedura amministrativa; RS 172.021) o un'altra legge federale (p. es. se la decisione individuale automatizzata può essere esaminata in una procedura d'opposizione non automatizzata). In questo modo la legge sulla protezione dei dati si conforma al diritto di procedura amministrativa della Confederazione.

Infine l'articolo 25 capoverso 2 lettera f prevede che l'interessato riceva, nel quadro del diritto d'accesso, indicazioni sull'esistenza di una decisione individuale automatizzata e la logica su cui si fonda (cfr. in merito le domande al n. 7.2).

Rimandi: in merito ai requisiti in termini di basi legali per consentire agli organi federali di emanare decisioni individuali automatizzate cfr. la nota UFG/LPD, pag. 22.

6.3 Valutazione d'impatto sulla protezione dei dati

6.3.1 **Domanda**: *cosa s'intende per valutazione d'impatto sulla protezione dei dati?*

Chi prevede un trattamento di dati implicante un rischio elevato per la personalità o i diritti fondamentali dell'interessato deve valutarne l'impatto sulla protezione dei dati (art. 22 cpv. 1 LPD). Concepita come strumento per inquadrare i rischi, la valutazione d'impatto sulla protezione dei dati contiene una descrizione del trattamento previsto, una valutazione dei rischi per la personalità o i diritti fondamentali della persona interessata nonché i provvedimenti a sua tutela (art. 22 cpv. 3 LPD). Non serve soltanto a proteggere le persone toccate da un trattamento dei dati particolarmente rischioso, ma è utile anche al titolare, in quanto gli permette di affrontare preventivamente eventuali problemi inerenti alla protezione dei dati.

La valutazione dev'essere conservata per almeno due anni dopo la fine del trattamento (art. 14 OPDa).

Rimandi: messaggio LPD, FF 2017 5939 pag. 6047 segg; rapporto esplicativo alla OPDa, pag. 36 seg.

6.3.2 **Domanda**: *quando va valutato l'impatto sulla protezione dei dati?*

La valutazione è necessaria quando il trattamento dei dati personali può comportare un rischio elevato per la personalità o i diritti fondamentali dell'interessato (art. 22 cpv. 1 LPD). La presenza di un tale rischio va determinata in base a vari fattori. Secondo l'articolo 22 capoverso 2 LPD, il rischio elevato risulta dal tipo, dall'entità, dalle circostanze e dallo scopo del trattamento, in particolare in caso di utilizzazione di nuove tecnologie. La legge indica a titolo di esempio due situazioni a rischio elevato: il trattamento su grande scala di dati personali degni di particolare protezione (cfr. in merito la domanda 3.6.2.3) e la sorveglianza sistematica di ampi spazi pubblici (art. 22 cpv. 2 lett. a e b LPD).

Sono *esentati* dall'obbligo di valutare l'impatto i titolari privati tenuti per legge a trattare i dati (art. 22 cpv. 4 LPD). In tale evenienza si può partire dal presupposto che il legislatore abbia ponderato gli eventuali rischi per gli interessati emanando, se del caso, le necessarie disposizioni a loro tutela.

Inoltre il titolare privato può rinunciare alla valutazione se utilizza un sistema, un prodotto o un servizio certificato secondo l'articolo 13 per l'impiego previsto o se rispetta un codice di condotta secondo l'articolo 11 che adempie vari criteri (art. 22 cpv. 5 LPD).

Rimandi: messaggio LPD, FF 2017 5939 pag. 6047 segg.

Documentazione concernente la valutazione d'impatto sulla protezione dei dati personali (VIPD) per gli organi federali:

- Direttive del Consiglio federale per l'esame preliminare dei rischi e la valutazione d'impatto sulla protezione dei dati in caso di trattamento di dati personali da parte dell'Amministrazione federale (FF 2023 1882)
- Strumento per l'esame preliminare dei rischi
- Guida VIPD (verrà pubblicata prossimamente)

6.3.3 **Domanda**: *quando va consultato l'IFPDT?*

Il titolare del trattamento deve chiedere il parere dell'IFPDT se dalla valutazione d'impatto sulla protezione dei dati emerge che, *nonostante* i provvedimenti del titolare, il trattamento previsto comporta un *rischio residuo elevato* per la personalità o i diritti fondamentali dell'interessato (art. 23 cpv. 1 LPD). In altre parole: il titolare del trattamento deve consultare l'IFPDT soltanto quando non riesce a gestire in maniera soddisfacente i rischi individuati.

L'IFPDT, se consultato, comunica entro due mesi al titolare le sue obiezioni al trattamento previsto. Il termine può essere prorogato di un mese se si tratta di un trattamento di dati complesso (art. 23 cpv. 2 LPD). Se ha obiezioni al trattamento previsto, l'IFPDT propone al titolare provvedimenti appropriati (art. 23 cpv. 3 LPD).

Il titolare privato del trattamento può *rinunciare* a consultare l'IFPDT se ha consultato il consulente per la protezione dei dati ai sensi dell'articolo 10 (cfr. in merito le domande 3.7.1 e 3.7.3).

6.4 Notifica di violazioni della sicurezza dei dati

6.4.1 **Domanda**: *cosa s'intende per violazione della sicurezza dei dati?*

Cfr. in merito la domanda 3.6.1.1.

6.4.2 **Domanda**: *all'IFPDT vanno notificate tutte le violazioni della sicurezza dei dati?*

No. La notifica all'IFPDT ai sensi dell'articolo 21 capoverso 1 LPD è necessaria soltanto se la violazione della sicurezza comporta verosimilmente un *rischio elevato* per la personalità o i diritti fondamentali dell'interessato. Il titolare del trattamento deve pertanto valutare le possibili ripercussioni della violazione per l'interessato. Vanno notificate soltanto le violazioni effettive della sicurezza dei dati, ma non i ciberattacchi inefficaci o respinti con successo. È possibile notificare a titolo volontario le violazioni considerate a basso rischio dal titolare.

Per la notifica all'IFPDT è stato implementato un apposito portale («Databreach»: <https://databreach.edoeb.admin.ch/report>). Il titolare è comunque libero di depositare la notifica in altro modo.

Rimandi: messaggio LPD, FF 2017 5939 pag. 6051 seg.

6.4.3 **Domanda**: *quali elementi deve contenere la notifica all'IFPDT?*

L'articolo 24 capoverso 2 LPD indica il contenuto minimo della notifica, ossia il tipo di violazione della sicurezza dei dati, le conseguenze e le misure disposte o previste. Il contenuto è ulteriormente specificato nell'articolo 15 capoverso 1 OPDa: oltre alle informazioni citate nella legge, vanno per quanto possibile notificati anche il momento e la durata della violazione e le categorie, il numero approssimativo delle persone e dei dati personali interessati dalla violazione (p. es. indirizzi, informazioni creditizie, dati sanitari). Queste informazioni sono importanti in quanto permettono all'IFPDT di valutare la portata della violazione. Il titolare deve inoltre indicare nomi e recapiti di una persona di contatto che funge da interlocutore sia dell'IFPDT sia, se del caso, degli interessati (cfr. in merito la domanda 6.4.5).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6051 seg.; rapporto esplicativo alla OPDa, pag. 36.

6.4.4 **Domanda**: *l'articolo 24 capoverso 1 LPD stabilisce che una violazione della sicurezza dei dati va notificata all'IFPDT «quanto prima». Cosa significa?*

Il titolare del trattamento deve notificare la violazione quando ne viene a conoscenza; in linea di massima deve agire rapidamente, ma dispone di un certo margine di apprezzamento. È

determinante, tra le altre cose, la probabilità del rischio di ledere l'interessato: quanto più elevati sono il rischio e il numero d'interessati, tanto più rapidamente il titolare dovrà informare l'IFPDT.

L'articolo 15 capoverso 2 OPDa consente al titolare d'informare l'IFPDT a scaglioni se non è possibile fornire subito tutte le informazioni al momento in cui scopre la violazione della sicurezza dei dati. In un primo momento può comunicare soltanto le informazioni di base che gli sono note, integrandole «quanto prima», come impone l'articolo 24 capoverso 1 LPD (cfr. domanda 6.4.4).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6051 seg.; rapporto esplicativo alla OPDa, pag. 36 seg.

6.4.5 **Domanda**: *in quali casi gli interessati vanno informati della violazione della sicurezza dei dati?*

Il titolare deve informare l'interessato sulla violazione della sicurezza dei dati se è necessario per proteggerlo o se lo esige l'IFPD (art. 24 cpv. 4 LPD). Il titolare ha un certo margine di apprezzamento per giudicare se, informando l'interessato, è possibile ridurre i rischi per la sua personalità e i suoi diritti fondamentali, ad esempio consentendogli di prendere provvedimenti per proteggersi (p. es. modificare i suoi dati d'accesso o le sue parole chiave).

L'articolo 15 capoverso 3 OPDa disciplina le informazioni da comunicare agli interessati specificando che devono essere semplici e comprensibili.

In determinati casi il titolare può limitare o differire l'informazione dell'interessato o addirittura rinunciarvi, ad esempio se sussiste un obbligo legale di serbare il segreto o se l'informazione è impossibile o richiede un onere sproporzionato. Le deroghe sono disciplinate nell'articolo 24 capoverso 5 LPD.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6053; rapporto esplicativo alla OPDa, pag. 37.

7. Diritti dell'interessato

7.1 Panoramica

Domanda: *quali sono i diritti delle persone interessate da un trattamento di dati?*

La revisione totale della LPD rende più trasparente il trattamento dei dati, il che è fondamentale per rafforzare i diritti degli interessati. Infatti solo chi sa che i suoi dati sono oggetto di trattamento può far valere le proprie pretese alla protezione di tali dati. Ecco perché, oltre all'obbligo del titolare d'informare in merito alla raccolta di dati personali (art. 19 seg. LPD; cfr. in merito le domande al n. 6.1), riveste un'importanza fondamentale anche il diritto d'accesso (art. 25 segg. LPD; cfr. in merito la domanda 7.2), che consente agli interessati di chiedere al titolare importanti informazioni in merito al trattamento dei propri dati. La legge riveduta prevede infine il diritto alla consegna o alla trasmissione dei dati (art. 28 seg. LPD; cfr. in merito la domanda 7.3), oltre ad altri diritti che consentono agli interessati d'intervenire nel trattamento dei propri dati. Ne fanno in particolare parte il diritto di opporsi al trattamento o alla comunicazione dei dati (art. 30 cpv. 2 lett. in combinato disposto con gli art. 32 cpv. 2 e 37 LPD), il diritto di far rettificare i dati personali inesatti (art. 32 cpv. 1 e 41 cpv. 2 lett. a LPD) e il diritto di far cancellare o distruggere i dati personali trattati illecitamente (art. 32 cpv. 2 lett. c e 41 cpv. 2 lett. a LPD).

Gli interessati possono adire un giudice indipendente nel quadro di un procedimento civile o amministrativo per far valere i loro diritti (art. 32 e 41 LPD). Possono inoltre denunciare

all'IFPDT la violazione delle disposizioni in materia di protezione dei dati (art. 49 cpv. 1 LPD). Gli interessati non hanno qualità di parte nell'eventuale inchiesta aperta dall'IFPDT (art. 52 cpv. 2 LPD e contrario), che però deve informarli sul seguito dato alla denuncia e sull'esito dell'inchiesta (art. 49 cpv. 4 LPD). Determinate azioni (p. es. violazione degli obblighi d'informare e di concedere l'accesso) possono infine essere denunciate alle autorità penali (art. 60 segg. LPD; cfr. in merito le domande al n. 11).

7.2 Diritto d'accesso

7.2.1 **Domanda**: *cosa s'intende per diritto d'accesso?*

L'articolo 25 capoverso 1 LPD dispone che chiunque può domandare al titolare se dati personali che lo concernono sono oggetto di trattamento. Tale diritto d'accesso è stato ampliato nel corso della revisione. L'interessato deve ricevere le informazioni necessarie a far valere i propri diritti secondo la LPD e a garantire un trattamento trasparente dei dati (art. 25 cpv. 2 periodo introduttivo LPD). Il diritto d'accesso consente all'interessato di controllare il trattamento dei propri dati e di opporsi all'eventuale trattamento illecito dei dati (cfr. domanda 7.1)

L'articolo 25 capoverso 2 LPD elenca tutte le informazioni che vanno fornite in ogni caso: all'interessato vanno comunicati l'identità e i dati di contatto del titolare, i dati personali trattati in quanto tali e lo scopo del trattamento (lett. a – c), oltre alla durata di conservazione dei dati personali o, se ciò non è possibile, ai criteri per stabilire tale durata (lett. d). Deve inoltre ricevere le informazioni disponibili sulla provenienza dei dati personali che non sono stati raccolti presso l'interessato stesso (lett. e). Se del caso va informato dell'esistenza di una decisione individuale automatizzata (cfr. in merito le domande 6.2.1 e 6.2.2), come pure della logica su cui si fonda la decisione. Gli vanno anche segnalati i destinatari o le categorie di destinatari cui sono comunicati dati personali. Se questi si trovano all'estero, l'interessato va informato dello Stato e delle garanzie previste o dell'eventuale applicazione di una deroga (lett. g; cfr. in merito n. 5).

Indicazione: una lettera modello e la procedura per la richiesta d'accesso sono reperibili sul sito dell'IFPDT:
<https://www.edoeb.admin.ch/edoeb/it/home/datenschutz/grundlagen/auskunftsrecht.html>.

Rimandi: messaggio LPD, FF 2017 5939, pag 6053 segg.; rapporto esplicativo alla OPDa, pag. 38 segg.

7.2.2 **Domanda**: *è possibile limitare il diritto d'accesso?*

In determinati casi il titolare del trattamento può rifiutare, limitare o differire l'informazione (art. 26 e 27 LPD), segnatamente in presenza di interessi privati o pubblici preponderanti. Tali restrizioni del diritto d'accesso riprendono in ampia misura il diritto previgente.

In futuro il titolare potrà inoltre rifiutare, limitare o differire l'informazione anche se la domanda d'accesso è manifestamente infondata, segnatamente se persegue uno scopo contrario alla protezione dei dati, o se è querulosa (art. 26 cpv. 1 lett. c LPD). Questa eccezione va interpretata in senso stretto perché in linea di massima il diritto d'accesso può essere fatto valere senza condizioni e senza interesse giustificativo. In una decisione di principio in materia, il Tribunale federale riconosce tuttavia che il motivo della richiesta può essere preso in considerazione a titolo eccezionale se il diritto d'accesso è fatto valere abusivamente, vale a dire a scopi contrari alla finalità della legge sulla protezione dei dati (DTF 138 III 425 consid. 5.5). Stando al Tribunale federale, si potrebbe ad esempio avere abuso di diritto quando l'accesso è chiesto con il solo scopo di spiare una (futura) controparte e procurarsi prove altrimenti non reperibili o di risparmiare le spese per la raccolta delle prove. Una vessazione è inoltre ipotizzabile anche

nei casi in cui l'accesso è chiesto soltanto per nuocere alla persona tenuta a informare. Alla luce dell'enorme importanza che il diritto d'accesso riveste per i diritti della personalità e i diritti fondamentali degli interessati (cfr. domanda 7.2.1), ai fini di tale interpretazione è tuttavia indispensabile che la domanda d'accesso sia manifestamente infondata, ossia depositata per motivi totalmente estranei alla protezione dei dati.

Il titolare del trattamento che rifiuta, limita o differisce la comunicazione dell'informazione deve indicarne il motivo (art. 26 cpv. 4 LPD). I motivi addotti devono permettere all'interessato di verificare se la restrizione del suo diritto d'accesso è legittima.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6056 segg.; rapporto esplicativo alla OPDa, pag. 38 segg.; DTF 138 III 425.

7.3 Diritto alla consegna o alla trasmissione dei dati

Domanda: *cosa s'intende per diritto alla consegna o alla trasmissione dei dati?*

Tale diritto è stato introdotto dal Parlamento nel corso delle deliberazioni sulla revisione totale della legge: l'articolo 28 LPD consente all'interessato di esigere dal titolare privato che gli consegni in formato elettronico usuale i dati personali comunicati o che li trasmetta a un altro titolare. Questo a condizione che il titolare tratti i dati in modo automatizzato (cfr. la domanda 2.2.2) e con il consenso dell'interessato oppure in relazione diretta con la conclusione o l'esecuzione di un contratto tra il titolare e l'interessato. Inoltre l'eventuale trasmissione a un altro titolare non deve richiedere un onere sproporzionato (art. 28 cpv. 2 LPD).

I dati personali consegnati secondo l'articolo 28 LPD possono essere utilizzati per vari scopi, ad esempio per uso puramente personale (p. es. salvataggio su un supporto personale) o per trasmissione a un altro fornitore di servizi online. Il nuovo diritto alla consegna o trasmissione dei dati intende rafforzare il controllo degli interessati sui propri dati e il loro utilizzo; semplifica il passaggio da un'offerta di servizi digitali all'altra, incentiva le soluzioni innovative e stimola la competizione tra i vari fornitori.

Le restrizioni del diritto alla consegna o alla trasmissione dei dati sono rette dall'articolo 29 LPD, che rimanda in ampia misura alle disposizioni in materia di diritto d'accesso (cfr. domanda 7.2.2).

Rimandi: il diritto alla consegna o trasmissione dei dati è approfondito nel rapporto esplicativo alla OPDa, pag. 41 segg.

8. Disposizioni speciali per il trattamento di dati da parte di privati

Domanda: *ai titolari privati serve un motivo che giustifichi il trattamento dei dati personali?*

Ai privati (aziende o persone fisiche) in Svizzera è in linea di massima consentito trattare dati personali. Il trattamento di dati va giustificato soltanto se nello specifico lede la personalità. La lesione della personalità non giustificata è considerata illecita (art. 30 cpv. 1 e 31 cpv. 1 LPD). La legge sulla protezione dei dati s'ispira quindi a quanto si applica già alla protezione della personalità secondo il Codice civile (art. 28 segg. CC; RS 210).

Non tutti i trattamenti di dati personali ledono la personalità. Solo quelli che arrecano un pregiudizio di una certa intensità sono considerati lesivi della personalità. L'articolo 30 capoverso 2 LPD elenca a titolo d'esempio alcune azioni costitutive della fattispecie, si è pertanto in presenza di una lesione della personalità se:

- sono trattati dati personali in violazione dei principi di cui agli articoli 6 e 8 (art. 30 cpv. 2 lett. a LPD; p. es. trattamento più lungo del necessario o contrario allo scopo originario);
- sono trattati dati personali contro l'espressa volontà dell'interessato (art. 30 cpv. 2 lett. b LPD); oppure
- sono comunicati a terzi dati personali degni di particolare protezione (art. 30 cpv. 2 lett. c LPD).

Non vi è invece lesione della personalità se l'interessato ha reso i suoi dati personali accessibili a chiunque e non si è opposto espressamente al trattamento (art. 30 cpv. 3 LPD).

Non è detto che il trattamento dei dati non sia permesso solo perché si ha una lesione della personalità: questa non è infatti illecita se sussiste un motivo giustificativo sufficiente per il trattamento (art. 31 cpv. 1 LPD). Sono tre i motivi giustificativi possibili.

- *base legale* per il trattamento dei dati;
- *interesse preponderante privato o pubblico:* richiede una ponderazione degli interessi e l'articolo 31 capoverso 2 LPD elenca una serie di situazioni per le quali è ipotizzabile un interesse preponderante del titolare;
- *consenso:* se un trattamento lesivo della personalità è giustificato dal consenso dell'interessato, tale consenso deve adempire i requisiti dell'articolo 6 capoversi 6 e 7 LPD (cfr. in merito la domanda 3.4.2).

Se non è possibile giustificare un trattamento di dati lesivo della personalità, l'interessato ha svariati diritti di carattere civile: in merito l'articolo 32 capoverso 2 LPD rimanda, come il diritto previgente, alle azioni secondo l'articolo 28 segg. CC, per cui l'interessato può far valere le stesse pretese applicabili ad altre lesioni della personalità. Per maggior chiarezza la legge esplicita inoltre alcune pretese specifiche, tra le quali in particolare il diritto alla cancellazione o distruzione di dati personali trattati illecitamente (art. 32 cpv. 2 lett. c LPD; cfr. in merito la domanda 7.1).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6063 segg.

9. Disposizioni speciali per il trattamento di dati da parte di organi federali

Indicazione: a differenza dei titolari privati (cfr. domanda 8), gli organi federali in genere necessitano di una base legale per poter trattare dati personali. L'UFG ha pubblicato due documenti ausiliari per facilitarne la redazione:

- Guida di legislazione - protezione dei dati
- Nota UFG/LPD

10. Incaricato federale della protezione dei dati e della trasparenza (IFPDT)

Domanda: *in che modo la LPD riveduta rafforza l'indipendenza e la vigilanza dell'IFPDT?*

Il capo dell'IFPDT è ormai eletto dall'Assemblea federale plenaria (art. 43 cpv. 1 LPD) e dispone di un proprio preventivo (art. 43 cpv. 5 primo periodo e art. 45 LPD), il che rafforza la sua indipendenza.

Saranno estese anche le sue competenze di vigilanza. Secondo la nuova legge l'IFPDT apre, d'ufficio o su denuncia, un'inchiesta nei confronti di un organo federale o di un privato se indizi sufficienti lasciano presumere che un trattamento di dati potrebbe violare le disposizioni sulla protezione dei dati (art. 49 cpv. 1 LPD). Può rinunciarvi se la violazione è di poco conto (art. 49 cpv. 2 LPD). Anche le attribuzioni d'inchiesta dell'IFPDT saranno estese (art. 50 LPD). Se constata che un trattamento di dati viola tali disposizioni, oltre a una raccomandazione, l'IFPDT potrà emanare anche una decisione impugnabile (art. 51 LPD), ordinando ad esempio di adeguare, sospendere o cessare del tutto il trattamento dei dati oppure di cancellare o distruggere i dati personali. Se l'interessato ha sporto denuncia, l'IFPDT lo informa sul seguito dato alla denuncia e sull'esito di un'eventuale inchiesta (art. 49 cpv. 4 LPD).

Ulteriori informazioni in merito all'IFPDT e ai suoi compiti sono reperibili sul suo sito: <https://www.edoeb.admin.ch/edoeb/it/home/datenschutz/grundlagen/rolle-edoeb.html>.

11. Disposizioni penali

11.1 Panoramica

Domanda: *come cambiano le norme penali nella LPD riveduta?*

Oltre a rafforzare la vigilanza sulla protezione dei dati, la legge riveduta inasprisce anche le norme penali per incentivare il rispetto delle proprie disposizioni: estende le fattispecie penali e aumenta da 10 000 a 250 000 franchi la multa massima per le violazioni (art. 60 segg. LPD).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6084 segg.

11.2 Destinatari delle disposizioni penali

Domanda: *perché le disposizioni penali della LPD non si applicano alle imprese, ma alle persone fisiche nelle imprese?*

È vero che le disposizioni penali della LPD sono destinate principalmente alle persone fisiche. Non si tratta di una specificità della legislazione sulla protezione dei dati: nel diritto penale svizzero i destinatari delle disposizioni penali sono infatti in primo luogo le persone fisiche e non quelle giuridiche.

Ad ogni modo l'articolo 6 DPA (Legge federale sul diritto penale amministrativo; RS 313.0) in combinato disposto con l'articolo 64 capoverso 1 LPD garantisce che, nel caso in cui un'impresa violi gli obblighi in materia di protezione dei dati, non siano i semplici collaboratori, ma i dirigenti a dover rispondere del reato. Ciò significa che sono responsabili soprattutto il padrone d'azienda, gli organi o i membri di un organo, i soci autorizzati nonché i dirigenti effettivi. È necessario avere potere decisionale autonomo in un determinato settore dell'impresa.

Esempi: l'obbligo d'informarsi sulla sicurezza dei dati offerta da un responsabile (art. 61 lett. b LPD) incombe ai dirigenti e non ai «semplici collaboratori». È invece punibile il collaboratore che viola il proprio obbligo del segreto (art. 62 LPD).

L'autorità penale competente può prescindere da un procedimento contro la persona fisica e invece infliggere una multa all'impresa (o azienda) se la multa applicabile non supera i 50 000 franchi e sarebbe sproporzionato individuare la persona punibile (art. 64 cpv. 2 LPD).

Rimandi: messaggio LPD, FF 2017 5939, pag. 6084 segg.

11.3 Competenza in materia penale

Domanda: *a chi compete l'azione penale?*

Non compete all'IFPDT perseguire e giudicare i reati secondo la legge sulla protezione dei dati. A differenza della maggior parte dei suoi omologhi degli Stati UE, l'IFPDT non è dotato di competenze sanzionatorie; tale attribuzione resta, come finora, in mano alle autorità penali cantonali (polizia, procura, tribunali penali; art. 65 cpv. 1 LPD). L'IFPDT può tuttavia sporgere denuncia presso l'autorità penale competente e avvalersi dei diritti di accusatore privato nel procedimento (art. 65 cpv. 2 LPD). Nelle sue decisioni può inoltre indicare la comminatoria di pena secondo l'articolo 63 LPD, che prevede una multa fino a 250 000 franchi per il privato che intenzionalmente non ottempera a una decisione dell'IFPDT. Anche in questo caso però il perseguimento penale compete alle autorità cantonali.

Rimandi: messaggio LPD, FF 2017 5939, pag. 6089 segg.

12. Sviluppi internazionali in materia di protezione dei dati

12.1 Direttiva (UE) 2016/680

Domanda: *qual è l'importanza della direttiva (UE) 2016/680 per la Svizzera?*

La direttiva (UE) 2016/680 costituisce uno sviluppo dell'acquis di Schengen che la Svizzera ha dovuto riprendere in base all'accordo di associazione a Schengen; ha un campo d'applicazione specifico e disciplina il trattamento dei dati da parte delle autorità allo scopo di perseguire reati, eseguire pene e prevenire pericoli per la sicurezza pubblica.

12.2 Regolamento generale dell'UE sulla protezione dei dati e valutazione dell'adeguatezza

12.2.1 **Domanda**: *qual è l'importanza del regolamento generale dell'UE sulla protezione dei dati per la Svizzera?*

Il regolamento generale sulla protezione dei dati disciplina la protezione dei dati trattati da privati o autorità degli Stati dell'UE. A differenza della direttiva (UE) 2016/680 per la protezione dei dati in materia penale (cfr. domanda 12.1), il regolamento generale sulla protezione dei dati non è uno sviluppo dell'acquis di Schengen e non vincola direttamente la Svizzera. Si applica tuttavia anche alle imprese in Svizzera che offrono merci o servizi a persone nell'UE o monitorano il comportamento di persone nell'UE. Inoltre per la Svizzera è importante che l'UE continui a riconoscere il nostro Paese come Stato terzo con un adeguato livello di protezione dei dati.

12.2.2 **Domanda**: *la legislazione svizzera in materia di protezione dei dati è conforme alle norme europee?*

Già nel 2000 la Commissione ha riconosciuto l'adeguatezza della protezione dei dati personali in Svizzera (decisione UE); l'adeguatezza a norma della direttiva europea è verificata a intervalli regolari. Il nuovo diritto permette di conformare maggiormente il livello di protezione svizzero allo standard europeo e ha portato l'UE a confermare che la Svizzera offre un livello adeguato di protezione dei dati (si veda il rapporto della Commissione europea del 15 gennaio 2024 e il documento di lavoro allegato contenente i rapporti dei Paesi; questi documenti non sono disponibili in italiano).

12.2.3 Domanda: *quali sono le conseguenze se la Commissione europea non dovesse più ritenere adeguato il livello di protezione dei dati della Svizzera?*

In assenza di una valutazione dell'adeguatezza da parte dell'UE, per comunicare dati verso la Svizzera occorrerebbero garanzie adeguate o determinate deroghe normative; ne conseguirebbero elevati oneri amministrativi, che intralcerebbero il libero flusso dei dati frenando l'innovazione con ripercussioni negative sulla piazza economica svizzera. Il 15 gennaio 2024, l'UE ha confermato che la Svizzera offre un livello adeguato di protezione dei dati (si veda il rapporto della Commissione europea del 15 gennaio 2024 e il documento di lavoro allegato contenente i rapporti dei Paesi; questi documenti non sono disponibili in italiano).

12.3 Convenzione 108+ del Consiglio d'Europa sulla protezione dei dati

Domanda: *perché la Svizzera ha aderito alla Convenzione 108 modernizzata del Consiglio d'Europa sulla protezione dei dati?*

Finora una cinquantina di Stati, tra cui la Svizzera, hanno ratificato la Convenzione 108 del Consiglio d'Europa. Si tratta del primo strumento internazionale vincolante in materia di protezione dei dati, redatto nel 1981 e ora portato nell'era digitale. La Svizzera ha ratificato la versione rivista o modernizzata della Convenzione 108 (Convenzione 108+) il 7 settembre 2023. Tuttavia, la Convenzione 108+ non entrerà in vigore finché non sarà stata ratificata da 38 Stati contraenti. La Svizzera può quindi continuare a mantenere un buon livello di protezione dei dati nei confronti dei propri partner internazionali, e quindi rafforzare la sua economia. Uno degli obiettivi della revisione totale della LPD è stato quello di adempiere i requisiti della Convenzione 108+.