Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Incaricato federale della protezione dei dati e della trasparenza
IFPDT

Protezione die dati

Guida per la notifica di violazioni della sicurezza dei dati e l'informazione alle persone interessate secondo l'articolo 24 LPD

Dal 06 febbraio 2025, ultimo aggiornamento il 23 aprile 2025
(Versione 1.2)

Versione

Versione 1.0	06.02.2025	Pubblicazione
Versione 1.1	26.02.2025	Chiarimenti linguistici nei punti 1.2 e 1.7
Versione 1.2	23.04.2025	Nuovo punto 1.2 Notificante e chiarimenti linguistici nel (nuovo) punto 1.4 Diritto di comunicazione

Contenu

La legge federale del 25 settembre 2020 sulla protezione dei dati (LPD; RS *235.1*) al primo articolo stabilisce che il suo scopo è proteggere la personalità e i diritti fondamentali delle persone fisiche i cui dati personali sono oggetto di trattamento. L'articolo 24 LPD disciplina gli obblighi dei titolari del trattamento e i diritti delle persone interessate nel caso in cui durante tale trattamento dei dati personali vi sia una violazione della sicurezza dei dati. In base all'articolo 5 lettera h LPD si parla di violazione della sicurezza dei dati quando si verifica 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.

Non rientrano pertanto nel campo d'applicazione dell'articolo 24 LPD le violazioni della sicurezza dei dati che, pur provocando gravi danni nell'ambito del segreto di fabbricazione o d'affari, del segreto d'ufficio o del segreto professionale, non interessano dati personali. Allo stesso modo, non rientrano nel campo di applicazione di tale articolo neppure i dati che riguardano esclusivamente persone decedute e che non consentono in alcun modo di risalire a persone in vita arrecando un danno alla loro personalità, in quanto secondo l'articolo 31 capoverso 1 del Codice civile (CC; RS *210*) la personalità finisce con la morte.

Questa guida dell'IFPDT tratta i requisiti legali per la notifica delle violazioni dei dati all'IFPDT, in particolare il concetto di "rischio verosimilmente elevato" ai sensi dell'art. 24 cpv. 1 LPD. Definisce inoltre i requisiti per l'informazione degli interessati in caso di violazione della sicurezza dei dati ai sensi dell'art. 24 cpv. 4 LPD.

1 Notifica di violazioni della sicurezza dei dati all'IFPDT

1.1 Oggetto della notifica

La notifica ha come oggetto la presentazione di fatti e valutazioni. Il titolare del trattamento illustra all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) la violazione della sicurezza dei dati fornendo informazioni segnatamente sul tipo di violazione, il momento in cui è avvenuta, la durata e l'entità della stessa e sulle conseguenze già note e temute per le persone interessate. All'articolo 15 capoverso 1 dell'ordinanza del 31 agosto 2022 sulla protezione dei dati (OPDa; RS *235.11*) sono elencate le informazioni che servono all'IFPDT per poter eventualmente intraprendere le azioni necessarie a tutelare le persone interessate dalla violazione della sicurezza dei dati, ad esempio ordinare che ricevano informazioni sull'incidente (cfr. n. 2).

1.2 Nofiticante

Le notifica all'IFPDT (così come l'informazione delle persone interessate) spettano al titolare del trattamento. Il responsabile del trattamento ha invece l'obbligo di informare il titolare del trattamento in caso di violazione della sicurezza dei dati. Tale obbligo di informazione non è subordinato a una valutazione dei rischi ai sensi dell'articolo 24 capoverso 1 LPD; il responsabile del trattamento deve informare il titolare del trattamento di qualsiasi violazione della sicurezza dei dati, indipendentemente dal fatto che essa comporti o meno un rischio elevato per la personalità o i diritti fondamentali dell'interessato.

1.3 Obbligo di notifica

In base all'articolo 24 capoverso 1 LPD il titolare del trattamento deve notificare quanto prima all'IFPDT ogni violazione della sicurezza dei dati di cui è venuto a conoscenza e che comporta verosimilmente un rischio elevato per la personalità o i diritti fondamentali della persona interessata. Se, al termine dell'analisi dei rischi condotta nei tempi ridotti tipici di una violazione della sicurezza dei dati, il titolare del trattamento rileva che verosimilmente sussiste un rischio elevato di questo tipo e che non può essere determinato con certezza definitiva o non può essere determinato in breve tempo (in merito al rischio v. n. 1.5), egli deve comunicare la violazione della sicurezza dei dati all'IFPDT. Ad esempio, in caso di attacchi ransomware, a seconda delle circostanze, in una prima analisi si dovrà presumere un «rischio presumibilmente elevato». Secondo la legge, il responsabile deve segnalarlo il più rapidamente possibile

e, di conseguenza, senza attendere l'esecuzione di accertamenti più lunghi che possano confermare o escludere senza dubbi il rischio presumibilmente elevato.

La notifica obbligatoria deve contenere tutte le informazioni riportate all'articolo 15 capoverso 1 OPDa, ma se sono soddisfatte le condizioni di cui al capoverso 2 è consentito fornire le informazioni mancanti anche successivamente (v. n. 1.4).

Se il titolare del trattamento non invia questa notifica, l'IFPDT, dopo essere venuto a conoscenza dell'incidente da altre fonti, può disporre che la notifica venga comunque inviata anche se in ritardo (art. 51 cpv. 3 lett. f LPD).

Dopo aver ricevuto la comunicazione, l'IFPDT verifica in modo sommario se le misure immediate e successive attuate o pianificate sono idonee, sufficienti e adeguate per quanto riguarda le tempistiche a tutelare le persone interessate e a ridurre gli effetti della violazione (cfr. art. 15 cpv. 1 lett. f OPDa). Se necessario, l'IFPDT può innanzitutto anche chiedere al titolare del trattamento di fornire maggiori dettagli sui fatti e sulle valutazioni riportati e di modificare o integrare le misure attuate o pianificate. L'IFPDT, eventualmente, può anche mettersi in contatto con il titolare del trattamento per accertare, ad esempio, che l'incidente sia stato documentato salvando i dati verbalizzati. Inoltre, verificherà che le persone interessate siano state adeguatamente informate in merito all'incidente e alle sue conseguenze (art. 15 cpv. 3 e 4 OPDa). Se il responsabile non si conforma alle richieste dell'IFPDT, quest'ultimo può avviare un'indagine formale ai sensi dell'art. 49 LPD e far rispettare le richieste con misure ai sensi dell'art. 51 LPD.

Infine, se ritiene che sia opportuno nell'interesse pubblico, in base all'articolo 57 capoverso 2 LPD l'IFPDT può informare il pubblico sui suoi accertamenti e sulle sue disposizioni.

1.4 Diritto di comunicazione

La pratica ha dimostrato che i titolari del trattamento desiderano talvolta notificare all'IFPDT anche violazioni della sicurezza dei dati per le quali non è stato identificato un rischio elevato. L'IFPDT raccoglie anche queste notifiche volontarie. Queste notifiche si rivelano utili per tutte le persone interessate e anche dal punto di vista dell'interesse pubblico in tutti quei casi in cui dall'analisi condotta, tenuto conto dei dati interessati, i rischi risultano essere ridotti, ma comunque potrebbero suscitare l'interesse dei media, ad esempio perché il numero di persone coinvolte è molto elevato (v. n. 1.5).

Dopo aver visionato a grandi linee la notifica, l'IFPDT decide se ordinare che vengano attuate o procedere direttamente con l'attuazione delle eventuali misure necessarie a informare le persone interessate o il pubblico.

1.5 Presentazione della notifica

Le notifiche devono essere presentate all'IFPDT quanto prima e devono riportare nel modo più completo possibile i fatti che hanno portato alla violazione della sicurezza dei dati e le relative conseguenze. Se non è in grado di comunicare contemporaneamente tutte le informazioni, il titolare del trattamento potrà fornire quelle mancanti successivamente ma comunque nel più breve tempo possibile (cfr. art. 15 cpv. 2 OPDa).

Per le notifiche obbligatorie l'IFPDT mette a disposizione un apposito portale (link) che garantisce la trasmissione sicura dei dati. Grazie al modulo interattivo, inoltre, viene garantito anche che la notifica contenga tutte le informazioni richieste all'articolo 15 capoverso 1 OPDa e quindi che l'obbligo di notifica sia assolto correttamente. Oltre a questo, il portale rilascia una conferma in cui è indicato il momento in cui è stata inviata la comunicazione e consente di inoltrare notifiche successive per integrare in qualsiasi momento una notifica precedente.

Le notifiche volontarie, invece, non vengono inviate attraverso il portale dedicato e, come spiegato in precedenza, in questi casi non è previsto alcun intervento d'ufficio dell'IFPDT.

1.6 Rischio elevato secondo l'articolo 24 capoverso 1 LPD

In base all'articolo 24 capoverso 1 LPD il titolare del trattamento deve notificare quanto prima all'IFPDT ogni violazione della sicurezza dei dati che comporta verosimilmente un rischio elevato per la personalità o i diritti fondamentali della persona interessata.

La LPD utilizza i termini «rischio elevato» e «rischio elevato verosimile» in numerose disposizioni. Per interpretare correttamente il concetto di «rischio elevato» è necessario però analizzare con la dovuta attenzione i diversi scopi di queste disposizioni.

Per valutare se vi è un rischio elevato in base a quanto disposto all'articolo 24 capoverso 1 LPD, i titolari del trattamento devono innanzitutto stabilire in che misura la violazione della sicurezza dei dati verificatasi ha già leso la personalità o i diritti fondamentali delle persone fisiche. Inoltre, dato il riferimento alla verosimiglianza presente nella norma, i titolari del trattamento nella loro valutazione devono tenere in considerazione anche le conseguenze che la violazione della sicurezza dei dati potrebbe avere per le potenziali persone interessate ma che, al momento in cui si deve stabilire se sussista l'obbligo di notifica, non possono né essere misurate in modo definitivo, né essere previste con sicurezza.

Il rischio elevato verosimile di cui all'articolo 24 capoverso 1 LPD deve essere individuato senza tenere conto delle misure che il titolare del trattamento ha pianificato, annunciato o attuato solo successivamente alla violazione della sicurezza dei dati. – In precedenza, invece, la prassi dell'IFPDT permetteva di tenere conto al momento della valutazione del rischio delle misure immediate che il titolare del trattamento poteva aver attuato prima ancora di inviare tempestivamente la notifica e che escludevano o riducevano in modo provato le conseguenze temute di una potenziale lesione della personalità. Ad esempio, nel caso in cui il titolare del trattamento attraverso le misure immediate adottate fosse riuscito a riprendere rapidamente il controllo sui database dei dati personali a cui non aveva potuto accedere per un periodo di tempo limitato e attraverso protocolli o altri indizi nel giro di qualche ora fosse riuscito a escludere con sufficiente probabilità che tali dati fossero stati trattati in modo improprio. In casi dubbi, però, se non si può quindi escludere con sufficiente probabilità che vi sia un rischio elevato, il titolare del trattamento deve adempiere senza indugio al proprio obbligo di notifica, ad esempio, se prima o dopo aver pagato il riscatto non è in grado di sapere come siano stati trattati dai cibercriminali i dati a cui ha di nuovo accesso.

I criteri per valutare la gravità dei possibili rischi derivanti dalla violazione della sicurezza dei dati sono i seguenti.

1.6.1 Gravità delle conseguenze:

per prima cosa è necessario stimare in che misura la personalità o i diritti fondamentali delle persone fisiche interessate siano stati già compromessi o si teme vengano lesi a seguito della violazione della sicurezza dei dati. Nell'effettuare questa valutazione è determinante la gravità del danno per la persona più gravemente colpita. Per stimare la gravità delle conseguenze si può fare ricorso ai seguenti criteri:

- il livello di protezione che deve essere garantito per i dati personali interessati. Il tipo di dati personali coinvolti nella violazione della sicurezza dei dati rappresenta un elemento centrale della valutazione. Più questi dati sono sensibili, infatti, maggiore è il rischio che siano stati lesi la personalità o i diritti fondamentali delle persone interessate. Se i dati sono dati personali degni di particolare protezione in base all'articolo 5 lettera c LPD, ad esempio dati sanitari, dati biometrici o dati concernenti le misure d'assistenza sociale, in molti casi bisogna presupporre che il rischio sia elevato. Ma esistono anche altri dati che, pur non rientrando in queste categorie, possono comportare un rischio elevato, ad esempio la perdita (o la copia) di documenti d'identità o le informazioni della carta di credito. A seconda del contesto nel quale vengono trattati i dati personali interessati dalla violazione della sicurezza, quindi, è necessario supporre che vi sia «verosimilmente un rischio elevato» anche quando i dati personali non sono degni di particolare protezione. Ad esempio, nel caso in cui la violazione della sicurezza dei dati riguardi indirizzi e dati di contatto trattati dalle persone autorizzate per scopi quali il perseguimento penale o le misure d'assistenza sociale, che solitamente rientrano nei dati degni di particolare protezione ai sensi dell'articolo 5 lettera c LPD. Se i dati personali interessati erano accessibili pubblicamente già prima della violazione della sicurezza dei dati, normalmente il rischio non deve essere valutato come elevato;
- tipo e circostanze della violazione nonché cerchia e motivi dei soggetti terzi non autorizzati. Ai fini della valutazione del rischio il fatto che la violazione della sicurezza dei dati sia da ricondurre a un errore umano, a un intento criminale o a un guasto tecnico può fare la differenza. A seconda di quale sia la causa, infatti, il rischio stimato può differire. Se i dati personali sottratti nel frattempo

sono stati messi a disposizione di un ampio pubblico, ad esempio tramite la pubblicazione sulla darknet, questo in generale deve far ipotizzare che il rischio sia elevato, indipendentemente dal fatto che i dati vi siano finiti per un guasto tecnico o a seguito di un'azione criminale. Nel caso in cui, invece, siano stati cancellati dei dati personali dal server del titolare del trattamento al solo scopo di provocare un danno, si può pensare che il rischio sia ridotto. Il fatto che il titolare del trattamento personalmente confidi, senza poterlo dimostrare in modo più preciso, nelle buone intenzioni dei soggetti sconosciuti destinatari dei dati, non permette invece di escludere un rischio oggettivamente elevato;

- sforzo necessario per risalire alle persone. Un altro fattore che deve essere preso in considerazione nella valutazione del rischio è il lavoro e le risorse economiche necessari per trattare le informazioni ottenute in modo illecito ed eventualmente messe anche a disposizione di un ampio pubblico, ad esempio tramite la darknet, in modo tale che sia possibile risalire a persone individuabili. Più è semplice risalire a una determinata persona a partire dai dati ottenuti in modo illecito, maggiore è il rischio per questa persona. Ad esempio, se la fuga di dati ha riguardato «solo» dei numeri clienti, ma non erano disponibili altri dati che, a partire da questi, permettevano di risalire alla persona interessata, il rischio è minore rispetto al caso in cui i dati ottenuti fossero stati indirizzi e-mail chiaramente associabili a una persona nome.cognome@XXXX.com.Se i dati personali interessati da una violazione della sicurezza dei dati erano stati crittografati in modo efficace dal titolare del trattamento, nessuno potrà leggerli senza la chiave. La legge in materia di protezione dei dati considera quindi questi dati anonimi per tutti i soggetti terzi non autorizzati all'accesso e pertanto in questi casi non si applica l'obbligo di notifica di cui all'articolo 24 capoverso 1 LPD. Al contrario, però, se i dati interessati da una violazione della sicurezza dei dati erano stati soltanto pseudonimizzati, questi saranno considerati dati personali e di conseguenza, se sussistono i requisiti, in caso di violazione si applica l'obbligo di notifica di cui alla suddetta disposizione;
- quantità e durata del trattamento. Un fattore determinante per stabilire la gravità dell'evento e che può essere preso in considerazione è la quantità di informazioni, relative a una stessa persona, oggetto della violazione della sicurezza dei dati e la durata del trattamento illecito;
- svantaggi ideali ed economici. Le singole persone interessate potranno subire conseguenze gravi nel caso in cui una violazione della sicurezza dei dati consenta abusi quali furto d'identità o truffe legate alle carte di credito, che comportano ad esempio danni alla reputazione, discriminazione o perdite di patrimonio e che, a loro volta, possono essere la causa di ripercussioni negative lesive della personalità, come preoccupazioni o paure;
- persone vulnerabili. Se una violazione della sicurezza dei dati riguarda, ad esempio, dati di minori o di persone con disabilità, anche in questo caso le conseguenze possono essere gravi;
- numero totale delle persone e dei dati interessati dalla violazione della sicurezza dei dati. Il fatto che l'evento abbia coinvolto un numero elevato di persone o una moltitudine di dati personali, da solo non basta per giustificare un rischio elevato. Quando le violazioni della sicurezza dei dati interessano molte persone può però esserci un interesse pubblico e privato a conoscere queste informazioni. Nella prassi capita non di rado che quando si verificano questi tipi di violazioni della sicurezza dei dati i titolari del trattamento inviino delle segnalazioni volontarie all'IFPDT (v. n. 1.3).

1.6.2 Probabilità che si arrivi alle conseguenze temute:

quando il titolare del trattamento si accorge che si è verificata una violazione della sicurezza dei dati, deve valutare con quale probabilità le conseguenze di tale violazione che non si possono ancora stimare in modo definitivo, o che non si sono ancora realizzate, potranno effettivamente raggiungere il danno potenziale temuto per la maggior parte delle persone interessate. Ad esempio, se la violazione della sicurezza dei dati avviene in un ospedale, che oltre a dati amministrativi e scientifici non personali tratta anche un elevato numero di dati personali degni di particolare protezione, il danno potenziale stimato dovrà essere maggiore rispetto a quello che si ipotizzerebbe se, ad esempio, l'incidente avesse coinvolto un rivenditore di prodotti alimentari. Quindi, quando in un ospedale si verifica una violazione della sicurezza dei dati, il titolare del trattamento per inviare la notifica all'IFPDT non deve aspettare di avere la certezza che l'incidente non abbia riguardato soltanto delle informazioni non personali ma anche dati personali dei propri pazienti. Quando si valuta la probabilità che si verifichino determinate ipotesi devono

essere escluse le misure pianificate, annunciate o attuate dal titolare del trattamento dopo che si è verificata la violazione della sicurezza dei dati. Ciò significa che i titolari del trattamento non devono aspettare l'attuazione e la valutazione delle misure future per comunicare all'IFPDT una violazione della sicurezza dei dati che, dato l'elevato potenziale di danno che può arrecare, è assoggettata all'obbligo di notifica.

1.7 Notifica di violazioni della sicurezza dei dati all'IFPDT e principio di trasparenza

L'attività dell'IFPDT in qualità di autorità di controllo della Confederazione per la protezione dei dati sottostà alla legge del 17 dicembre 2004 sulla trasparenza (LTras; RS *152.3*). Le notifiche inviate in qualsivoglia forma dal titolare del trattamento, così come eventuali scambi tra l'IFPDT e il titolare del trattamento o il suo responsabile del trattamento, in generale devono essere considerati documenti ufficiali ai sensi della LTras. I documenti ufficiali ricevuti dall'IFPDT nell'ambito del suo mandato legale per la gestione delle violazioni della sicurezza dei dati sono quindi in linea di principio accessibili al pubblico secondo quanto stabilito dalla LTras. Questo vale segnatamente per tutte le notifiche di violazioni della sicurezza dei dati, indipendentemente dal fatto che siano state inviate per adempiere all'obbligo di notifica di cui all'articolo 24 capoverso 1 LPD o in modo volontario. Per quanto riguarda la gestione delle domande di accesso fondate sulla LTras l'IFPDT valuta se e in che misura è possibile limitare o differire un eventuale accesso in base alle disposizioni derogatorie di cui all'articolo 7 e seguenti LTras. Durante la procedura l'IFPDT, se necessario, deve ascoltare i soggetti terzi interessati prima di pronunciarsi. La decisione circa la possibilità di accedere viene comunicata attraverso una presa di posizione o, su richiesta, con l'emanazione di una decisione. Non viene svolta una procedura di mediazione come descritto all'articolo 13 LTras. (cfr. sentenza del Tribunale amministrativo federale A-4781/2019 del 17 giugno 2020 consid. 3).

1.8 Obbligo di notifica e sanzioni

Se, pur essendovi obbligato in base all'articolo 24 capoverso 1 LPD, il titolare del trattamento non ha comunicato la violazione della sicurezza dei dati all'IFPDT, nel momento in cui quest'ultimo viene a conoscenza dell'accaduto in altro modo può disporre che l'obbligo di notifica venga comunque assolto, anche se in ritardo (art. 51 cpv. 3 lett. f LPD). In relazione alla violazione della sicurezza dei dati l'IFPDT può disporre anche altre misure amministrative, ad esempio nel caso in cui non siano rispettate le disposizioni di cui all'articolo 8 LPD.

La LPD non prevede sanzioni penali in caso di mancato rispetto totale o parziale dell'obbligo di notifica in sé. Una violazione della sicurezza dei dati può però essere rilevante dal punto di vista penale nel caso in cui, ad esempio, il titolare del trattamento non ha rispettato i requisiti minimi in materia di sicurezza dei dati (art. 61 lett. c LPD). L'articolo 24 capoverso 6 LPD prevede in merito che le notifiche obbligatorie non possano essere usate nel quadro di un procedimento penale contro la persona soggetta all'obbligo di notifica senza il suo consenso. Questo vale anche per le notifiche volontarie (cfr. Basler Kommentar Datenschutzgesetz, 4a edizione [BSK] art. 24 n. marg. 98 con rimando a P. MEIER/S. MÉTILLE, in P. Meier/S. Métille (a c. di), *Commentaire romand, Loi fédérale sur la protection des données*, Basilea 2023, art. 24 n. marg. 35).

2 Informazione alle persone interessate dalla violazione della sicurezza dei dati

L'obbligo di notifica del titolare del trattamento di cui all'articolo 24 capoverso 1 LPD deve essere distinto dal suo obbligo di informare le persone interessate dalla violazione della sicurezza dei dati. In base all'articolo 24 capoverso 4 LPD il titolare del trattamento deve informare le persone interessate della violazione della sicurezza dei dati se ciò è necessario per proteggerle o se lo esige l'IFPDT.

L'obbligo di informazione nei confronti delle persone interessate di cui al capoverso 4 deve essere interpretato in modo indipendente dal capoverso 1 e dal concetto ivi utilizzato di rischio elevato (cfr. Mathys/Thomann, in Vasella/Blechta (a c. di), BSK art. 24 n. marg. 63).

Se il titolare del trattamento può dimostrare che non è necessario fornire ulteriori informazioni, perché le persone interessate sono già sufficientemente informate sulla violazione della sicurezza dei dati e le relative conseguenze e sanno quali sono le misure che possono o devono attuare per proteggersi, l'obbligo di informare può essere considerato assolto.

2.1 Obbligo di informare per la necessità di proteggere le persone interessate

Si deve supporre che sussista la necessità di proteggere le persone interessate menzionata all'articolo 24 capoverso 4 LPD, nel caso in cui tali persone possano o debbano prendere dei provvedimenti per ridurre o scongiurare un danno derivante dalla violazione della sicurezza dei dati. Ad esempio, quando devono modificare i loro dati d'accesso o le loro parole chiave (cfr. messaggio del 15 set. 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, in particolare 6053). La necessità di proteggere le persone interessate può sussistere però anche in altri casi, ad esempio quando è necessario bloccare una carta di credito o analizzare in modo critico estratti conto o messaggi e richieste, le cosiddette e-mail di phishing (cfr. MATHYS/THOMANN, BSK, art. 24 n. marg. 67).

Il rischio elevato verosimile di cui all'articolo 24 capoverso 1 LPD che determina l'obbligo di notifica del titolare del trattamento all'IFPDT, non costituisce un presupposto legale che motiva l'obbligo di informare le persone interessate in base al capoverso 4 di questo articolo. L'obbligo di informare può sussistere anche nel caso in cui il titolare del trattamento possa escludere un rischio oggettivamente elevato sulla base delle proprie conoscenze da insider e attraverso argomentazioni accettabili, ma le persone potenzialmente interessate dalla violazione della sicurezza dei dati, non conoscendo la situazione, temono il peggio. Al contrario, nel caso vi sia verosimilmente un rischio elevato in base all'articolo 24 capoverso 1 LPD, di solito vi è anche l'obbligo di informare secondo quanto disposto dal capoverso 4 della stessa disposizione.

2.2 Obbligo di informazione in base a un ordine dell'IFPDT

Secondo l'articolo 24 capoverso 4 LPD, l'IFPDT può esigere che il titolare del trattamento informi le persone interessate. L'IFPDT è autorizzato a impartire un ordine di questo tipo a prescindere che sia stato informato prima della violazione dal titolare del trattamento in modo volontario o in adempimento dell'obbligo di notifica di cui all'articolo 24 capoverso 1 LPD o non sia stato affatto informato.

L'IFPDT richiede al titolare del trattamento di informare le persone interessate nel caso in cui a suo parere sia necessario proteggerle dalla violazione della sicurezza dei dati. Inoltre, può formulare questa richiesta anche perché a suo giudizio, dato l'elevato numero di persone interessate o la copertura da parte dei media, è di pubblico interesse che il titolare del trattamento fornisca in modo adeguato informazioni più dettagliate sulle conseguenze di una violazione della sicurezza dei dati al numero elevato di persone interessate e, così facendo, in modo indiretto anche al vasto pubblico. Un interesse di questo tipo può sussistere in particolare nel caso in cui tale misura sia in grado di evitare o ridurre sensibilmente le conseguenze che potrebbero instillare paure e dare adito a speculazioni tra il vasto pubblico. Nella prassi proprio in questi casi i titolari del trattamento non di rado decidono di segnalare volontariamente l'accaduto all'IFPDT, il quale li accoglie sempre con favore (v. n. 1.3; Diritto di comunicazione).

In linea di principio in queste circostanze l'IFPDT, in base all'articolo 57 capoverso 2 LPD, è autorizzato a informare il pubblico sui suoi accertamenti e sulle sue raccomandazioni in merito, in quanto si tratta di casi d'interesse generale. Solitamente, però, la comunicazione è molto più efficace quando il titolare del trattamento informa in modo indipendente le persone interessate.

2.3 Informazione

In base all'articolo 15 capoverso 3 OPDa le informazioni devono essere comunicate alle persone interessate «in una lingua semplice e comprensibile» ed è necessario fornire almeno le seguenti informazioni: tipo di violazione, quindi cosa è successo; conseguenze della violazione, compresi i rischi per le persone interessate, quali misure sono state attuate o sono previste, da un lato per risolvere il problema e dall'altro per ridurre le conseguenze. Nella comunicazione deve essere fornito anche il nome e i dati di contatto di un referente.

Fatti salvi questi requisiti, non esistono disposizioni di tipo formale su come deve avvenire l'informazione. Il titolare del trattamento può scegliere liberamente il metodo che ritiene opportuno.

In linea di principio le persone interessate dovrebbero essere informate direttamente e in modo personale. In casi eccezionali è possibile ricorrere a una comunicazione pubblica, come previsto

all’articolo 24 capoverso 5 lettera c LPD, se è possibile garantire l’informazione delle singole persone interessate in modo equivalente. Attraverso la comunicazione pubblica, però, l’obbligo di informare non viene abolito, ma solo modificato (cfr. CÉLIAN HIRSCH, *Le devoir d’informer lors d’une violation de la sécurité des données. Avec un regard particulier sur les données bancaires*, Ginevra 2023, p. 315).

2.4 Obbligo di informare e sanzioni

Se il titolare del trattamento, in base all’articolo 24 capoverso 4 LPD, doveva informare le persone interessate di una violazione della sicurezza dei dati perché queste dovevano essere protette o su richiesta dell’IFPDT, in caso di mancata informazione o di rifiuto a informare l’IFPDT può disporre che l’obbligo di informazione venga assolto comunque, seppur in ritardo (art. 51 cpv. 3 lett. f LPD). In relazione alla violazione della sicurezza dei dati l’IFPDT può disporre anche altre misure amministrative, ad esempio nel caso in cui non siano rispettate le disposizioni di cui all’articolo 8 LPD.