GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

ISTITUTO COMPRENSIVO - "IGNAZIO SILONE"-LUCO DEI MARSI
Prot. 0009228 del 14/11/2025
I-4 (Uscita)

18/IT

WP250rev.01

Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679

adottate il 3 ottobre 2017

Versione emendata e adottata in data 6 febbraio 2018

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B-1049 Bruxelles, Belgio, ufficio MO-59 05/35.

Sito Internet: ://ec.europa.eu/justice/data-protection/index_en.htm

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 della stessa,

visto il suo regolamento interno,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

INDICE

INTRODUZIONE **5**

I. NOTIFICA DELLE VIOLAZIONI DEI DATI PERSONALI AI SENSI DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI **6**

A. CONSIDERAZIONI DI BASE IN MATERIA DI SICUREZZA 6

B. CHE COS'È UNA VIOLAZIONE DEI DATI PERSONALI? 7

1. Definizione *7*

2. Tipi di violazioni dei dati personali *8*

3. Possibili conseguenze di una violazione dei dati personali *10*

II. ARTICOLO 33 - NOTIFICA ALL'AUTORITÀ DI CONTROLLO **11**

A. QUANDO EFFETTUARE LA NOTIFICA 11

1. Prescrizioni dell'articolo 33 ..... *11*

2. Quando il titolare del trattamento viene "a conoscenza" di una violazione? *11*

3. Contitolari del trattamento *14*

4. Obblighi del responsabile del trattamento *14*

B. FORNIRE INFORMAZIONI ALL'AUTORITÀ DI CONTROLLO 15

1. Informazioni da fornire *15*

2. Notifica per fasi *16*

3. Notifiche effettuate in ritardo *17*

C. VIOLAZIONI TRANSFRONTALIERE E VIOLAZIONI PRESSO STABILIMENTI NON UE 18

1. Violazioni transfrontaliere *18*

2. Violazioni presso stabilimenti non UE *19*

D. CIRCOSTANZE NELLE QUALI NON È RICHIESTA LA NOTIFICA 20

III. ARTICOLO 34 – COMUNICAZIONE ALL'INTERESSATO **21**

A. INFORMARE L'INTERESSATO 21

B. INFORMAZIONI DA FORNIRE 22

C. CONTATTARE L'INTERESSATO 22

D. CIRCOSTANZE NELLE QUALI NON È RICHIESTA LA COMUNICAZIONE 24

IV. VALUTAZIONE DELL'ESISTENZA DI UN RISCHIO O DI UN RISCHIO ELEVATO **25**

A. RISCHIO COME FATTORE CHE FA SCATTARE L'OBBLIGO DI NOTIFICA 25

B. FATTORI DA CONSIDERARE NELLA VALUTAZIONE DEL RISCHIO 25

V. RESPONSABILIZZAZIONE E TENUTA DI REGISTRI **29**

A. DOCUMENTARE LE VIOLAZIONI 29

B. RUOLO DEL RESPONSABILE DELLA PROTEZIONE DEI DATI 30

VI. OBBLIGHI DI NOTIFICA A NORMA DI ALTRI STRUMENTI GIURIDICI 31

VII. ALLEGATO 33

A. DIAGRAMMA DI FLUSSO CHE ILLUSTRA GLI OBBLIGHI DI NOTIFICA 33

B. ESEMPI DI VIOLAZIONI DEI DATI PERSONALI E DEI SOGGETTI A CUI NOTIFICARLE 34

INTRODUZIONE

Il regolamento generale sulla protezione dei dati introduce l'obbligo di notificare una violazione dei dati personali (in appresso: "violazione") all'autorità di controllo[1] nazionale competente (oppure, in caso di violazione transfrontaliera, all'autorità capofila) e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione.

Attualmente l'obbligo di notifica delle violazioni esiste già per determinate organizzazioni, quali i fornitori di servizi di comunicazione elettronica accessibili al pubblico (come specificato nella direttiva 2009/136/CE e nel regolamento (UE) n. 611/2013)[2]. Inoltre, alcuni Stati membri dell'UE prevedono già un obbligo nazionale di notifica delle violazioni, che può consistere nell'obbligo di notificare violazioni che coinvolgono categorie di titolari del trattamento diversi dai fornitori di servizi di comunicazione elettronica accessibili al pubblico (ad esempio Germania e Italia) oppure nell'obbligo di segnalare tutte le violazioni riguardanti dati personali (ad esempio Paesi Bassi). Altri Stati membri dispongono di codici di buona pratica (ad esempio Irlanda[3]). Sebbene un certo numero di autorità di protezione dei dati dell'UE incoraggi già il titolare del trattamento a segnalare le violazioni, la direttiva 95/46/CE sulla protezione dei dati[4], che viene sostituita dal regolamento generale sulla protezione dei dati, non contiene uno obbligo specifico di notifica delle violazioni, pertanto tale obbligo sarà nuovo per numerose organizzazioni. Il regolamento generale sulla protezione dei dati rende ora la notifica obbligatoria per tutti i titolari del trattamento a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche[5]. Anche i responsabili del trattamento hanno un ruolo importante da svolgere e devono notificare qualsiasi violazione al proprio titolare del trattamento[6].

Il Gruppo di lavoro articolo 29 ("Gruppo di lavoro") ritiene che il nuovo obbligo di notifica presenti una serie di vantaggi. All'atto della notifica all'autorità di controllo, il titolare del trattamento può ottenere consulenza sull'eventuale necessità di informare le persone fisiche interessate. In effetti l'autorità di controllo può ordinare al titolare del trattamento di informare le persone fisiche interessate dalla violazione[7]. La comunicazione della violazione alle persone fisiche interessate consente al titolare del trattamento di fornire loro informazioni sui rischi derivanti dalla violazione e sui provvedimenti che esse possono prendere per proteggersi dalle potenziali conseguenze della violazione. Qualsiasi piano di risposta alle violazioni dovrebbe mirare a proteggere le persone fisiche e i loro dati personali. Di conseguenza, la notifica della violazione dovrebbe essere vista come uno

[1] Cfr. l'articolo 4, punto 21, del regolamento generale sulla protezione dei dati.

[2] Cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32009L0136 e http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32013R0611.

[3] Cfr. (in inglese) https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm.

[4] Cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:31995L0046.

[5] I diritti sanciti dalla Carta dei diritti fondamentali dell'Unione europea, disponibile all'indirizzo: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:12012P/TXT.

[6] Cfr. articolo 33, paragrafo 2. Questo concetto è analogo all'articolo 5 del regolamento (UE) n. 611/2013 nel quale si afferma che un fornitore incaricato di erogare una parte dei servizi di comunicazione elettronica (che non ha un legame contrattuale diretto con gli abbonati) è tenuto a notificare il fornitore che lo ha ingaggiato in caso di violazione di dati personali.

[7] Cfr. articolo 34, paragrafo 4 e articolo 58, paragrafo 2, lettera e).

strumento per migliorare la conformità in materia di protezione dei dati personali. Allo stesso tempo, va osservato che la mancata segnalazione di una violazione a una persona fisica o all'autorità di controllo può comportare l'imposizione di una sanzione al titolare del trattamento ai sensi dell'articolo 83.

I titolari e i responsabili del trattamento sono pertanto incoraggiati a pianificare anticipatamente e a mettere in atto processi per essere in grado di rilevare e limitare tempestivamente gli effetti di una violazione, valutare il rischio per le persone fisiche[8] e stabilire se sia necessario notificare la violazione all'autorità di controllo competente e comunicarla alle persone fisiche interessate, ove necessario. La notifica all'autorità di controllo dovrebbe costituire parte del piano di intervento in caso di incidente.

Il regolamento contiene disposizioni che specificano quando e a chi la violazione deve essere notificata e quali informazioni devono essere fornite nel contesto della notifica. Le informazioni richieste per la notifica possono essere fornite procedendo per fasi, tuttavia il titolare del trattamento deve agire sempre in maniera tempestiva in caso di violazione.

Nel parere 03/2014 sulla notifica delle violazioni dei dati personali[9], il Gruppo di lavoro ha fornito orientamenti ai titolari del trattamento per aiutarli a decidere se effettuare la notifica agli interessati in caso di violazione. Il parere ha preso in considerazione l'obbligo dei fornitori di comunicazioni elettroniche ai sensi della direttiva 2002/58/CE e ha fornito esempi afferenti a più settori, nel contesto dell'allora progetto di regolamento generale sulla protezione dei dati, e ha illustrato le buone prassi per tutti i titolari del trattamento.

Le presenti linee guida spiegano gli obblighi di notifica e di comunicazione delle violazioni sanciti dal regolamento, nonché alcune misure che i titolari e i responsabili del trattamento possono intraprendere per soddisfare questi nuovi obblighi. Forniscono inoltre esempi di vari tipi di violazioni e i soggetti ai quali esse devono essere notificate nei diversi scenari.

I. Notifica delle violazioni dei dati personali ai sensi del regolamento generale sulla protezione dei dati

A. Considerazioni di base in materia di sicurezza

Una delle prescrizioni del regolamento prevede che, mediante misure tecniche e organizzative adeguate, i dati personali siano trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali[10].

Di conseguenza, il regolamento impone tanto al titolare quanto al responsabile del trattamento di disporre di misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati. Tali soggetti dovrebbero tenere conto: dello stato

[8] Ciò può essere garantito rispettando l'obbligo di monitoraggio e riesame previsto da una valutazione d'impatto sulla protezione dei dati, richiesta per i trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche (articolo 35, paragrafi 1 e 11).

[9] Cfr. parere 03/2014 sulla notifica delle violazioni dei dati personali (in inglese) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

[10] Cfr. articolo 5, paragrafo 1, lettera f) e articolo 32.

dell'arte e dei costi di attuazione; della natura, dell'oggetto, del contesto e delle finalità del trattamento; del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche[11]. Inoltre, il regolamento impone di mettere in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali, il che a sua volta consente di stabilire se scatta l'obbligo di notifica[12].

Di conseguenza, un aspetto fondamentale di qualsiasi politica di sicurezza dei dati è la capacità, ove possibile, di prevenire una violazione e, laddove essa si verifichi ciò nonostante, di reagire tempestivamente.

B. Che cos'è una violazione dei dati personali?

1. Definizione

Per poter porre rimedio a una violazione occorre innanzitutto che il titolare del trattamento sia in grado di riconoscerla. All'articolo 4, punto 12, il regolamento definisce la "violazione dei dati personali" come segue:

> "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Il significato di "distruzione" dei dati personali dovrebbe essere abbastanza chiaro: si ha distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento. Anche il concetto di "danno" dovrebbe essere relativamente evidente: si verifica un danno quando i dati personali sono stati modificati, corrotti o non sono più completi. Con "perdita" dei dati personali si dovrebbe invece intendere il caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso. Infine, un trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del regolamento.

Esempio

Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del titolare del trattamento. Un altro esempio può essere il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un *ransomware* (*malware* del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso.

Ciò che dovrebbe essere chiaro è che una violazione è un tipo di incidente di sicurezza. Tuttavia, come indicato all'articolo 4, punto 12, il regolamento si applica soltanto in caso di violazione di *dati personali*. La conseguenza di tale violazione è che il titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del regolamento. Questo punto mette in luce la differenza tra un incidente di sicurezza e una violazione

[11] Articolo 32; cfr. anche considerando 83.

[12] Cfr. considerando 87.

dei dati personali: mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali[13].

I potenziali effetti negativi di una violazione sulle persone fisiche sono esaminati in appresso.

2. Tipi di violazioni dei dati personali

Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro ha spiegato che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni[14]:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazione della disponibilità", in caso di perdita, accesso[15] o distruzione accidentali o non autorizzati di dati personali.

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Mentre stabilire se vi sia stata una violazione della riservatezza o dell'integrità è relativamente evidente, può essere meno ovvio determinare se vi è stata una violazione della disponibilità. Una violazione sarà sempre considerata una violazione della disponibilità se si è verificata una perdita o una distruzione permanente dei dati personali.

Esempio

Esempi di perdita di disponibilità possono aversi quando i dati vengono cancellati accidentalmente o da una persona non autorizzata, oppure, in caso di dati crittografati in maniera sicura, quando la chiave di decifratura viene persa. Se il titolare del trattamento non è in grado di ripristinare l'accesso ai dati, ad esempio ricorrendo a un backup, la perdita di disponibilità sarà considerata permanente.

Può verificarsi perdita di disponibilità anche in caso di interruzione significativa del servizio abituale di un'organizzazione, ad esempio un'interruzione di corrente o attacco da "blocco di servizio" (*denial of service*) che rende i dati personali indisponibili.

Ci si potrebbe chiedere se una perdita temporanea della disponibilità dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. L'articolo 32 del

[13] Va osservato che un incidente di sicurezza non si limita ai modelli di minacce nei quali un attacco viene effettuato ai danni di un'organizzazione dall'esterno della stessa, bensì include anche incidenti derivanti dal trattamento interno che violano i principi di sicurezza.

[14] Cfr. parere 03/2014.

[15] È un fatto assodato che "l'accesso" è una componente fondamentale della "disponibilità". Cfr. ad esempio il documento NIST SP800-53rev4, che definisce la "disponibilità" come la "garanzia di un accesso e un uso tempestivi e affidabili delle informazioni", disponibile (in inglese) all'indirizzo http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Anche il documento CNSSI-4009 fa riferimento a un "accesso tempestivo e affidabile ai dati e ai servizi dell'informazione per gli utenti autorizzati." Cfr. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. Anche la norma ISO/IEC 27000:2016 definisce la "disponibilità" come la "proprietà di essere accessibile e utilizzabile su richiesta da un soggetto autorizzato": (in inglese) https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en.

regolamento ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".

Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'articolo 4, punto 12.

Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrebbe essere documentata in conformità all'articolo 33, paragrafo 5. Ciò aiuta il titolare del trattamento a dimostrare l'assunzione di responsabilità all'autorità di controllo, che potrebbe chiedere di consultare tali registrazioni[16]. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte. Il titolare del trattamento dovrà valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all'articolo 33, il titolare del trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso.

Esempi

L'indisponibilità, anche solo temporanea, di dati medici critici di pazienti di un ospedale potrebbe presentare un rischio per i diritti e le libertà delle persone interessate, poiché, ad esempio, potrebbe comportare l'annullamento di operazioni e mettere a rischio le vite dei pazienti.

Viceversa, se i sistemi di una società di comunicazione non sono disponibili per diverse ore (ad esempio a causa di un'interruzione dell'alimentazione) e tale società non riesce a inviare newsletter ai propri abbonati è improbabile che ciò presenti un rischio per i diritti e le libertà delle persone fisiche.

Va notato che, sebbene una perdita di disponibilità dei sistemi del titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il titolare del trattamento consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi.

Esempio

Un'infezione da *ransomware* (software dannoso che cifra i dati del titolare del trattamento finché non viene pagato un riscatto) potrebbe comportare una perdita temporanea di disponibilità se i dati possono essere ripristinati da un backup. Tuttavia, si è comunque verificata un'intrusione nella rete e potrebbe essere richiesta una notifica se l'incidente è qualificato come violazione della riservatezza (ad esempio se chi ha effettuato l'attacco ha avuto accesso a dati personali) e ciò presenta un rischio per i diritti e le libertà delle persone fisiche.

[16] Cfr. articolo 33, paragrafo 5.

3. Possibili conseguenze di una violazione dei dati personali

Una violazione può avere potenzialmente numerosi effetti negativi significativi sulle persone fisiche, che possono causare danni fisici, materiali o immateriali, ad esempio la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo alle persone fisiche interessate[17].

Di conseguenza, il regolamento impone al titolare del trattamento di notificare le violazioni all'autorità di controllo competente, fatta salva l'improbabilità che la violazione presenti il rischio che si verifichino detti effetti negativi. Laddove sia altamente probabile che tali effetti negativi si verifichino, il regolamento impone al titolare del trattamento di comunicare la violazione alle persone fisiche interessate non appena ciò sia ragionevolmente fattibile[18].

L'importanza di essere in grado di identificare una violazione, di valutare il rischio per le persone fisiche e, di conseguenza, di effettuare la notifica se necessario, è sottolineata nel considerando 87 del regolamento:

> "È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento".

Ulteriori linee guida sulla valutazione del rischio di effetti negativi per le persone fisiche sono considerate nella sezione IV.

Se il titolare del trattamento omette di notificare una violazione dei dati all'autorità di controllo o agli interessati oppure a entrambi, nonostante siano soddisfatte le prescrizioni di cui agli articoli 33 e/o 34, l'autorità di controllo dovrà effettuare una scelta e prendere in considerazione tutte le misure correttive a sua disposizione, tra cui l'imposizione di una sanzione amministrativa pecuniaria appropriata[19], in associazione a una misura correttiva ai sensi dell'articolo 58, paragrafo 2, oppure come sanzione indipendente. Qualora l'autorità opti per una sanzione amministrativa pecuniaria il suo valore può ammontare fino a un massimo di 10 000 000 EUR o fino al 2% del fatturato totale annuo globale di un'impresa ai sensi dell'articolo 83, paragrafo 4, lettera a), del regolamento. È altresì importante ricordare che, in alcuni casi, la mancata notifica di una violazione potrebbe rivelare l'assenza di misure di sicurezza o la loro inadeguatezza. Gli orientamenti del Gruppo di lavoro in materia di sanzioni amministrative affermano che "qualora nell'ambito di un singolo caso siano state commesse congiuntamente più violazioni diverse, l'autorità di controllo può applicare le sanzioni amministrative pecuniarie a un livello che risulti effettivo, proporzionato e dissuasivo entro i limiti

[17] Cfr. anche considerando 85 e 75.

[18] Cfr. anche il considerando 86.

[19] Per ulteriori dettagli, consultare le linee guida del Gruppo di lavoro riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie disponibili qui: https://www.garanteprivacy.it/documents/10160/0/WP+253++Linee+guida+sanzioni+amministrative+pecuniarie+Reg+UE+2016+679.

della violazione più grave". In tal caso, l'autorità di controllo avrà altresì la possibilità di comminare sanzioni per la mancata notifica o comunicazione della violazione (articoli 33 e 34), da un lato, e l'assenza di misure di sicurezza (adeguate) (articolo 32), dall'altro, in quanto si tratta di due infrazioni separate.

II. Articolo 33 - Notifica all'autorità di controllo

A. Quando effettuare la notifica

1. Prescrizioni dell'articolo 33

L'articolo 33, paragrafo 1, stabilisce che:

> "In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".

Il considerando 87[20] stabilisce che:

> "È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento".

2. Quando il titolare del trattamento viene "a conoscenza" di una violazione?

Come indicato in precedenza, il regolamento impone al titolare del trattamento di notificare una violazione senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Questo solleva la questione relativa al momento in cui il titolare del trattamento può considerarsi "a conoscenza" di una violazione. Il Gruppo di lavoro ritiene che il titolare del trattamento debba considerarsi "a conoscenza" nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali.

Tuttavia, come già osservato, il regolamento impone al titolare del trattamento di attuare tutte le misure tecniche e organizzative di protezione adeguate per stabilire immediatamente se si è verificata una violazione e informare tempestivamente l'autorità di controllo e gli interessati. Afferma altresì che è opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione e delle sue conseguenze e dei suoi effetti negativi per l'interessato[21]. Il titolare del trattamento è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate.

[20] Anche il considerando 85 è importante in questo caso.

[21] Cfr. considerando 87.

Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

Esempi

1. In caso di perdita di una chiave USB contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati. Tuttavia, anche se il titolare del trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, tale caso deve essere notificato, in quanto sussiste una ragionevole certezza del fatto che si è verificata una violazione della disponibilità; il titolare del trattamento si considera venuto "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB.

2. Un terzo informa il titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata. Dato che al titolare del trattamento è stata presentata una prova evidente di una violazione della riservatezza, non vi è dubbio che ne sia venuto "a conoscenza".

3. Un titolare del trattamento rileva che c'è stata una possibile intrusione nella sua rete. Controlla quindi i propri sistemi per stabilire se i dati personali ivi presenti sono stati compromessi e ne ottiene conferma. Ancora una volta, dato che il titolare del trattamento ha una chiara prova di una violazione non può esserci dubbio che sia venuto "a conoscenza" della stessa.

4. Un criminale informatico viola il sistema del titolare del trattamento e lo contatta per chiedere un riscatto. In tal caso, dopo aver verificato il suo sistema per accertarsi dell'attacco, il titolare del trattamento dispone di prove evidenti che si è verificata una violazione e non vi è dubbio che ne sia venuto a conoscenza.

Se una persona, un'organizzazione di comunicazione o un'altra fonte informa il titolare del trattamento di una potenziale violazione o se egli stesso rileva un incidente di sicurezza, il titolare del trattamento può effettuare una breve indagine per stabilire se la violazione si sia effettivamente verificata. Durante il periodo di indagine il titolare del trattamento non può essere considerato "a conoscenza". Tuttavia, si prevede che l'indagine iniziale inizi il più presto possibile e stabilisca con ragionevole certezza se si è verificata una violazione; può quindi seguire un'indagine più dettagliata.

Dopo che il titolare del trattamento è venuto a conoscenza di una violazione soggetta a notifica, la stessa deve essere notificata senza ingiustificato ritardo e, ove possibile, entro 72 ore. Durante questo periodo il titolare del trattamento dovrebbe valutare il rischio probabile per le persone fisiche al fine di stabilire se è soddisfatto il requisito per la notifica e quali siano le azioni necessarie per far fronte alla violazione. Tuttavia, il titolare del trattamento potrebbe già disporre di una valutazione iniziale del rischio potenziale che potrebbe derivare da una violazione come parte di una valutazione d'impatto sulla protezione dei dati[22] effettuata prima dello svolgimento del trattamento interessato. Tuttavia, tale valutazione può essere più generale rispetto alle circostanze specifiche di un'effettiva violazione e, pertanto, in ogni caso dovrà essere effettuata una valutazione aggiuntiva che tenga conto di tali circostanze. Per maggiori dettagli sulla valutazione del rischio, si rinvia alla sezione IV.

[22] Cfr. le linee guida del Gruppo di lavoro in materia di valutazioni d'impatto sulla protezione dei dati qui: https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati.

Nella maggior parte dei casi queste azioni preliminari dovrebbero essere completate subito dopo l'allerta iniziale (ossia quando il titolare o il responsabile del trattamento sospetta che si sia verificato un incidente di sicurezza che potrebbe interessare dati personali); dovrebbe richiedere più tempo soltanto in casi eccezionali.

Esempio

Una persona informa il titolare del trattamento di aver ricevuto un'e-mail da un soggetto che si fa passare per il titolare del trattamento, contenente dati personali relativi al suo (effettivo) utilizzo del servizio del titolare del trattamento, aspetto questo che suggerisce che la sicurezza del titolare del trattamento sia stata compromessa. Il titolare del trattamento conduce una breve indagine e individua un'intrusione nella propria rete e la prova di un accesso non autorizzato ai dati personali. Il titolare del trattamento si considera "a conoscenza" della violazione in questo momento e dovrà procedere alla notifica all'autorità di controllo a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Il titolare del trattamento dovrà prendere le opportune misure correttive per far fronte alla violazione.

Di conseguenza, il titolare del trattamento dovrebbe disporre di procedure interne per poter rilevare una violazione e porvi rimedio. Ad esempio, per rilevare talune irregolarità nel trattamento dei dati, il titolare o il responsabile del trattamento può utilizzare alcune misure tecniche certe come il flusso di dati e gli analizzatori di registri, dai quali è possibile definire eventi e allerte correlando qualsiasi dato di registro[23]. È importante che quando viene rilevata una violazione, la stessa venga segnalata al livello superiore appropriato di gestione, in maniera da poter essere trattata e, se del caso, notificata in conformità all'articolo 33 e, se necessario, all'articolo 34. Tali misure e meccanismi di segnalazione potrebbero essere dettagliati nei piani di intervento in caso di incidente del titolare del trattamento e/o nei dispositivi di governo societario. Ciò consentirà al titolare del trattamento di pianificare in maniera efficace e di stabilire chi ha la responsabilità operativa all'interno dell'organizzazione per la gestione di una violazione, nonché le modalità o l'opportunità di segnalare un incidente al livello gerarchico superiore, se del caso.

Il titolare del trattamento dovrebbe inoltre disporre di accordi con i responsabili del trattamento ai quali fa ricorso, i quali hanno a loro volta l'obbligo di notificare al titolare del trattamento eventuali violazioni (cfr. in appresso).

Sebbene spetti al titolare e al responsabile del trattamento mettere in atto misure adeguate per essere in grado di prevenire, reagire e affrontare una violazione, alcune misure pratiche dovrebbero essere prese in ogni caso:

- le informazioni relative a tutti gli eventi concernenti la sicurezza dovrebbero essere indirizzate a una persona responsabile o alle persone incaricate di gestire gli incidenti, stabilire l'esistenza di una violazione e valutare il rischio;
- il rischio per le persone fisiche a seguito di una violazione dovrebbe quindi essere valutato (probabilità di nessun rischio, di rischio o di rischio elevato) e le sezioni pertinenti dell'organizzazione dovrebbero esserne informate;
- se necessario si dovrebbe procedere alla notifica all'autorità di controllo ed eventualmente alla comunicazione della violazione alle persone fisiche interessate;
- allo stesso tempo, il titolare del trattamento dovrebbe agire in maniera tale da arginare la violazione e risolverla;

[23] Va osservato che anche i dati di registro che facilitano la verificabilità, ad esempio, della memorizzazione, delle modifiche o della cancellazione dei dati possono essere considerati dati personali relativi alla persona che ha avviato il trattamento corrispondente.

- la violazione dovrebbe essere documentata durante tutta la sua evoluzione.

Di conseguenza, dovrebbe essere chiaro che il titolare del trattamento è tenuto ad agire in relazione a qualsiasi allerta e stabilire se effettivamente si sia verificata una violazione. Tale breve periodo consente lo svolgimento di alcune indagini e dà al titolare del trattamento la possibilità di raccogliere prove e altre informazioni pertinenti. Tuttavia, dopo che il titolare del trattamento ha stabilito con ragionevole certezza che si è verificata una violazione, qualora siano soddisfatte le condizioni di cui all'articolo 33, paragrafo 1, è quindi necessario informare l'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore[24]. Se il titolare del trattamento non agisce in maniera tempestiva e risulta evidente che si è verificata una violazione, la sua inazione potrebbe essere considerata una mancata notifica ai sensi dell'articolo 33.

L'articolo 32 chiarisce che il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello adeguato di sicurezza dei dati personali: la capacità di individuare, trattare e segnalare tempestivamente una violazione deve essere considerata un aspetto essenziale di queste misure.

3. Contitolari del trattamento

L'articolo 26 riguarda i contitolari del trattamento e specifica che essi devono determinare le rispettive responsabilità in merito all'osservanza del regolamento[25]. Ciò includerà la determinazione di chi sarà responsabile di adempiere agli obblighi di cui agli articoli 33 e 34. Il Gruppo di lavoro raccomanda che gli accordi contrattuali tra i contitolari del trattamento includano disposizioni che stabiliscano quale titolare del trattamento assumerà il comando o sarà responsabile del rispetto degli obblighi di notifica delle violazioni previsti dal regolamento.

4. Obblighi del responsabile del trattamento

Sebbene il titolare del trattamento conservi la responsabilità generale per la protezione dei dati personali, il responsabile del trattamento svolge un ruolo importante nel consentire al titolare del trattamento di adempiere ai propri obblighi, segnatamente in materia di notifica delle violazioni. L'articolo 28, paragrafo 3, dispone che il trattamento da parte di un responsabile del trattamento è disciplinato da un contratto o da un altro atto giuridico, e precisa, alla lettera f), che il contratto o altro atto giuridico deve prevedere che il responsabile del trattamento "assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento".

L'articolo 33, paragrafo 2, chiarisce che se il titolare del trattamento ricorre a un responsabile del trattamento e quest'ultimo viene a conoscenza di una violazione dei dati personali che sta trattando per conto del titolare del trattamento, il responsabile del trattamento deve notificarla al titolare del trattamento "senza ingiustificato ritardo". Va notato che il responsabile del trattamento non deve valutare la probabilità di rischio derivante dalla violazione prima di notificarla al titolare del trattamento; spetta infatti a quest'ultimo effettuare la valutazione nel momento in cui viene a conoscenza della violazione. Il responsabile del trattamento deve soltanto stabilire se si è verificata una violazione e quindi notificarla al titolare del trattamento. Poiché quest'ultimo si serve del responsabile del trattamento per conseguire le proprie finalità, in linea di principio dovrebbe considerarsi "a conoscenza" della violazione non appena il responsabile del trattamento gliela

[24] Cfr. il regolamento (CEE, Euratom) n. 1182/71 che stabilisce le norme applicabili ai periodi di tempo, alle date e ai termini, disponibile all'indirizzo: http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:31971R1182&from=IT.

[25] Cfr. anche il considerando 79.

notifica. L'obbligo del responsabile del trattamento di effettuare la notifica al titolare del trattamento consente a quest'ultimo di far fronte alla violazione e di stabilire se deve notificarla all'autorità di controllo ai sensi dell'articolo 33, paragrafo 1, e alle persone fisiche interessate ai sensi dell'articolo 34, paragrafo 1. Il titolare del trattamento potrebbe anche indagare sulla violazione, in quanto il responsabile del trattamento potrebbe non conoscere tutti i fatti pertinenti connessi alla violazione, ad esempio potrebbe ignorare se il titolare del trattamento detiene comunque una copia o un backup dei dati personali distrutti o persi. Tale circostanza può influire sull'eventualità che il titolare del trattamento debba effettuare la notifica.

Il regolamento non fissa un termine esplicito entro il quale il responsabile del trattamento deve avvertire il titolare del trattamento, salvo specificare che deve farlo "senza ingiustificato ritardo". Di conseguenza, il Gruppo di lavoro raccomanda al responsabile del trattamento di effettuare la notifica al titolare del trattamento tempestivamente, fornendo successivamente le eventuali ulteriori informazioni sulla violazione di cui venga a conoscenza. Ciò è importante al fine di aiutare il titolare del trattamento a soddisfare l'obbligo di notifica all'autorità di controllo entro 72 ore.

Come precedentemente spiegato, il contratto tra il titolare del trattamento e il responsabile del trattamento dovrebbe specificare le modalità per il soddisfacimento delle prescrizioni di cui all'articolo 33, paragrafo 2, e delle altre disposizioni del regolamento, tra cui i requisiti per la notifica tempestiva da parte del responsabile del trattamento, che serve per aiutare il titolare del trattamento a rispettare l'obbligo di segnalare la violazione all'autorità di controllo entro 72 ore.

Qualora fornisca servizi a più titolari del trattamento tutti interessati dal medesimo incidente, il responsabile del trattamento dovrà segnalare i dettagli dell'incidente a ciascun titolare del trattamento.

Il responsabile del trattamento può effettuare la notifica per conto del titolare del trattamento qualora quest'ultimo gli abbia concesso l'opportuna autorizzazione e ciò faccia parte degli accordi contrattuali tra il titolare del trattamento e il responsabile del trattamento. La notifica deve essere effettuata conformemente agli articoli 33 e 34. Tuttavia, è importante osservare che la responsabilità legale della notifica rimane in capo al titolare del trattamento.

B. Fornire informazioni all'autorità di controllo

1. Informazioni da fornire

Quando il titolare del trattamento notifica una violazione all'autorità di controllo, l'articolo 33, paragrafo 3 stabilisce che la notifica deve almeno:

> "a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
>
> b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
>
> c) descrivere le probabili conseguenze della violazione dei dati personali;
>
> d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi".

Il regolamento non definisce le categorie di interessati né le registrazioni di dati personali. Tuttavia, il Gruppo di lavoro suggerisce che le categorie di interessati si riferiscono ai vari tipi di persone fisiche i cui dati personali sono stati oggetto di violazione: a seconda dei descrittori utilizzati, ciò potrebbe includere, tra gli altri, minori e altri gruppi vulnerabili, persone con disabilità, dipendenti o clienti.

Analogamente, le categorie di registrazioni dei dati personali fanno riferimento ai diversi tipi di registrazioni che il titolare del trattamento può trattare, quali dati sanitari, registri didattici, informazioni sull'assistenza sociale, dettagli finanziari, numeri di conti bancari, numeri di passaporto, ecc.

Il considerando 85 chiarisce che uno degli scopi della notifica consiste nel limitare i danni alle persone fisiche. Di conseguenza, se i tipi di interessati o di dati personali rivelano un rischio di danno particolare a seguito di una violazione (ad esempio usurpazione d'identità, frode, perdite finanziarie, minaccia al segreto professionale) è importante che la notifica indichi tali categorie. In questo modo, l'obbligo di descrivere le categorie si collega all'obbligo di descriverne le probabili conseguenze della violazione.

Il fatto che non siano disponibili informazioni precise (ad esempio il numero esatto di interessati coinvolti) non dovrebbe costituire un ostacolo alla notifica tempestiva delle violazioni. Il regolamento consente di effettuare approssimazioni sul numero di persone fisiche interessate e di registrazioni dei dati personali coinvolte. Ci si dovrebbe preoccupare di far fronte agli effetti negativi della violazione piuttosto che di fornire cifre esatte. Di conseguenza, quando è evidente che c'è stata una violazione ma non se ne conosce ancora la portata, un modo sicuro per soddisfare gli obblighi di notifica è procedere a una notifica per fasi (cfr. in appresso).

L'articolo 33, paragrafo 3, stabilisce che nella notifica il titolare del trattamento "deve almeno" fornire le informazioni previste; di conseguenza il titolare del trattamento può, se necessario, fornire ulteriori informazioni. I diversi tipi di violazioni (riservatezza, integrità o disponibilità) possono richiedere la fornitura di ulteriori informazioni per spiegare in maniera esaustiva le circostanze di ciascun caso.

Esempio

Nell'ambito della notifica all'autorità di controllo, il titolare del trattamento può ritenere utile indicare il nome del responsabile del trattamento, qualora quest'ultimo sia la causa di fondo della violazione, in particolare se quest'ultima ha provocato un incidente ai danni delle registrazioni dei dati personali di molti altri titolari del trattamento che fanno ricorso al medesimo responsabile del trattamento.

In ogni caso, l'autorità di controllo può richiedere ulteriori dettagli nel contesto dell'indagine su una violazione.

2. Notifica per fasi

A seconda della natura della violazione, il titolare del trattamento può avere la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente. L'articolo 33, paragrafo 4, afferma pertanto:

"Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo".

Ciò significa che il regolamento prende atto del fatto che il titolare del trattamento non sempre dispone di tutte le informazioni necessarie su una violazione entro 72 ore dal momento in cui ne è venuto a conoscenza, dato che non sempre sono disponibili entro tale termine dettagli completi ed esaustivi su un incidente. Pertanto, il regolamento consente una notifica per fasi. È più probabile che ciò si verifichi in caso di violazioni più complesse, quali alcuni tipi di incidenti di sicurezza informatica nel contesto dei quali, ad esempio, può essere necessaria un'indagine forense approfondita per stabilire appieno la natura della violazione e la portata della compromissione dei dati personali. Di conseguenza, in molti casi il titolare del trattamento dovrà effettuare ulteriori indagini e dare seguito alla notifica fornendo informazioni supplementari in un secondo momento. Ciò è

consentito a condizione che il titolare del trattamento indichi i motivi del ritardo, in conformità all'articolo 33, paragrafo 1. Il Gruppo di lavoro raccomanda che, all'atto della prima notifica all'autorità di controllo, il titolare del trattamento informi quest'ultima del fatto che non dispone ancora di tutte le informazioni richieste e che fornirà ulteriori dettagli in un momento successivo. L'autorità di controllo dovrebbe concordare le modalità e le tempistiche per la fornitura delle informazioni supplementari. Questo non impedisce al titolare del trattamento di trasmettere ulteriori informazioni in qualsiasi altro momento, qualora venga a conoscenza di ulteriori dettagli rilevanti sulla violazione che devono essere forniti all'autorità di controllo.

L'obiettivo dell'obbligo di notifica consiste nell'incoraggiare il titolare del trattamento ad agire prontamente in caso di violazione, a contenerla e, se possibile, a recuperare i dati personali compromessi e a chiedere un parere pertinente all'autorità di controllo. La notifica all'autorità di controllo entro le prime 72 ore può consentire al titolare del trattamento di assicurarsi che le decisioni in merito alla notifica o alla mancata notifica alle persone fisiche siano corrette.

Tuttavia, lo scopo della notifica all'autorità di controllo non è solo di ottenere orientamenti sull'opportunità di effettuare o meno la notifica alle persone fisiche interessate. In certi casi sarà evidente che, a causa della natura della violazione e della gravità del rischio, il titolare del trattamento dovrà effettuare la notifica alle persone fisiche coinvolte senza indugio. Ad esempio, se esiste una minaccia immediata di usurpazione d'identità oppure se categorie particolari di dati personali[26] vengono divulgate online, il titolare del trattamento deve agire senza ingiustificato ritardo per contenere la violazione e comunicarla alle persone fisiche coinvolte (cfr. sezione III). In circostanze eccezionali, ciò potrebbe persino aver luogo prima della notifica all'autorità di controllo. Più in generale, la notifica all'autorità di controllo non può fungere da giustificazione per la mancata comunicazione della violazione all'interessato laddove la comunicazione sia richiesta.

È opportuno inoltre precisare che se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il titolare del trattamento può informarne l'autorità di controllo. Tali informazioni possono quindi essere aggiunte alle informazioni già fornite all'autorità di controllo e l'incidente può essere quindi registrato come un evento che non costituisce una violazione. Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione.

Esempio

Un titolare del trattamento notifica all'autorità di controllo entro 72 ore l'individuazione di una violazione derivante dalla perdita di una chiave USB contenente una copia dei dati personali di alcuni dei suoi clienti. In seguito scopre che la chiave USB non era stata messa al suo posto e la recupera. Il titolare del trattamento aggiorna l'autorità di controllo e chiede la modifica della notifica.

Va osservato che un approccio per fasi alla notifica esiste già in forza degli obblighi di cui alla direttiva 2002/58/CE, del regolamento 611/2013 e nel quadro di altri incidenti segnalati di propria iniziativa.

3. Notifiche effettuate in ritardo

L'articolo 33, paragrafo 1, chiarisce che, qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo deve essere corredata dei motivi del ritardo. Questa disposizione, unitamente al concetto di notifica in fasi, riconosce che il titolare del trattamento potrebbe non essere sempre in grado di notificare una violazione entro tale termine e che una notifica tardiva può essere consentita.

[26] Cfr. articolo 9.

Tale scenario potrebbe aver luogo, ad esempio, qualora il titolare del trattamento subisca in poco tempo violazioni della riservatezza multiple e simili che coinvolgono allo stesso modo un gran numero di interessati. Il titolare del trattamento potrebbe prendere atto di una violazione e, nel momento in cui inizia l'indagine e prima della notifica, rilevare ulteriori violazioni analoghe, che hanno cause differenti. A seconda delle circostanze, il titolare del trattamento può impiegare del tempo per stabilire l'entità delle violazioni e, anziché notificare ciascuna violazione separatamente, effettuare una notifica significativa che rappresenta diverse violazioni molto simili tra loro, con possibili cause diverse. La notifica all'autorità di controllo potrebbe quindi aver luogo in ritardo, oltre le 72 ore dopo che il titolare del trattamento è venuto a conoscenza di tali violazioni.

A rigore di termini, ogni singola violazione costituisce un incidente segnalabile. Tuttavia, per evitare che il processo diventi eccessivamente oneroso, il titolare del trattamento può presentare una notifica "cumulativa" che rappresenta tutte le violazioni in questione, a condizione che riguardino il medesimo tipo di dati personali e che questi siano stati violati nel medesimo modo in un lasso di tempo relativamente breve. Se si verificano diverse violazioni riguardanti tipi diversi di dati personali, violati in maniere diverse, la notifica deve procedere secondo l'iter normale, segnalando ogni violazione conformemente all'articolo 33.

Sebbene il regolamento consenta di effettuare la notifica in ritardo, questa non dovrebbe essere vista come la regola. È opportuno sottolineare che le notifiche cumulative possono essere effettuate anche per più violazioni analoghe segnalate entro 72 ore.

C. Violazioni transfrontaliere e violazioni presso stabilimenti non UE

1. Violazioni transfrontaliere

In caso di trattamento transfrontaliero[27] dei dati personali, una violazione può riguardare interessati in più Stati membri. L'articolo 33, paragrafo 1, chiarisce che quando si è verificata una violazione, il titolare del trattamento deve effettuare una notifica all'autorità di controllo competente ai sensi dell'articolo 55 del regolamento[28]. L'articolo 55, paragrafo 1, afferma che:

> "Ogni autorità di controllo è competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del presente regolamento nel territorio del rispettivo Stato membro".

Tuttavia, l'articolo 56, paragrafo 1, stabilisce che:

> "Fatto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60".

Inoltre, l'articolo 56, paragrafo 6, afferma che:

> "L'autorità di controllo capofila è l'unico interlocutore del titolare del trattamento o del responsabile del trattamento in merito al trattamento transfrontaliero effettuato da tale titolare del trattamento o responsabile del trattamento".

[27] Cfr. articolo 4, paragrafo 23.

[28] Cfr. anche il considerando 122.

Ciò significa che ogniqualvolta si verifichi una violazione nel contesto di un trattamento transfrontaliero e si renda necessaria la notifica, il titolare del trattamento dovrà effettuare la notifica all'autorità di controllo capofila[29]. Pertanto, nel redigere il proprio piano di risposta alle violazioni, il titolare del trattamento deve valutare quale autorità di controllo sia l'autorità capofila a cui indirizzare le notifiche[30]. Il titolare del trattamento sarà così in grado di rispondere tempestivamente alle violazioni e di adempiere i propri obblighi di cui all'articolo 33. Dovrebbe essere chiaro che, in caso di violazione che comporta un trattamento transfrontaliero, la notifica deve essere effettuata all'autorità di controllo capofila, che non si trova necessariamente nel luogo in cui si trovano gli interessati coinvolti o dove si è verificata la violazione. Al momento della notifica all'autorità capofila, il titolare del trattamento dovrebbe indicare, se del caso, se la violazione coinvolge stabilimenti situati in altri Stati membri e gli Stati membri in cu potrebbero esserci interessati colpiti dalla violazione. Se nutre dei dubbi sull'identità dell'autorità di controllo capofila, il titolare del trattamento deve come minimo effettuare la notifica all'autorità di controllo locale del luogo in cui si è verificata la violazione.

2. Violazioni presso stabilimenti non UE

L'articolo 3 definisce l'ambito di applicazione territoriale del regolamento, che si applica anche al trattamento di dati personali effettuato da un titolare del trattamento o un responsabile del trattamento che non è stabilito nell'UE. In particolare, l'articolo 3, paragrafo 2, afferma che[31]:

> "Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
>
> a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
>
> b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione".

Anche l'articolo 3, paragrafo 3, è pertinente al riguardo e afferma che[32]:

> "Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico".

Se un titolare del trattamento non stabilito nell'UE è soggetto all'articolo 3, paragrafo 2, oppure all'articolo 3, paragrafo 3, e constata una violazione, è quindi comunque vincolato agli obblighi di notifica di cui agli articoli 33 e 34. L'articolo 27 impone al titolare del trattamento (e al responsabile del trattamento) di designare un rappresentante nell'Unione europea nel caso in cui si applichi l'articolo 3, paragrafo 2. In tali casi, il Gruppo di lavoro raccomanda di inviare la notifica all'autorità

---

[29] Cfr. linee guida del Gruppo di lavoro per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento, disponibile (in inglese) all'indirizzo http://ec.europa.eu/newsroom/document.cfm?doc_id=44102.

[30] Un elenco dei dati di contatto per tutte le autorità nazionali europee per la protezione dei dati è disponibile (in inglese) all'indirizzo: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

[31] Cfr. anche considerando 23 e 24.

[32] Cfr. anche il considerando 25.

di controllo dello Stato membro in cui è stabilito il rappresentante del titolare del trattamento nell'UE[33]. Analogamente, se un responsabile del trattamento è soggetto all'articolo 3, paragrafo 2, sarà tenuto a rispettare gli obblighi imposti ai responsabili del trattamento, in particolare l'obbligo di notificare una violazione al titolare del trattamento ai sensi dell'articolo 33, paragrafo 2.

D. Circostanze nelle quali non è richiesta la notifica

L'articolo 33, paragrafo 1, chiarisce che se è "improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche" tale violazione non è soggetta a notifica all'autorità di controllo. Un esempio potrebbe essere quello di dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica. Questa esenzione dalla notifica è in contrasto con gli attuali obblighi di notifica delle violazioni imposti ai fornitori di servizi di comunicazione elettronica accessibili al pubblico di cui alla direttiva 2009/136/CE, che stabilisce che tutte le violazioni rilevanti devono essere notificate all'autorità competente.

Nel parere 03/2014 sulla notifica delle violazioni[34], il Gruppo di lavoro ha spiegato che una violazione della riservatezza di dati personali crittografati con un algoritmo all'avanguardia costituisce in ogni caso una violazione dei dati personali e deve essere notificata. Se però la riservatezza della chiave rimane intatta (ossia se la chiave non è stata compromessa nell'ambito di una violazione della sicurezza ed è stata generata in maniera tale da non poter essere individuata con i mezzi tecnici disponibili da qualcuno che non è autorizzato ad accedervi), in linea di principio i dati risultano incomprensibili. Di conseguenza è improbabile che la violazione possa influire negativamente sulle persone fisiche e quindi non dovrebbe essere loro comunicata[35]. Tuttavia, anche se i dati sono crittografati, una perdita o alterazione può avere effetti negativi per gli interessati ove il responsabile del trattamento non disponga delle necessarie copie di riserva. In tal caso, la notifica agli interessati dovrebbe essere necessaria anche se sono state adottate misure di protezione mediante crittografia.

Il Gruppo di lavoro ha altresì spiegato che lo stesso ragionamento si applica anche nel caso in cui dati personali, quali password, siano stati codificati in modo sicuro con un hash e un salt, il valore hash sia stato calcolato con una funzione di hash con chiave crittografica all'avanguardia, la chiave utilizzata per l'hashing dei dati non sia stata compromessa nell'ambito di una violazione della sicurezza e sia stata generata in maniera tale da non poter essere individuata con i mezzi tecnologici a disposizione di qualcuno che non è autorizzato ad accedervi.

Di conseguenza, se i dati personali sono stati resi sostanzialmente incomprensibili ai soggetti non autorizzati e se esiste una copia o un backup, una violazione della riservatezza che coinvolga dati personali correttamente crittografati potrebbe non dover essere notificata all'autorità di controllo, poiché è improbabile che tale violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche. Di conseguenza potrebbe non essere necessario nemmeno informare la persona interessata, dato che è improbabile che vi siano rischi elevati. Tuttavia, si dovrebbe tenere presente che, sebbene inizialmente la notifica possa non essere richiesta se non esiste un rischio probabile per i diritti e le libertà delle persone fisiche, la situazione può cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato. Ad esempio, se la chiave risulta successivamente essere stata compromessa o essere stata esposta a una vulnerabilità nel software di cifratura, è possibile che sia ancora necessario procedere alla notifica.

---

[33] Cfr. considerando 80 e articolo 27.

[34] Gruppo di lavoro, Parere 03/2014 sulla notifica delle violazioni, (in inglese): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

[35] Cfr. anche articolo 4, paragrafi 1 e 2, del regolamento 611/2013.

Inoltre, va osservato che se si verifica una violazione in assenza di backup dei dati personali crittografati si è in presenza di una violazione della disponibilità che potrebbe presentare rischi per le persone fisiche e pertanto potrebbe richiedere la notifica. Analogamente, laddove si verifichi una violazione che implichi la perdita di dati crittografati, anche se esiste una copia di backup dei dati personali si potrebbe comunque trattare di una violazione soggetta a segnalazione, a seconda del periodo di tempo necessario per ripristinare i dati dal backup e dell'effetto che la mancanza di disponibilità ha sulle persone fisiche. Come afferma l'articolo 32, paragrafo 1, lettera c), un importante fattore di sicurezza è "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".

Esempio

Una violazione che non richiederebbe la notifica all'autorità di controllo sarebbe la perdita di un dispositivo mobile crittografato in maniera sicura, utilizzato dal titolare del trattamento e dal suo personale. Se la chiave di cifratura rimane in possesso del titolare del trattamento e non si tratta dell'unica copia dei dati personali, questi ultimi sarebbero inaccessibili a qualsiasi pirata informatico. Ciò significa che è improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati in questione. Se in seguito diventa evidente che la chiave di cifratura è stata compromessa o che il software o l'algoritmo di cifratura è vulnerabile, il rischio per i diritti e le libertà delle persone fisiche cambia e potrebbe quindi essere necessaria la notifica.

Tuttavia, si avrà mancato rispetto dell'articolo 33 se il titolare del trattamento non effettua la notifica all'autorità di controllo nel caso in cui i dati non siano stati effettivamente crittografati in maniera sicura. Di conseguenza, nel selezionare il software di cifratura, il titolare del trattamento deve valutare attentamente la qualità e la corretta attuazione della cifratura offerta, capire il livello di protezione effettivamente offerto e se quest'ultimo è appropriato in ragione dei rischi presentati. Il titolare del trattamento dovrebbe altresì avere familiarità con le specifiche modalità di funzionamento del prodotto di cifratura. Ad esempio, un dispositivo può essere crittografato una volta spento, ma non mentre è in modalità stand-by. Alcuni prodotti che utilizzano la cifratura dispongono di "chiavi predefinite" che devono essere modificate da ciascun cliente per essere efficaci. La cifratura potrebbe essere considerata adeguata dagli esperti di sicurezza al momento della sua messa in atto, ma diventare obsoleta nel giro di pochi anni, il che significa che può essere messo in discussione il fatto che i dati siano sufficientemente crittografati dal prodotto in questione e che quest'ultimo fornisca un livello appropriato di protezione.

III. Articolo 34 – Comunicazione all'interessato

A. Informare l'interessato

In alcuni casi, oltre a effettuare la notifica all'autorità di controllo, il titolare del trattamento è tenuto a comunicare la violazione alle persone fisiche interessate.

L'articolo 34, paragrafo 1, afferma che:

"Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo".

Il titolare del trattamento dovrebbe tenere a mente che la notifica all'autorità di controllo è obbligatoria a meno che sia improbabile che dalla violazione possano derivare rischi per i diritti e le libertà delle persone fisiche. Inoltre, laddove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche occorre informare anche queste ultime. La soglia per la comunicazione

delle violazioni alle persone fisiche è quindi più elevata rispetto a quella della notifica alle autorità di controllo, pertanto non tutte le violazioni dovranno essere comunicate agli interessati, il che li protegge da inutili disturbi arrecati dalla notifica.

Il regolamento afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "senza ingiustificato ritardo", il che significa il prima possibile. L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi[36]. Come osservato in precedenza, a seconda della natura della violazione e del rischio presentato, la comunicazione tempestiva aiuterà le persone a prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

L'allegato B delle presenti linee guida fornisce un elenco non esaustivo di esempi di casi in cui una violazione può presentare un rischio elevato per le persone fisiche e, di conseguenza, in cui il titolare del trattamento deve comunicarla agli interessati.

B. Informazioni da fornire

Ai fini della comunicazione alle persone fisiche, l'articolo 34, paragrafo 2, specifica che:

> "La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d)".

Secondo tale disposizione, il titolare del trattamento deve fornire almeno le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Come esempio di misure adottate per far fronte alla violazione e attenuarne i possibili effetti negativi, il titolare del trattamento può dichiarare che, dopo aver notificato la violazione all'autorità di controllo pertinente, ha ricevuto consigli sulla gestione della violazione e sull'attenuazione del suo impatto. Se del caso, il titolare del trattamento dovrebbe anche fornire consulenza specifica alle persone fisiche sul modo in cui proteggersi dalle possibili conseguenze negative della violazione, ad esempio reimpostando le password in caso di compromissione delle credenziali di accesso. Ancora una volta, il titolare del trattamento può scegliere di fornire informazioni supplementari rispetto a quanto richiesto qui.

C. Contattare l'interessato

In linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c).

[36] Cfr. anche il considerando 86.

Nel comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard. Ciò contribuisce a rendere la comunicazione della violazione chiara e trasparente.

Esempi di metodi trasparenti di comunicazione sono: la messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto), banner o notifiche su siti web di primo piano, comunicazioni postali e pubblicità di rilievo sulla stampa. Una semplice comunicazione all'interno di un comunicato stampa o di un blog aziendale non costituirebbe un mezzo efficace per comunicare una violazione all'interessato. Il Gruppo di lavoro raccomanda al titolare del trattamento di scegliere un mezzo che massimizzi la possibilità di comunicare correttamente le informazioni a tutte le persone interessate. A seconda delle circostanze, ciò potrebbe significare che il titolare del trattamento dovrebbe utilizzare diversi metodi di comunicazione, anziché un singolo canale di contatto.

Inoltre il titolare del trattamento potrebbe dover garantire che la comunicazione sia accessibile in formati alternativi appropriati e lingue pertinenti al fine di assicurarsi che le persone fisiche siano in grado di comprendere le informazioni fornite loro. Ad esempio, nel comunicare una violazione a una persona, sarà di norma appropriata la lingua utilizzata durante il precedente normale corso degli scambi commerciali con il destinatario. Tuttavia, se la violazione riguarda interessati con i quali il titolare del trattamento non ha precedentemente interagito o, in particolare, interessati che risiedono in un altro Stato membro o in un altro paese non UE diverso da quello nel quale è stabilito il titolare del trattamento, la comunicazione nella lingua nazionale locale potrebbe essere accettabile, tenendo conto della risorsa richiesta. L'obiettivo principale è aiutare gli interessati a comprendere la natura della violazione e le misure che possono adottare per proteggersi.

Il titolare del trattamento è nella posizione migliore per stabilire il canale di contatto più appropriato per comunicare una violazione agli interessati, soprattutto se interagisce frequentemente con i suoi clienti. Tuttavia, è chiaro che il titolare del trattamento dovrebbe essere cauto nell'usare un canale di contatto compromesso dalla violazione, in quanto tale canale potrebbe essere utilizzato anche da autori di attacchi che si fanno passare per il titolare del trattamento.

Il considerando 86 spiega che:

> "Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione".

Il titolare del trattamento potrebbe quindi contattare e consultare l'autorità di controllo non soltanto per chiedere consiglio sull'opportunità di informare gli interessati in merito a una violazione ai sensi dell'articolo 34, ma anche sui messaggi appropriati da inviare loro e sul modo più opportuno per contattarli.

Parallelamente, il considerando 88 indica che la notifica di una violazione dovrebbe tenere "conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali". Ciò può significare che in determinate circostanze, ove giustificato e su consiglio delle autorità incaricate dell'applicazione della legge, il titolare del trattamento può ritardare la comunicazione della violazione agli interessati fino a quando la comunicazione non pregiudica più tale indagine. Tuttavia, passato tale arco di tempo, gli interessati dovrebbero comunque essere tempestivamente informati.

Se non ha la possibilità di comunicare una violazione all'interessato perché non dispone di dati sufficienti per contattarlo, il titolare del trattamento dovrebbe informarlo non appena sia ragionevolmente possibile farlo (ad esempio quando l'interessato esercita il proprio diritto ai sensi dell'articolo 15 di accedere ai dati personali e fornisce al titolare del trattamento le informazioni supplementari necessarie per essere contattato).

D. Circostanze nelle quali non è richiesta la comunicazione

L'articolo 34, paragrafo 3, stabilisce tre condizioni che, se soddisfatte, non richiedono la comunicazione agli interessati in caso di violazione, ossia:

- il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi. Ciò potrebbe prevedere ad esempio la protezione dei dati personali con cifratura allo stato dell'arte oppure mediante tokenizzazione;
- immediatamente dopo una violazione, il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche. Ad esempio, a seconda delle circostanze del caso, il titolare del trattamento può aver immediatamente individuato e intrapreso un'azione contro il soggetto che ha avuto accesso ai dati personali prima che questi fosse in grado di utilizzarli in qualsiasi modo. È necessario altresì tenere in debito conto delle possibili conseguenze di qualsiasi violazione della riservatezza, anche in questo caso, a seconda della natura dei dati in questione;
- contattare gli interessati richiederebbe uno sforzo sproporzionato[37], ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti. Si pensi, ad esempio, al magazzino di un ufficio statistico che si è allagato e i documenti contenenti dati personali erano conservati soltanto in formato cartaceo. In tale circostanza il titolare del trattamento deve invece effettuare una comunicazione pubblica o prendere una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace. In caso di sforzo sproporzionato, si potrebbe altresì prevedere l'adozione di disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta, soluzione questa che potrebbe rivelarsi utile per le persone fisiche che potrebbero essere interessate da una violazione ma che il titolare del trattamento non può altrimenti contattare.

Conformemente al principio di responsabilizzazione, il titolare del trattamento dovrebbe essere in grado di dimostrare all'autorità di controllo di soddisfare una o più di queste condizioni[38]. Va tenuto presente che, sebbene la comunicazione possa inizialmente non essere richiesta se non vi è alcun rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato.

Se il titolare del trattamento decide di non comunicare una violazione all'interessato, l'articolo 34, paragrafo 4, spiega che l'autorità di controllo può richiedere che lo faccia, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato. In alternativa, può ritenere che siano state soddisfatte le condizioni di cui all'articolo 34, paragrafo 3, nel qual caso la comunicazione all'interessato non è richiesta. Qualora stabilisca che la decisione di non effettuare la comunicazione

[37] Cfr. linee guida del Gruppo di lavoro sulla trasparenza, che prendono in considerazione la questione dello sforzo sproporzionato, disponibile (in inglese) all'indirizzo http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850.

[38] Cfr. articolo 5, paragrafo 2.

all'interessato non sia fondata, l'autorità di controllo può prendere in considerazione l'esercizio dei poteri e delle sanzioni a sua disposizione.

IV. Valutazione dell'esistenza di un rischio o di un rischio elevato

A. Rischio come fattore che fa scattare l'obbligo di notifica

Sebbene il regolamento introduca l'obbligo di notificare una violazione, non è obbligatorio farlo in tutte le circostanze:

- la notifica all'autorità di controllo competente è obbligatoria a meno che sia improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche;
- la comunicazione di una violazione alle persone fisiche diventa necessaria soltanto laddove la violazione possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Ciò significa che non appena il titolare del trattamento viene a conoscenza di una violazione, è fondamentale che non si limiti a contenere l'incidente, ma valuti anche il rischio che potrebbe derivarne. Questo per due motivi: innanzitutto conoscere la probabilità e la potenziale gravità dell'impatto sulle persone fisiche aiuterà il titolare del trattamento ad adottare misure efficaci per contenere e risolvere la violazione; in secondo luogo, ciò lo aiuterà a stabilire se è necessaria la notifica all'autorità di controllo e, se necessario, alle persone fisiche interessate.

Come spiegato in precedenza, la notifica di una violazione è obbligatoria a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche, mentre la comunicazione di una violazione agli interessati deve essere effettuata se è probabile che la violazione presenti un rischio *elevato* per i diritti e le libertà delle persone fisiche. Tale rischio sussiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone fisiche i cui dati sono stati violati. Esempi di tali danni sono la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie e il pregiudizio alla reputazione. Il verificarsi di tale danno dovrebbe essere considerato probabile quando la violazione riguarda dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure che includono dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza[39].

B. Fattori da considerare nella valutazione del rischio

I considerando 75 e 76 del regolamento suggeriscono che, di norma, nella valutazione del rischio si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità del rischio per i diritti e le libertà degli interessati. Inoltre il regolamento afferma che il rischio dovrebbe essere valutato in base a una valutazione oggettiva.

Va osservato che la valutazione del rischio per i diritti e le libertà delle persone fisiche a seguito di una violazione esamina il rischio in maniera diversa rispetto alla valutazione d'impatto sulla protezione dei dati[40]. Quest'ultima considera tanto i rischi del trattamento dei dati svolto come pianificato, quanto quelli in caso di violazione. Nel considerare una potenziale violazione, esamina in termini generali la probabilità che la stessa si verifichi e il danno all'interessato che potrebbe

[39] Cfr. considerando 75 e 85.

[40] Cfr. le linee guida del Gruppo di lavoro in materia di valutazioni d'impatto sulla protezione dei dati qui: https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati.

derivarne; in altre parole, si tratta di una valutazione di un evento ipotetico. Nel caso di una violazione effettiva, l'evento si è già verificato, quindi l'attenzione si concentra esclusivamente sul rischio risultante dell'impatto di tale violazione sulle persone fisiche.

Esempio

Una valutazione d'impatto sulla protezione dei dati suggerisce che l'uso proposto di un determinato software di sicurezza per proteggere i dati personali costituisce una misura adeguata per garantire un livello di sicurezza adeguato al rischio che il trattamento presenterebbe altrimenti per le persone fisiche. Tuttavia, laddove una vulnerabilità diventi nota successivamente, ciò modifica l'idoneità del software a contenere il rischio per i dati personali protetti e richiede quindi una rivalutazione nel contesto di una valutazione d'impatto sulla protezione dei dati in corso.

Una vulnerabilità nel prodotto viene sfruttata in un secondo momento e si verifica una violazione. Il titolare del trattamento dovrebbe valutare le circostanze specifiche della violazione, i dati interessati e il potenziale livello di impatto sulle persone fisiche, nonché la probabilità che tale rischio si concretizzi.

Di conseguenza, nel valutare il rischio per le persone fisiche derivante da una violazione, il titolare del trattamento dovrebbe considerare le circostanze specifiche della violazione, inclusa la gravità dell'impatto potenziale e la probabilità che tale impatto si verifichi. Pertanto il Gruppo di lavoro raccomanda che la valutazione tenga conto dei seguenti criteri[41].

- Tipo di violazione

Il tipo di violazione verificatosi può influire sul livello di rischio presentato per le persone fisiche. Ad esempio, una violazione della riservatezza che ha portato alla divulgazione di informazioni mediche a soggetti non autorizzati può avere conseguenze diverse per una persona fisica rispetto a una violazione in cui i dettagli medici di una persona fisica sono stati persi e non sono più disponibili.

- Natura, carattere sensibile e volume dei dati personali

Ovviamente, un elemento fondamentale della valutazione del rischio sono il tipo e il carattere sensibile dei dati personali che sono stati compromessi dalla violazione. Solitamente più i dati sono sensibili, maggiore è il rischio di danni per le persone interessate; tuttavia si dovrebbero prendere in considerazione anche altri dati personali che potrebbero già essere disponibili sull'interessato. Ad esempio, è improbabile che la divulgazione del nome e dell'indirizzo di una persona fisica in circostanze ordinarie causi un danno sostanziale. Tuttavia, se il nome e l'indirizzo di un genitore adottivo sono divulgati a un genitore biologico, le conseguenze potrebbero essere molto gravi tanto per il genitore adottivo quanto per il bambino.

Violazioni relative a dati sulla salute, documenti di identità o dati finanziari come i dettagli di carte di credito, possono tutte causare danni di per sé, ma se tali dati fossero usati congiuntamente si potrebbe avere un'usurpazione d'identità. Di norma una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale.

[41] L'articolo 3, paragrafo 2, del regolamento 611/2013 fornisce orientamenti sui fattori che dovrebbero essere presi in considerazione in relazione alla notifica di violazioni nel settore dei servizi di comunicazione elettronica che possono essere utili nel contesto della notifica ai sensi del regolamento generale sulla protezione dei dati. Cfr. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:it:PDF.

Alcuni tipi di dati personali possono sembrare relativamente innocui, tuttavia occorre valutare attentamente ciò che questi dati possono rivelare sull'interessato. Un elenco di clienti che accettano consegne regolari potrebbe non essere particolarmente sensibile, tuttavia gli stessi dati relativi a clienti che hanno richiesto l'interruzione delle loro consegne durante le vacanze potrebbero essere informazioni utili per dei criminali.

Analogamente, una piccola quantità di dati personali altamente sensibili può avere un impatto notevole su una persona fisica, mentre una vasta gamma di dettagli può rivelare molte più informazioni in merito alla stessa persona. Inoltre, una violazione che interessa grandi quantità di dati personali relative a molte persone può avere ripercussioni su un numero corrispondentemente elevato di persone.

- Facilità di identificazione delle persone fisiche

Un fattore importante da considerare è la facilità con cui un soggetto che può accedere a dati personali compromessi riesce a identificare persone specifiche o ad abbinare i dati con altre informazioni per identificare persone fisiche. A seconda delle circostanze, l'identificazione potrebbe essere possibile direttamente dai dati personali oggetto di violazione senza che sia necessaria alcuna ricerca speciale per scoprire l'identità dell'interessato, oppure potrebbe essere estremamente difficile abbinare i dati personali a una particolare persona fisica, ma sarebbe comunque possibile a determinate condizioni. L'identificazione può essere direttamente o indirettamente possibile a partire dai dati oggetto di violazione, tuttavia può dipendere anche dal contesto specifico della violazione e dalla disponibilità pubblica dei corrispondenti dettagli personali. Quest'ultima eventualità potrebbe essere più rilevante per le violazioni della riservatezza e della disponibilità.

Come indicato in precedenza, i dati personali protetti da un livello appropriato di cifratura saranno incomprensibili a persone non autorizzate che non dispongono della chiave di decifratura. Inoltre, anche una pseudonimizzazione opportunamente attuata (definita all'articolo 4, punto 5, come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile") può ridurre la probabilità che le persone fisiche vengano identificate in caso di violazione. Tuttavia, le tecniche di pseudonimizzazione da sole non possono essere considerate sufficienti a rendere i dati incomprensibili.

- Gravità delle conseguenze per le persone fisiche

A seconda della natura dei dati personali coinvolti in una violazione, ad esempio categorie particolari di dati, il danno potenziale alle persone che potrebbe derivarne può essere particolarmente grave soprattutto se la violazione può comportare furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione. Se la violazione riguarda dati personali relativi a persone fisiche vulnerabili, queste ultime potrebbero essere esposte a un rischio maggiore di danni.

Il fatto che il titolare del trattamento sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale. Prendiamo una violazione della riservatezza nel cui ambito i dati personali vengono comunicati a un terzo di cui all'articolo 4, punto 10, o ad altri destinatari per errore. Una tale situazione può verificarsi, ad esempio, nel caso in cui i dati personali vengano inviati accidentalmente all'ufficio sbagliato di un'organizzazione o a un'organizzazione fornitrice utilizzata frequentemente. Il titolare del trattamento può chiedere al destinatario di restituire o distruggere in maniera sicura i dati ricevuti. In entrambi i casi, dato che il titolare del trattamento ha una relazione continuativa con tali soggetti e potrebbe essere a conoscenza delle loro procedure, della loro storia e di altri dettagli pertinenti, il destinatario può essere considerato "affidabile". In altre parole, il titolare del trattamento può ritenere che il destinatario goda di una certa affidabilità e può ragionevolmente aspettarsi che non

leggerà o accederà ai dati inviati per errore e che rispetterà le istruzioni di restituirli. Anche se i dati fossero stati consultati, il titolare del trattamento potrebbe comunque confidare nel fatto che il destinatario non intraprenderà ulteriori azioni in merito agli stessi e restituirà tempestivamente i dati al titolare del trattamento e coopererà per garantirne il recupero. In tali casi, questo aspetto può essere preso in considerazione nella valutazione del rischio effettuata dal titolare del trattamento in seguito alla violazione; il fatto che il destinatario sia affidabile può neutralizzare la gravità delle conseguenze della violazione, anche se questo non significa che non si sia verificata una violazione. La probabilità che detta violazione presenti un rischio per le persone fisiche verrebbe però meno, quindi non sarebbe più necessaria la notifica all'autorità di controllo o alle persone fisiche interessate. Ancora una volta, tutto dipenderà dalle circostanze del caso concreto. Ciò nonostante il titolare del trattamento deve comunque conservare informazioni relative alla violazione nel contesto del suo dovere generale di conservare registrazioni in merito alle violazioni (cfr. seguente sezione V).

Si dovrebbe altresì tener conto della permanenza delle conseguenze per le persone fisiche laddove l'impatto possa essere considerato maggiore qualora gli effetti siano a lungo termine.

- Caratteristiche particolari dell'interessato

Una violazione può riguardare dati personali relativi a minori o ad altre persone fisiche vulnerabili, che possono di conseguenza essere soggette a un rischio più elevato di danno. Altri fattori concernenti la persona fisica potrebbero influire sul livello di impatto della violazione sulla stessa.

- Caratteristiche particolari del titolare del trattamento di dati

La natura e il ruolo del titolare del trattamento e delle sue attività possono influire sul livello di rischio per le persone fisiche in seguito a una violazione. Ad esempio, un'organizzazione medica tratterà categorie particolari di dati personali, il che significa che vi è una minaccia maggiore per le persone fisiche nel caso in cui i loro dati personali vengano violati, rispetto a una mailing list di un quotidiano.

- Numero di persone fisiche interessate

Una violazione può riguardare solo una o poche persone fisiche oppure diverse migliaia di persone fisiche, se non molte di più. Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere. Tuttavia, una violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi. Ancora una volta, l'aspetto fondamentale consiste nel considerare la probabilità e la gravità dell'impatto sulle persone interessate.

- Aspetti generali

Pertanto, nel valutare il rischio che potrebbe derivare da una violazione, il titolare del trattamento dovrebbe considerare tanto la gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche e quanto la probabilità che tale impatto si verifichi. Chiaramente, se le conseguenze di una violazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze si verifichino è maggiore, maggiore è anche il rischio. In caso di dubbio, il titolare del trattamento dovrebbe restare molto prudente ed effettuare la notifica. L'allegato B fornisce alcuni esempi utili di diversi tipi di violazioni che comportano rischi o rischi elevati per le persone fisiche.

L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha elaborato raccomandazioni in merito a una metodologia di valutazione della gravità di una violazione, che

possono essere utili per i titolari del trattamento e i responsabili del trattamento nella progettazione del loro piano di risposta per la gestione delle violazioni[42].

V. Responsabilizzazione e tenuta di registri

A. Documentare le violazioni

Indipendentemente dal fatto che una violazione debba o meno essere notificata all'autorità di controllo, il titolare del trattamento deve conservare la documentazione di tutte le violazioni, come spiegato all'articolo 33, paragrafo 5:

> "Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo".

Tale obbligo è collegato al principio di responsabilizzazione, di cui all'articolo 5, paragrafo 2. Lo scopo della tenuta di registri delle violazioni non notificabili, oltre a quelle notificabili, è collegato anche agli obblighi del titolare del trattamento ai sensi dell'articolo 24, e l'autorità di controllo può richiedere di consultare tali registri. Di conseguenza il titolare del trattamento è incoraggiato a creare un registro interno delle violazioni, indipendentemente dal fatto che sia tenuto a effettuare la notifica o meno[43].

Sebbene spetti al titolare del trattamento determinare quale metodo e struttura utilizzare per documentare una violazione, determinate informazioni chiave dovrebbero essere sempre incluse. Come richiesto dall'articolo 33, paragrafo 5, il titolare del trattamento è tenuto a registrare i dettagli relativi alla violazione, comprese le cause, i fatti e i dati personali interessati. Dovrebbe altresì indicare gli effetti e le conseguenze della violazione e i provvedimenti adottati per porvi rimedio.

Il regolamento non specifica un periodo di conservazione della documentazione. Nel caso in cui i registri contengano dati personali, spetterà al titolare del trattamento stabilire il periodo appropriato di conservazione in conformità ai principi connessi al trattamento dei dati personali[44] e soddisfare una base legittima per il trattamento[45]. Dovrà conservare la documentazione in conformità dell'articolo 33, paragrafo 5, nella misura in cui può essere chiamato a fornire prove all'autorità di controllo in merito al rispetto di tale articolo oppure, più in generale, del principio di responsabilizzazione. Ovviamente se i registri non contengono dati personali, il principio di limitazione della conservazione[46] previsto dal regolamento non si applica.

---

[42] ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches* [Raccomandazioni in merito a una metodologia di valutazione della gravità delle violazioni dei dati personali], (disponibile in inglese) https://www.enisa.europa.eu/publications/dbn-severity.

[43] Il titolare del trattamento può scegliere di documentare le violazioni nel contesto del suo registro delle attività di trattamento che è mantenuto ai sensi dell'articolo 30. Non è richiesto un registro separato, a condizione che le informazioni rilevanti per la violazione siano chiaramente identificabili come tali e possano essere estratte su richiesta.

[44] Cfr. articolo 5.

[45] Cfr. articolo 6 e anche articolo 9.

[46] Cfr. articolo 5, paragrafo 1, lettera e).

Oltre a queste informazioni, il Gruppo di lavoro raccomanda al titolare del trattamento di documentare anche il ragionamento alla base delle decisioni prese in risposta a una violazione. In particolare, se una violazione non viene notificata, è opportuno documentare una giustificazione di tale decisione. La giustificazione dovrebbe includere i motivi per cui il titolare del trattamento ritiene improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche[47]. In alternativa, se ritiene che una delle condizioni di cui all'articolo 34, paragrafo 3, sia soddisfatta, il titolare del trattamento dovrebbe essere in grado di fornire prove adeguate della circostanza che ricorre nel caso di specie.

Se il titolare del trattamento notifica una violazione all'autorità di controllo, ma la notifica avviene in ritardo, il titolare del trattamento deve essere in grado di fornire i motivi del ritardo; la documentazione relativa a tale circostanza potrebbe contribuire a dimostrare che il ritardo nella segnalazione è giustificato e non eccessivo.

Laddove comunichi una violazione alle persone fisiche interessate, il titolare del trattamento dovrebbe essere trasparente in merito alla violazione e comunicare in maniera efficace e tempestiva. Di conseguenza, conservando le prove di tale comunicazione il titolare del trattamento faciliterebbe la dimostrazione della propria assunzione di responsabilità e del proprio rispetto delle norme.

Per agevolare il rispetto degli articoli 33 e 34, sarebbe vantaggioso tanto per il titolare del trattamento quanto per il responsabile del trattamento disporre di una procedura di notifica documentata, che stabilisca la procedura da seguire una volta individuata una violazione, ivi compreso come contenere, gestire e porre rimedio all'incidente, valutare il rischio e notificare la violazione. A questo proposito, per dimostrare il rispetto del regolamento potrebbe anche essere utile dimostrare che i dipendenti sono stati informati dell'esistenza di tali procedure e meccanismi e che sanno come reagire alle violazioni.

Si noti che la mancata corretta documentazione di una violazione può comportare l'esercizio da parte dell'autorità di controllo dei suoi poteri ai sensi dell'articolo 58 e l'imposizione di una sanzione amministrativa pecuniaria ai sensi dell'articolo 83.

B. Ruolo del responsabile della protezione dei dati

Il titolare del trattamento o il responsabile del trattamento può avere un responsabile della protezione dei dati[48], come richiesto dall'articolo 37 oppure su decisione volontaria come buona prassi. L'articolo 39 del regolamento stabilisce una serie di compiti obbligatori per il responsabile della protezione dei dati, ma non impedisce l'assegnazione di ulteriori compiti da parte del titolare del trattamento, se del caso.

Tra i compiti obbligatori del responsabile della protezione dei dati di particolare rilevanza per la notifica delle violazioni figurano quelli di fornire consulenza e informazioni al titolare del trattamento o al responsabile del trattamento, sorvegliare l'osservanza del regolamento e fornire un parere in merito alle valutazioni d'impatto sulla protezione dei dati. Il responsabile della protezione dei dati deve inoltre cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo e per gli interessati. Va inoltre osservato che, ai fini della notifica della violazione all'autorità di controllo, l'articolo 33, paragrafo 3, lettera b), impone al titolare del trattamento di fornire il nome e i dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto.

---

[47] Cfr. considerando 85.

[48] Cfr. le linee guida del Gruppo di lavoro sui responsabili della protezione dei dati qui: https://www.garanteprivacy.it/documents/10160/0/WP+243+-+Linee-guida+sui+responsabili+della+protezione+dei+dati+%28RPD%29.pdf.

Per quanto riguarda la documentazione delle violazioni, il titolare del trattamento o il responsabile del trattamento potrebbe chiedere il parere del proprio responsabile della protezione dei dati in merito alla struttura, all'impostazione e all'amministrazione della documentazione. Al responsabile della protezione dei dati potrebbe altresì essere affidato il compito di tenere i registri.

Questi compiti indicano che il responsabile della protezione dei dati dovrebbe svolgere un ruolo chiave nel fornire assistenza nella prevenzione delle violazioni o nella preparazione alle stesse, fornendo consulenza e monitorando il rispetto delle norme, nonché durante una violazione (ossia nel processo di notifica all'autorità di controllo) e durante qualsiasi successiva indagine da parte dell'autorità di controllo. In tale ottica, il Gruppo di lavoro raccomanda di informare tempestivamente il responsabile della protezione dei dati dell'esistenza di una violazione e di coinvolgerlo nella gestione delle violazioni e nel processo di notifica.

VI. Obblighi di notifica a norma di altri strumenti giuridici

Separatamente e in aggiunta alla notifica e alla comunicazione delle violazioni ai sensi del regolamento, il titolare del trattamento deve altresì essere a conoscenza di qualsiasi obbligo di notifica di incidenti di sicurezza previsto da altri atti legislativi associati cui potrebbe essere soggetto, e dell'eventuale obbligo parallelo di notificare all'autorità di controllo una violazione dei dati personali. Tali obblighi possono variare a seconda degli Stati membri. Esempi di obblighi di notifica sanciti in altri strumenti giuridici e di modalità con cui si correlano con il regolamento generale sulla protezione dei dati sono i seguenti:

- Regolamento (UE) n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS)[49].

L'articolo 19, paragrafo 2, del regolamento eIDAS impone ai prestatori di servizi fiduciari di notificare all'organismo di vigilanza una violazione della sicurezza o la perdita di integrità che hanno un impatto significativo sul servizio fiduciario fornito o sui dati personali conservati in tale contesto. Ove applicabile, ossia quando tale violazione o perdita costituiscono altresì una violazione dei dati personali ai sensi del regolamento generale sulla protezione dei dati, il prestatore di servizi fiduciari deve effettuare la notifica anche all'autorità di controllo.

- Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS)[50].

Gli articoli 14 e 16 della direttiva NIS impongono agli operatori di servizi essenziali e ai fornitori di servizi digitali di notificare gli incidenti di sicurezza alle loro autorità competenti. Come riconosciuto dal considerando 63 della direttiva NIS[51], gli incidenti di sicurezza possono spesso comportare una compromissione di dati personali. Sebbene la direttiva NIS imponga alle autorità competenti e alle autorità di controllo di cooperare e scambiare informazioni in tale contesto, rimane comunque il fatto che qualora tali incidenti siano o diventino violazioni di dati personali ai sensi del regolamento generale sulla protezione dei dati, tali operatori e/o fornitori sono tenuti a effettuare la notifica

[49] Cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ITA.

[50] Cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ITA.

51 Considerando 63: *"In molti casi gli incidenti compromettono dati personali. Al riguardo è opportuno che le autorità competenti e le autorità responsabili della protezione dei dati collaborino e si scambino informazioni su tutti gli aspetti pertinenti per affrontare le violazioni ai dati personali determinate dagli incidenti"*.

all'autorità di controllo in maniera distinta dagli obblighi di notifica degli incidenti a norma della direttiva NIS.

Esempio

Un fornitore di servizi cloud che notifica una violazione ai sensi della direttiva NIS può comunque essere tenuto a notificarla al titolare del trattamento se tale violazione include una violazione dei dati personali. Analogamente, un prestatore di servizi fiduciari che effettua una notifica a norma del regolamento eIDAS può anche essere tenuto a effettuare una notifica all'autorità competente per la protezione dei dati in caso di violazione.

- Direttiva 2009/136/CE (direttiva sui diritti dei cittadini) e regolamento (UE) n. 611/2013 (regolamento sulla notifica delle violazioni).

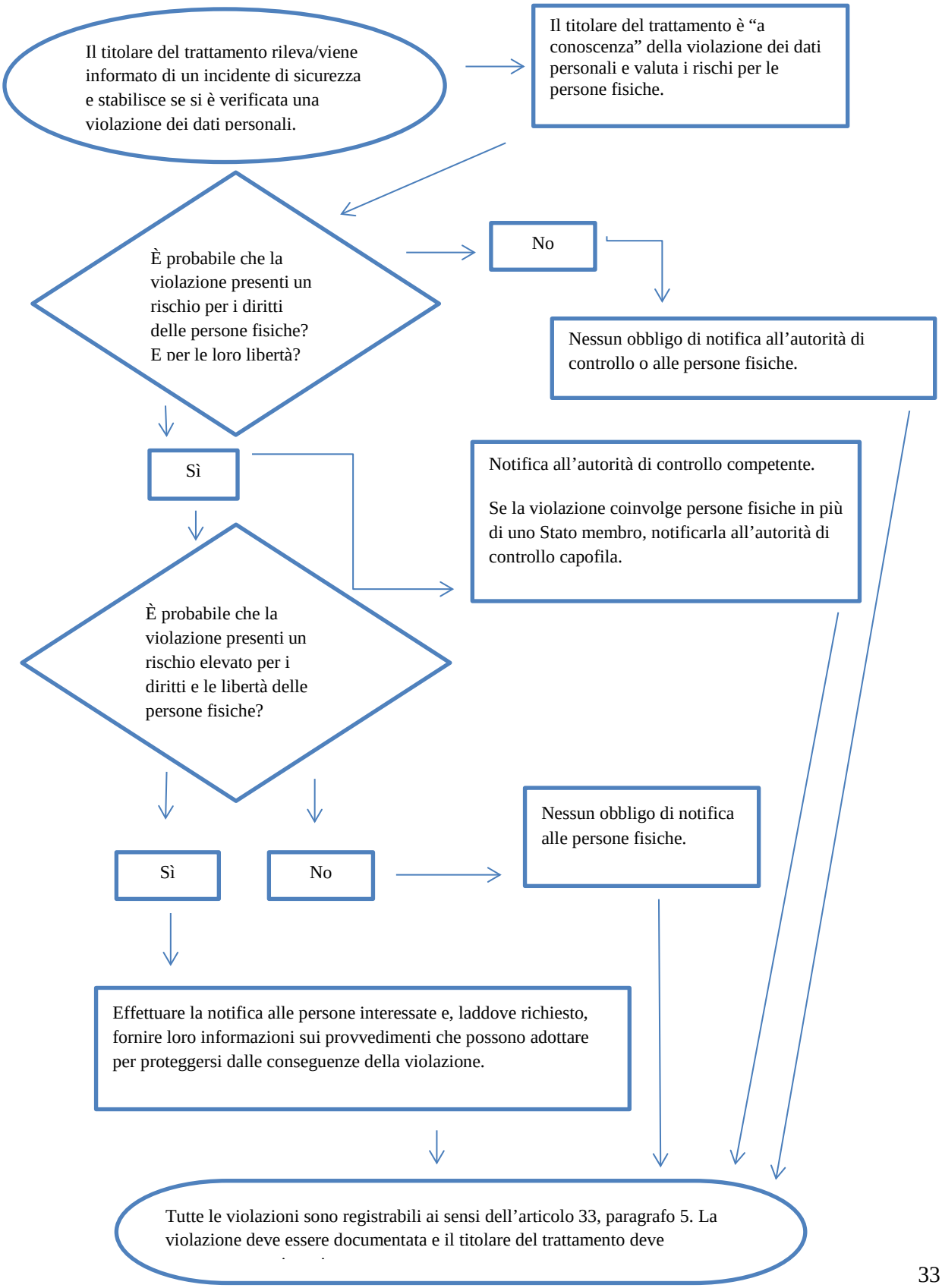
I fornitori di servizi di comunicazione elettronica accessibili al pubblico nel contesto della direttiva 2002/58/CE[52] devono notificare le violazioni alle autorità nazionali competenti.

Il titolare del trattamento dovrebbe altresì essere a conoscenza di eventuali ulteriori obblighi di notifica in ambito giuridico, medico o professionale previsti da altri regimi applicabili.

[52] Il 10 gennaio 2017, la Commissione europea ha proposto un direttiva relativa alla vita privata e alle comunicazioni elettroniche che sostituirà la direttiva 2009/136/CE e sopprimerà gli obblighi di notifica. Tuttavia, fino a quando tale proposta non sarà approvata dal Parlamento europeo, l'attuale obbligo di notifica rimane in vigore, cfr. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

VII. **Allegato**

A. Diagramma di flusso che illustra gli obblighi di notifica



B. Esempi di violazioni dei dati personali e dei soggetti a cui notificarle

I seguenti esempi non esaustivi aiuteranno il titolare del trattamento a stabilire se deve effettuare la notifica in diversi scenari di violazione dei dati personali. Questi esempi possono altresì contribuire a distinguere tra rischio e rischio elevato per i diritti e le libertà delle persone fisiche.

Esempio	**Notifica all'autorità di controllo?**	**Comunicazione all'interessato?**	**Note/raccomandazioni**
Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
ii. Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati. Il titolare del trattamento ha clienti in un solo Stato membro.	Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata.	
iii. Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del trattamento e accedere alle proprie registrazioni.	No.	No.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. Il titolare del trattamento deve conservare adeguate registrazioni in merito.
iv. Un titolare del trattamento subisce un	Sì, effettuare la segnalazione	Sì, effettuare la segnalazione alle	Se fosse stato disponibile un backup e i dati

attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa evidente che l'unica funzionalità dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.	all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente con altri mezzi, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'articolo 32.
v. Una persona telefona al call center di una banca per segnalare una violazione dei dati. La persona ha ricevuto l'estratto conto mensile da un soggetto diverso. Il titolare del trattamento intraprende una breve indagine (ossia la conclude entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e che vi è una potenziale carenza sistemica che potrebbe comportare il coinvolgimento già occorso o potenziale di altre persone fisiche.	Sì.	La comunicazione va effettuata soltanto alle persone fisiche coinvolte in caso di rischio elevato e se è evidente che altre persone fisiche non sono state interessate dall'evento.	Se dopo ulteriori indagini si stabilisce che l'evento ha interessato un numero maggiore di persone fisiche è necessario comunicare questo sviluppo all'autorità di controllo, e il titolare del trattamento deve informarne le altre persone fisiche interessate se sussiste un rischio elevato per loro.

vi. Un titolare del trattamento gestisce un mercato online e ha clienti in più Stati membri. Tale mercato subisce un attacco informatico a seguito del quale i nomi utente, le password e la cronologia degli acquisti vengono pubblicati online dall'autore dell'attacco.	Sì, segnalare l'evento all'autorità di controllo capofila se la violazione riguarda un trattamento transfrontaliero.	Sì, dato che la violazione potrebbe comportare un rischio elevato.	Il titolare del trattamento dovrebbe prendere delle misure, ad esempio forzare il ripristino delle password degli account interessati, e altri provvedimenti per attenuare il rischio. Il titolare del trattamento dovrebbe altresì considerare qualsiasi altro obbligo di notifica, ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali.
vii. Una società di *hosting* di siti web che funge da responsabile del trattamento individua un errore nel codice che controlla l'autorizzazione dell'utente. A causa di tale vizio, qualsiasi utente può accedere ai dettagli dell'account di qualsiasi altro utente.	In veste di responsabile del trattamento, la società di *hosting* di siti web deve effettuare la notifica ai clienti interessati (i titolari del trattamento) senza ingiustificato ritardo. Supponendo che la società di *hosting* di siti web abbia condotto le proprie indagini, i titolari del trattamento interessati dovrebbero essere ragionevolmente certi di aver subito una violazione e pertanto è probabile che vengano considerati "a conoscenza" della violazione nel momento in cui hanno ricevuto la notifica da parte della società di *hosting* (il responsabile del trattamento). Il titolare del trattamento deve quindi effettuare la notifica all'autorità di controllo.	Qualora non vi siano probabili rischi elevati per le persone fisiche non è necessario effettuare una comunicazione a tali persone.	La società di *hosting* di siti web (responsabile del trattamento) deve prendere in considerazione qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali). Qualora non vi sia alcuna prova che tale vulnerabilità sia sfruttata presso uno dei suoi titolari del trattamento, la violazione potrebbe non essere soggetta all'obbligo di notifica, tuttavia potrebbe essere una violazione da registrare o essere il segno di un mancato rispetto dell'articolo 32.

viii. Le cartelle cliniche di un ospedale sono indisponibili per un periodo di 30 ore a causa di un attacco informatico.	Sì, l'ospedale è tenuto a effettuare la notifica in quanto può verificarsi un rischio elevato per la salute e la tutela della vita privata dei pazienti.	Sì, informare le persone fisiche coinvolte.	
ix. I dati personali di un gran numero di studenti vengono inviati per errore a una mailing list sbagliata con più di 1 000 destinatari.	Sì, segnalare l'evento all'autorità di controllo.	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	
x. Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se è interessato un numero elevato di persone, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, il messaggio di posta elettronica contiene le password iniziali).	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.