693/14/IT
WP 213

Parere 03/2014 sulla notifica delle violazioni dei dati personali

adottato il 25 marzo 2014

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 cittadinanza dell'Unione) della Commissione europea, direzione generale Giustizia, B -1049 Bruxelles, Belgio, ufficio MO-59 02/13.

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

[NdT] Ai fini del presente parere, con "responsabile del trattamento" e con "incaricato del trattamento" si intendono rispettivamente il "titolare" e il "responsabile" di cui all'articolo 4, lettera f) e lettera g) del decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali).

Sintesi

Nel presente parere il Gruppo di lavoro articolo 29 fornisce orientamenti ai responsabili del trattamento per aiutarli a stabilire se occorra informare gli interessati nell'eventualità di una "violazione dei dati personali". Pur tenendo conto del vigente obbligo dei fornitori di servizi di comunicazione elettronica ai sensi della direttiva 2002/58/CE, il parere offre esempi tratti da molteplici settori, nel contesto della proposta di regolamento sulla protezione dei dati, e illustra buone pratiche per tutti i responsabili del trattamento.

Mentre la notifica all'autorità competente deve avvenire, secondo il disposto della direttiva 2002/58/CE, per tutte le violazioni dei dati, il presente parere esamina le violazioni dei dati personali per le quali è richiesta la notifica agli interessati ed espone ciò che i responsabili del trattamento avrebbero potuto fare nella messa in opera dei loro sistemi per prevenire a monte la violazione dei dati personali o, quanto meno, quali misure si sarebbero potute attuare in primo luogo per esentare il responsabile del trattamento dall'obbligo di notifica agli interessati.

Inoltre, il parere fornisce risposte ad alcune delle principali questioni relative alle violazioni dei dati personali e all'applicazione della direttiva 2002/58/CE.

1. Introduzione

La "violazione dei dati personali" è definita dall'articolo 2, lettera i), della direttiva 2002/58/CE come una "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico nella Comunità".

La direttiva 2002/58/CE (così come la proposta di regolamento europeo sulla protezione dei dati) stabilisce che le violazioni dei dati personali devono essere notificate alle autorità nazionali competenti. Le informazioni che devono essere fornite in tale notifica sono indicate in modo particolareggiato nell'allegato I del regolamento (UE) n. 611/2013.

Quando la violazione dei dati personali rischia di pregiudicare i dati personali o la vita privata della persona interessata[1], il responsabile del trattamento deve comunicare senza indebito ritardo l'avvenuta violazione anche a tale persona[2].

La direttiva 2002/58/CE, al pari del regolamento (UE) n. 611/2013, prevede un'esenzione dall'obbligo di notifica alle persone interessate nel caso in cui i dati siano stati resi incomprensibili. Se il fornitore ha dimostrato in modo convincente all'autorità competente di aver utilizzato le opportune misure tecnologiche di protezione per rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi[3] e che tali misure erano state applicate ai dati interessati dalla violazione della sicurezza, non è richiesta la notifica di una violazione dei dati personali alla persona interessata[4].

Il motivo alla base di tale esenzione dall'obbligo di notifica agli interessati è che misure adeguate possono ridurre a livelli trascurabili i rischi residui per la vita privata. 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 comunicata all'autorità. Se però la riservatezza della chiave rimane intatta, in linea di principio i dati risultano incomprensibili a chiunque non sia autorizzato ad accedervi, così che la violazione non rischia di ledere la persona interessata e, pertanto, non deve esserle comunicata.

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.

---

[1] Nel presente parere utilizziamo l'espressione "persona interessata" (o "interessato") quale definita dalla direttiva 95/46/CE. Nel contesto della direttiva 2002/58/CE, tale espressione corrisponde a "abbonato o altra persona".

[2] Ai sensi della direttiva 2002/58/CE e del regolamento (UE) n. 611/2013, la notifica all'autorità deve essere effettuata entro un termine di 24 ore a partire dal rilevamento della violazione, ove possibile, prorogabile in alcuni casi a 72 ore. La notifica all'abbonato o altra persona deve essere effettuata senza indebito ritardo (nel senso dell'articolo 2, paragrafo 2, del regolamento (UE) n. 611/2013) dopo la scoperta della violazione di dati personali. La notifica alla persona interessata è indipendente dalla notifica all'autorità nazionale competente.

[3] Articolo 4, paragrafo 3, della direttiva 2002/58/CE; articolo 4, paragrafo 1, del regolamento (UE) n. 611/2013; articolo 32, paragrafo 3, del regolamento generale sulla protezione dei dati, nel testo consolidato non ufficiale votato della commissione LIBE e messo a disposizione dal relatore.

[4] Va rilevato che, qualora la chiave venga successivamente compromessa, devono essere notificate tutte le precedenti violazioni che non sono state comunicate in virtù della segretezza della chiave.

Pertanto, è importante che i responsabili del trattamento siano proattivi e procedano a un'adeguata pianificazione. L'articolo 17 della direttiva 95/46/CE e l'articolo 4, paragrafi 1 e 1 *bis*, della direttiva 2002/58/CE prevedono che i responsabili del trattamento debbano attuare misure tecniche ed organizzative appropriate per "garantire […] un livello di sicurezza appropriato rispetto ai rischi" presentati dal trattamento. A tale scopo occorre predisporre un idoneo quadro di gestione dei rischi, che definisca gli elementi minimi che un tale approccio dovrebbe comprendere e che contempli una serie di opportuni controlli tecnici ed organizzativi minimi, che possono essere stabiliti dal responsabile del trattamento, con particolare attenzione ai controlli per rendere incomprensibili i dati, ove necessario. Le imprese dovrebbero inoltre istituire preventivamente piani appropriati per il trattamento delle violazioni dei dati personali, idonei a garantire che esse reagiscano a siffatte violazioni in modo rapido ed efficace.

Quando l'articolo 17 è attuato correttamente, vale a dire prima di dare inizio al trattamento dei dati, i rischi connessi a una violazione dei dati personali sono stati valutati e ridotti in via preventiva. In tal caso, le violazioni dei dati personali dovrebbero verificarsi più raramente e avere minori ripercussioni sulle persone interessate. Poiché la notifica agli interessati non è richiesta quando la violazione non pregiudica i dati personali o la vita privata di tali persone o quando sono state applicate opportune misure tecnologiche di protezione ai dati interessati dalla violazione, il modo migliore per evitare di dover informare le persone interessate consiste nell'integrare appropriati meccanismi di tutela della vita privata nei progetti implicanti il trattamento di dati personali.

La notifica alle persone interessate deve essere effettuata senza indebito ritardo[5] ed è indipendente dalla notifica della violazione dei dati personali all'autorità nazionale competente. Il responsabile del trattamento dovrebbe tenere presente che, pur non costituendo un criterio per stabilire se occorra o meno informare le persone interessate, uno dei principali vantaggi della notifica consiste nel fornire a tali persone le informazioni necessarie per ridurre gli effetti negativi derivanti dalle circostanze della violazione. Qualora il responsabile del trattamento non sappia se possano verificarsi effetti negativi sui dati personali o sulla vita privata degli interessati, dovrebbe procedere alla notifica in via precauzionale. Occorre inoltre tenere conto della possibilità che le autorità competenti richiedano la comunicazione agli interessati in seguito a una successiva valutazione della notifica.

Il presente parere contiene un **elenco non esaustivo di casi in cui occorre procedere alla notifica alle persone interessate [6]**. Ogni violazione dei dati personali viene esaminata alla luce dei tre criteri classici in materia di sicurezza: l'espressione "violazione della disponibilità" si riferisce alla distruzione accidentale o illecita o alla perdita di dati personali, "violazione dell'integrità" all'alterazione di dati personali e "violazione della riservatezza" alla divulgazione o all'accesso non autorizzati a dati personali. Il parere fornisce poi **orientamenti generali** sui casi che non richiedono la notifica. Infine, **tratta i principali problemi** che i responsabili del trattamento possono incontrare al momento di stabilire se occorra o meno informare gli interessati.

[5] Ai sensi della direttiva 2002/58/CE e del regolamento (UE) n. 611/2013, la notifica all'autorità deve essere effettuata entro un termine di 24 ore a partire dal rilevamento della violazione di dati personali, ove possibile, prorogabile in alcuni casi a 72 ore. La notifica all'abbonato o altra persona deve essere effettuata senza indebito ritardo dopo la scoperta della violazione di dati personali.

[6] Dal momento che la proposta di regolamento sulla protezione dei dati prevede l'estensione generalizzata dell'obbligo di notifica a tutti i settori, e poiché alcuni Stati membri hanno già stabilito un obbligo legale di notifica, gli esempi forniti nel presente parere non riguardano soltanto il settore delle comunicazioni elettroniche.

2. Violazioni che rischiano di recare pregiudizio agli interessati

Le violazioni devono essere notificate senza indebito ritardo alle persone interessate qualora rischino di pregiudicarne i dati personali o la vita privata. Questa sezione contiene alcuni esempi di violazioni che rispondono a tali criteri. Fornisce inoltre esempi di misure tecniche che, se fossero state adottate prima dell'incidente, avrebbero potuto evitare la notifica agli interessati.

Caso 1. *In un istituto di cura per l'infanzia sono stati rubati quattro computer portatili contenenti dati sensibili sullo stato di salute e sulla protezione sociale e altri dati personali di 2 050 minori.*

Tale violazione dei dati personali riguarda sia la riservatezza sia (nel caso in cui il responsabile del trattamento non abbia predisposto una copia di riserva) la disponibilità e l'integrità dei dati.

Possibili conseguenze ed effetti negativi della violazione della riservatezza:

- Il primo impatto è una violazione del segreto medico: la base dati contiene informazioni mediche riservate sui minori alle quali potrebbero accedere soggetti non autorizzati.
- La pubblicazione di tali dati potrebbe avere un impatto sull'ambiente scolastico e/o familiare dei minori (ad esempio informazioni su abusi, patologie di lunga durata, problemi psichici, difficoltà sociali o economiche della famiglia, ecc.).
- La violazione potrebbe avere ripercussioni emotive sui minori e sui loro genitori.
- I dati potrebbero essere utilizzati per ricattare i genitori e i minori stessi (a seconda della loro età).
- I genitori di minori gravemente malati potrebbero essere presi di mira da soggetti intenzionati a sfruttarne la posizione di debolezza (ad es. ciarlatani, sette, ecc.).

Possibili conseguenze ed effetti negativi della violazione della disponibilità:

- Potrebbe interferire con la continuità delle terapie somministrate ai minori determinando l'aggravarsi delle patologie o ricadute.
- Potrebbe provocare intossicazioni accidentali dovute ad allergie ai farmaci o a farmaci confliggenti, con conseguenti problemi di salute o decessi.
- Potrebbe comportare indebiti ritardi nei rimborsi o nell'erogazione di prestazioni di assistenza finanziaria alle persone interessate, con conseguenti ripercussioni economiche sulle famiglie coinvolte.

Possibili conseguenze ed effetti negativi della violazione dell'integrità:

- La perdita dei dati potrebbe compromettere l'integrità delle cartelle cliniche e provocare l'interruzione delle terapie somministrate ai minori. Ad esempio,

qualora fossero disponibili solo vecchie copie di riserva di tali cartelle, tutte le modifiche inserite sui computer rubati andrebbero perdute, con conseguente pregiudizio all'integrità dei dati. L'utilizzo di cartelle cliniche non aggiornate potrebbe pregiudicare la continuità terapeutica determinando l'aggravarsi delle patologie o ricadute.

A seconda dei possibili effetti, in questo caso si dovrebbe procedere alla notifica, ma è importante anche tenere conto dell'età e del grado di maturità degli interessati. Nella fattispecie potrebbe essere più appropriato informare, oltre che il minore stesso, un genitore o tutore legale che si occupi già attivamente della sua assistenza medica, ove ciò risulti opportuno o sia prescritto dalla legge applicabile.

In tal modo, i genitori destinatari della notifica potranno segnalare anomalie nella continuità terapeutica, verificare le allergie note all'istituto di cura o chiedere nuovi esami medici per assicurarsi che i figli ricevano le cure adatte. Potrebbero anche scegliere di informare direttamente altre persone in merito alle condizioni di salute dei minori al fine di arginare alcuni degli impatti sul loro ambiente.

Esempi di misure di salvaguardia appropriate che avrebbero potuto ridurre i rischi, se attuate preventivamente:

- Predisponendo una copia di riserva sufficientemente aggiornata si sarebbe potuta evitare la violazione della disponibilità e dell'integrità, o mitigarne le conseguenze e gli effetti negativi.
- Proteggendo i dati con un idoneo prodotto di crittografia dotato di una chiave sufficientemente forte e segreta sarebbe stato possibile attenuare eventuali conseguenze ed effetti negativi della violazione della riservatezza.

Se tali misure di salvaguardia sono state attuate e sono rimaste sicure (ossia la chiave è rimasta segreta e la copia di riserva è ancora disponibile), in linea di principio la notifica agli interessati potrebbe non essere necessaria. Tale circostanza andrebbe dimostrata in modo persuasivo all'autorità competente.

Caso 2. *I dati personali relativi ai clienti di un mediatore di assicurazione del ramo vita sono stati oggetto di un accesso indebito effettuato sfruttando le vulnerabilità di un'applicazione web. Gli interessati sono stati identificati attraverso nome e indirizzo e i dati comprendevano questionari medici compilati. La violazione ha riguardato 700 persone interessate.*

Possibili conseguenze ed effetti negativi della violazione della riservatezza:

- La pubblicazione dei dati su Internet da parte dell'autore dell'attacco potrebbe pregiudicare le possibilità degli interessati di trovare lavoro (ad es. risposte relative a problemi di salute, gravidanza, ecc.).
- Potrebbe avere un impatto sull'ambiente di lavoro e/o familiare degli interessati.
- Potrebbe avere anche un impatto emotivo sugli interessati che tengano celata la loro patologia.
- Potrebbe condurre a usurpazioni di identità.

- I dati (ad esempio il fatto di essere cliente o di acquistare determinati servizi) potrebbero essere utilizzati a scopo di "phishing".

Dal momento che tale violazione rischia di ledere gli interessati, deve essere loro notificata.

Esempi di misure di salvaguardia appropriate che avrebbero potuto ridurre i rischi, se attuate preventivamente:

- Un monitoraggio costante dei possibili punti deboli delle tecnologie utilizzate che comprendesse, tra l'altro, un controllo periodico della vulnerabilità del sito web e l'aggiornamento del software (compreso il software di sicurezza) avrebbe potuto prevenire la violazione o limitarne l'impatto.

  Sebbene non sia facile evitare le vulnerabilità di sicurezza "zero-day", politiche adeguate ed efficaci volte a prevenire in modo proattivo lo sfruttamento di tali vulnerabilità, anche mediante la revisione dei codici, possono ridurre il margine di rischio a livelli accettabili. Inoltre, una buona politica di gestione degli incidenti di sicurezza potrebbe mitigare le conseguenze della violazione limitando la durata e la portata dei suoi effetti negativi.

- Come nel caso precedente, le possibili conseguenze e i possibili effetti negativi della violazione della riservatezza avrebbero potuto essere attenuati proteggendo i dati dei clienti con un idoneo prodotto per la crittografia dotato di una chiave sufficientemente forte e segreta. Tale misura potrebbe garantire una tutela particolarmente efficace contro il furto del disco o circostanze analoghe.

- Infine, la compagnia di assicurazioni avrebbe potuto utilizzare varie tecnologie per il rafforzamento della tutela della vita privata al fine di ridurre al minimo i dati e/o l'identificabilità delle persone interessate. Ad esempio, avrebbe potuto inviare per posta ai clienti un numero di identificazione casuale ai fini della compilazione del questionario medico online. In tal modo si sarebbe evitato di inserire in detto questionario domande relative a nome, indirizzo, data di nascita o numero di telefono.

Caso 3. *Un dipendente di un fornitore di servizi Internet ha rivelato ad un terzo il login e la password di un account con privilegi di accesso completo alla base dati dei clienti. Utilizzando tale account, il terzo può accedere a tutte le informazioni relative ai clienti, senza alcuna restrizione. La base dati contiene nomi, indirizzi, indirizzi di posta elettronica, numeri di telefono, dati di accesso e altri dati di identificazione (nome utente, hash delle password, ID dei clienti) nonché dati di pagamento (numero di conto corrente, dati della carta di credito, ecc.). Sebbene questi ultimi siano stati cifrati con un algoritmo all'avanguardia, l'account master compromesso è stato autorizzato ad accedervi, così che anche il terzo ha avuto accesso a tali dati. La società ha oltre 100 000 clienti.*

Possibili conseguenze ed effetti negativi della violazione della riservatezza:

- L'utilizzo abusivo dei dati di pagamento (in particolare dei dati delle carte di credito) avrebbe un impatto finanziario sui clienti.

- Poiché le password sono state codificate con un semplice hash, il terzo potrebbe facilmente ricavarne il corrispondente testo in chiaro. Sarebbe possibile accedere all'account di qualsiasi cliente anche dopo la chiusura dell'account violato.

- Il terzo potrebbe facilmente utilizzare la posta elettronica e le password degli interessati per accedere ad account di altri servizi online, dal momento che molte persone utilizzano la medesima password per una pluralità di servizi online diversi.

Possibili conseguenze ed effetti negativi della violazione dell'integrità:

- Il terzo ha avuto pieno accesso alla base dati e potrebbe avere modificato, cancellato o aggiunto alcuni dati degli account.
    - Se il servizio ISP comprendeva posta elettronica o web hosting, il terzo potrebbe avere acceduto, modificato o cancellato tale contenuto, modificato le impostazioni DNS o chiuso l'account dell'interessato.

Sebbene i dati finanziari fossero cifrati, il terzo ha avuto accesso ai dati decifrati attraverso l'interfaccia utente e pertanto non si applica l'esenzione dall'obbligo di notifica.

Se i file di log protetti sono affidabili (ossia non compromessi) e indicano che l'account non ha acceduto all'anagrafica clienti, la notifica agli interessati non dovrebbe essere obbligatoria.

In caso contrario, dal momento che potrebbero verificarsi effetti negativi sugli interessati e l'esenzione non è applicabile, la violazione andrebbe notificata ai clienti coinvolti.

Se le password sono state compromesse, il responsabile del trattamento dovrebbe provvedere affinché gli interessati siano obbligati a creare nuove password, accertandosi che tutte le nuove password vengano immesse da utenti autorizzati e non da terzi che abbiano ottenuto le credenziali di accesso. All'atto pratico, ciò potrebbe corrispondere alla procedura sicura per il rinnovo delle password perdute e andrebbero esplicitati i motivi per i quali le password vengono rinnovate. La notifica agli utenti dovrebbe contenere anche la raccomandazione di non usare più la password precedente né una simile e di modificare le password compromesse in tutti gli account per i quali sono state utilizzate.

Esempi di misure di salvaguardia appropriate che avrebbero potuto ridurre i rischi, se attuate preventivamente:

- A ciascun utente devono essere attribuiti i propri account e l'accesso ai dati personali dovrebbe essere autorizzato esclusivamente applicando principi di necessità di sapere e di privilegio minimo. Ciò vale anche per i venditori, gli incaricati della manutenzione e altri soggetti che abbiano necessità di accedere temporaneamente alla base dati: i terzi dovrebbero essere autorizzati ad accedere solo alla funzionalità e ai dati di cui hanno bisogno per espletare i compiti loro assegnati, per un periodo di tempo non superiore a quello strettamente necessario. Andrebbe limitato l'utilizzo di account con "accesso completo" alla base dati e si dovrebbero mettere in atto sistemi per tracciare e limitare l'utilizzo di questo tipo di account. Attuando tali misure di salvaguardia si sarebbe potuta prevenire la violazione o attenuarne l'impatto.
- Se le password fossero state memorizzate in modo sicuro (ad esempio con un salt e utilizzando una funzione crittografica di hash), si sarebbero notevolmente ridotti gli effetti negativi secondari sugli interessati. Tuttavia, gli utenti che avessero scelto password deboli potrebbero ancora essere a rischio, in particolare qualora utilizzino le medesime credenziali di accesso per altri servizi online. Tale rischio avrebbe potuto essere attenuato suggerendo a detti utenti di scegliere password più forti.

Caso 4. *Una busta contenente ricevute di pagamento con carta di credito è stata gettata per errore in un cestino gettacarte anziché essere distrutta in modo sicuro. Il cestino è stato svuotato in un bidone lasciato all'esterno del negozio ai fini della raccolta dei rifiuti. Un terzo ha prelevato la busta da quest'ultimo bidone e ha sparso le ricevute in un quartiere limitrofo. I dati comprendevano i dettagli completi delle carte di credito[7] e i nomi dei titolari. In alcuni casi erano visibili anche le firme dei titolari. Le persone interessate sono 800.*

Possibili conseguenze ed effetti negativi della violazione della riservatezza:

- La violazione potrebbe avere un impatto finanziario sugli interessati qualora i dati delle loro carte fossero ancora validi e venissero utilizzati abusivamente[8].

Poiché la violazione rischia di ledere gli interessati, deve essere loro notificata. Nella fattispecie, se non sono stati tenuti altri registri, potrebbe risultare difficile informare individualmente tutti gli interessati, poiché potrebbe non essere noto esattamente quali ricevute fossero contenute nella busta. Il negozio dovrebbe avvisare i gestori delle carte di credito, di modo che possano monitorare eventuali transazioni fraudolente. Un altro orientamento pratico proposto nel regolamento (UE) n. 611/2013[9] prevede che il fornitore, qualora, "malgrado i ragionevoli sforzi profusi, non sia in grado di individuare entro il termine di cui [all'articolo 3,] paragrafo 3[,] tutte le persone che potrebbero essere lese dalla violazione di dati personali, può informare tali persone entro lo stesso termine attraverso annunci pubblicitari nei principali mezzi di comunicazione nazionali o regionali negli Stati membri interessati". Pertanto, nel caso in cui il negozio abbia una clientela prevalentemente locale, potrebbe essere sufficiente la notifica attraverso un quotidiano regionale. Inoltre, informando le società delle carte di credito della violazione si potrebbe contribuire alla tutela dei loro clienti.

Se la busta fosse stata recuperata dal responsabile del trattamento da uno dei contenitori dei rifiuti, o comunque non venisse aperta, difficilmente l'imprevisto potrebbe ledere i titolari delle carte; pertanto, non occorrerebbe notificare la violazione agli interessati.

Esempi di misure di salvaguardia appropriate che avrebbero potuto ridurre i rischi, se attuate preventivamente:

- Informando i dipendenti delle possibili conseguenze di siffatte violazioni e utilizzando un idoneo distruggidocumenti[10] o un servizio di distruzione degli archivi per distruggere le ricevute dei pagamenti effettuati con carte di credito (e analoghi documenti cartacei contenenti dati personali) prima di buttarle nei rifiuti, si ridurrebbe notevolmente il rischio di violazioni di questo tipo.

[7] Sebbene la prassi migliore consista nel troncamento dei dati della carta di credito sulla ricevuta cartacea del cliente, tale funzione non è disponibile in tutti i terminali POS e i dati completi potrebbero comunque essere stampati sulle copie delle ricevute per l'esercente.

[8] Poiché i dati delle carte di credito possono essere utilizzati anche senza CVV (o codice equivalente), devono essere notificate anche le violazioni che non riguardino tale codice.

[9] A prescindere dalla circostanza che detto regolamento sia inapplicabile in questo contesto.

[10] Ad esempio, un distruggidocumenti di classe 2 con un livello di sicurezza P-4 o superiore secondo la classificazione DIN 66399 per i documenti cartacei.

- Utilizzare terminali POS che non stampino i dati completi delle carte di credito.

Caso 5. *Il computer portatile cifrato di un consulente finanziario è stato rubato dal bagagliaio di un'autovettura. La violazione riguarda tutti i dati delle analisi finanziarie – ad es. mutui, stipendi, richieste di finanziamento – relative a 1 000 interessati. La passphrase utilizzata come chiave di crittografia non è stata compromessa, ma non sono disponibili copie di riserva.*

Possibili conseguenze ed effetti negativi della violazione della riservatezza:

- A seconda della natura esatta dei dati violati, il loro utilizzo abusivo potrebbe avere vari impatti sugli interessati. Tuttavia, poiché l'intero disco del computer era stato sottoposto a crittografia (all'avanguardia) con una passphrase forte che non è stata compromessa, non si sono verificate divulgazioni non autorizzate.

Possibili conseguenze ed effetti negativi:

- L'indisponibilità dei dati implica che gli interessati debbano fornire nuovamente le informazioni necessarie. Ciò comporta un effetto negativo modesto che si sostanzia in dispendi di tempo e disagi.
- In alcuni casi potrebbe anche causare la mancata presentazione di un documento o l'inosservanza del termine fissato a tale scopo, il che potrebbe avere diversi impatti secondari sugli interessati, a seconda del contesto: sanzioni pecuniarie, perdita di reddito o di profitti previsti, perdita di opportunità, risoluzione di contratti di compravendita, ecc.

Poiché le informazioni sono andate perdute e gli effetti della violazione della disponibilità non sono stati attenuati, la violazione dei dati personali rischia di ledere gli interessati. Pertanto, deve essere loro notificata. Con tale comunicazione, oltre a segnalare la necessità di fornire nuovamente i dati al consulente finanziario, si informeranno gli interessati in merito alle conseguenze e agli effetti negativi che potrebbero derivare dalla violazione.

Esempio di misura di salvaguardia appropriata che avrebbe potuto ridurre i rischi, se attuata preventivamente:

- Una soluzione di backup sicura ed efficace avrebbe consentito di recuperare i dati. Se fosse stata disponibile una copia di riserva aggiornata dei dati, non si sarebbe verificata alcuna violazione della disponibilità e la notifica non sarebbe stata necessaria.

Caso 6. *Il gestore di una rete di telefonia mobile fornisce un servizio di account online, al quale gli abbonati possono accedere per visionare fatture e attività dell'account recenti. È stato rilevato un accesso illecito alla base dati in cui sono conservate le password di un sito web. Il terzo ha acceduto ai dati di autenticazione degli utenti (nomi utente e password codificati con un hash MD5 senza salt).*

Possibili conseguenze ed effetti negativi della violazione della riservatezza:

- Disponendo dei nomi utente, il terzo potrebbe ricavarne le password e quindi accedere all'account di qualsiasi cliente.
- Poiché molte persone utilizzano la medesima combinazione di nome utente e password per una molteplicità di account online, il terzo potrebbe accedere ad altri account degli interessati, compresi, in alcuni casi, quelli di posta elettronica.

Dal momento che le password erano state codificate con un semplice hash, non possono essere considerate incomprensibili ai sensi dell'articolo 4, paragrafo 2, del regolamento (UE) n. 611/2013[11] della Commissione. Pertanto, non si applica l'esenzione dall'obbligo di notifica agli interessati.

Atteso che tale violazione rischia di ledere gli interessati e l'esenzione non è applicabile, si dovrebbero informare i clienti coinvolti raccomandando chiaramente agli utenti di modificare le loro password in tutti gli account che condividono la medesima password compromessa. In ogni caso, tutti gli utenti dovrebbero essere obbligati a modificare la loro password – utilizzando un metodo sicuro - nel momento in cui tentano di accedere al servizio.

Esempio di misura di salvaguardia appropriata che avrebbe potuto ridurre i rischi, se attuata preventivamente:

- Se le password fossero state memorizzate in modo sicuro (ossia codificate mediante hash crittografici e salt con una funzione di hash all'avanguardia e una chiave o salt), si sarebbero fortemente ridotti gli effetti negativi sugli interessati. Tuttavia, gli utenti che avessero scelto password deboli potrebbero essere ancora a rischio, specialmente qualora utilizzassero le medesime credenziali di accesso per altri servizi online.

Caso 7. *Un fornitore di servizi Internet mette a disposizione un servizio attraverso il quale gli abbonati possono visionare i dettagli dei loro account, la cronologia di navigazione in Internet comprensiva di banda mensile e i siti visitati frequentemente. Un errore di codifica nel sito web provoca la mancata convalida delle credenziali di accesso dell'utente e rende i dati accessibili attraverso una modifica del valore ID dell'abbonato indicato nei parametri URL. È possibile accedere ai dati degli account di tutti i clienti scorrendo ciclicamente gli ID consecutivi degli abbonati.*

[11] L'articolo 4, paragrafo 2, stabilisce che i dati sono considerati incomprensibili se:

a) sono stati crittografati in modo sicuro mediante un algoritmo standardizzato, la chiave utilizzata per decifrarli non è stata compromessa nell'ambito di una violazione della sicurezza ed è stata generata in modo tale da non poter essere individuata con i mezzi tecnologici disponibili da qualcuno che non sia autorizzato ad accedervi; o

b) sono stati sostituiti dal loro valore hash calcolato mediante una funzione di hash con chiave crittografica normalizzata, la chiave utilizzata per l'hashing dei dati non è stata compromessa nell'ambito di una violazione della sicurezza ed è stata generata in modo tale da non poter essere individuata con i mezzi tecnologici disponibili da qualcuno che non sia autorizzato ad accedervi.

Possibili conseguenze ed effetti negativi della violazione della riservatezza:

- I dati potrebbero essere utilizzati a fini di "spamming" nei confronti degli interessati tramite messaggi di posta elettronica o chiamate telefoniche.
- I dati potrebbero delineare un profilo dell'abbonato, e rivelano dettagli del suo comportamento dai quali potrebbero emergere informazioni sensibili. Ciò potrebbe avere un impatto sull'ambiente lavorativo e/o familiare degli interessati.

Tale violazione rischia di ledere gli interessati e pertanto deve essere notificata ai clienti.

Esempio di misura di salvaguardia appropriata che avrebbe potuto ridurre i rischi, se attuata preventivamente:

- Il monitoraggio delle possibili vulnerabilità delle tecnologie impiegate, come illustrato nel caso 2, lo svolgimento di test su una piattaforma preproduzione prima della messa in funzione nonché la revisione dei codici avrebbero potuto scongiurare la violazione.

3. Possibili scenari nei quali non è richiesta la notifica agli interessati

Sebbene le conseguenze di una violazione dei dati personali debbano essere valutate caso per caso, al fine di prendere in debita considerazione tutti gli elementi rilevanti nella valutazione delle presumibili ripercussioni negative sugli interessati, il responsabile del trattamento può tenere conto, come criterio generale e in aggiunta alle ipotesi di esenzione descritte nella sezione precedente, anche del fatto che la notifica agli interessati non è richiesta in taluni casi specifici.

Fra tali casi possono rientrare:

- La violazione dei dati personali riguardante unicamente la riservatezza, se i dati sono stati crittografati in modo sicuro con un algoritmo all'avanguardia, la chiave utilizzata per decifrare i dati non è stata compromessa nell'ambito di una violazione della sicurezza ed è stata generata in modo tale da non poter essere individuata con i mezzi tecnologici disponibili da qualcuno che non sia autorizzato ad accedervi. Infatti, tali misure rendono i dati incomprensibili a chiunque non sia autorizzato all'accesso.

- I dati, quali le password, sono stati codificati in modo sicuro con un hash e un salt. Il valore hash è stato calcolato mediante una funzione di hash con chiave crittografica all'avanguardia, la chiave utilizzata per l'hashing dei dati non è stata compromessa nell'ambito di una violazione della sicurezza ed è stata generata in modo tale da non poter essere individuata con i mezzi tecnologici disponibili da qualcuno che non sia autorizzato ad accedervi.

4. Domande e risposte

In quali casi non è obbligatorio informare gli interessati?

- Quando la violazione della sicurezza non costituisce una violazione dei dati personali (v. domanda seguente).

- Quando è stato dimostrato in modo convincente all'autorità competente che, secondo i risultati di una valutazione della gravità, la violazione non rischia di pregiudicare i dati personali o la vita privata degli interessati.
- Quando il fornitore ha dimostrato in modo convincente all'autorità competente di avere utilizzato le opportune misure tecnologiche di protezione e che tali misure erano state applicate ai dati interessati dalla violazione della sicurezza. Ad esempio, nel caso in cui la violazione (della sola riservatezza) dei dati personali riguardi unicamente dati cifrati con un algoritmo all'avanguardia oppure dati codificati con un salt o un hash con chiave generato mediante una funzione hash all'avanguardia, e tali chiavi segrete o salt non siano stati compromessi.
- La notifica delle violazioni dei dati descritte nel presente parere costituisce una buona pratica per tutti i responsabili del trattamento, anche nel caso in cui la notifica non sia obbligatoria.

In quali circostanze una violazione della sicurezza diventa una violazione dei dati personali?

Una violazione della sicurezza costituisce una violazione dei dati personali quando i dati violati sono dati personali, quali definiti dall'articolo 2, lettera a), della direttiva 95/46/CE, secondo cui si intende per "dati personali": qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale".

Il parere 4/2007 precisa che tale violazione riguarda i dati relativi ad una persona: "una persona può essere identificata direttamente attraverso il nome o indirettamente attraverso il numero di telefono, il numero identificativo della automobile, il numero di sicurezza sociale, del passaporto o una combinazione di criteri significativi che ne consentano il riconoscimento all'interno del gruppo al quale appartiene (età, occupazione, luogo di residenza, ecc.)". Il parere 4/2007 fornisce ulteriori orientamenti al riguardo.

Si devono prendere in considerazione i probabili effetti secondari?

Sì, le violazioni dei dati devono essere notificate agli interessati se la violazione rischia di pregiudicarne i dati personali o la vita privata.
Pertanto, occorre prendere in considerazione tutte le possibili conseguenze e i potenziali effetti negativi sugli interessati.

> ***Esempio 1:*** *Il sito web di una società di intrattenimento musicale è stato violato e la base dati degli utenti è stata rubata e pubblicata in rete. I dati personali trafugati comprendono nomi e cognomi, preferenze musicali, nonché nomi utente e password degli utenti registrati sul sito della società. Gli utenti interessati sono 9 000.*

In tali circostanze, nella maggior parte dei casi l'effetto negativo diretto potrebbe apparire molto limitato (trattandosi di una fuga di informazioni relative a preferenze musicali) e ci si potrebbe quindi domandare se sia necessario informare gli interessati. Tuttavia, dal momento che le password sono state compromesse, dovranno essere rinnovate dal responsabile del trattamento. Nel corso di tale operazione occorrerà informare gli utenti dei motivi per i quali

si procede al rinnovo delle password. Inoltre, poiché molti utenti utilizzano la medesima password per account diversi[12], la violazione comporta presumibilmente, come effetto negativo secondario, una violazione della riservatezza in relazione ad altri account. Gli interessati potranno ridurre al minimo tali effetti secondari modificando le proprie password di tutti gli altri account. Pertanto, la notifica dovrebbe anche contenere le informazioni relative ai possibili effetti negativi su altri account e, conseguentemente, la raccomandazione di utilizzare password diverse sui vari siti web e di rinnovare le password di tutti gli account per i quali venivano utilizzate le password compromesse.

> ***Esempio 2:*** *Un secondo esempio potrebbe essere quello dello smarrimento di un CD spedito ad un avvocato tramite raccomandata e contenente elementi di prova da utilizzare nell'ambito di un procedimento penale.*

La violazione diretta riguarda la disponibilità. L'impatto sull'interessato (o sugli interessati) potrebbe essere trascurabile o molto grave, a seconda che si possano o meno adottare tempestivamente le misure necessarie.
Tuttavia, potrebbero verificarsi effetti negativi secondari qualora il CD non fosse adeguatamente protetto e si verificasse un accesso ai dati. Infatti, i terzi che venissero in possesso del CD potrebbero leggerlo, venderlo a giornalisti, ecc. Tale effetto secondario potrebbe avere un impatto molto grave sull'interessato (o sugli interessati).

Nella fattispecie, se il CD potesse essere inviato nuovamente in tempo utile, l'impatto diretto sull'interessato (o sugli interessati) sarebbe trascurabile e la notifica non sarebbe richiesta, mentre la potenziale violazione secondaria potrebbe avere conseguenze molti gravi e andrebbe certamente notificata.

Se la persona interessata è una sola, la violazione deve esserle notificata?

Sì, la direttiva 2002/58/CE non subordina la notifica di una violazione dei dati personali all'esistenza di un numero minimo di interessati. L'articolo 3, paragrafo 1, del regolamento (UE) n. 611/2013 prevede che "*[q]uando la violazione di dati personali rischia di pregiudicare i dati personali o la vita privata di un abbonato o di altra persona, in aggiunta alla notifica di cui all'articolo 2 il fornitore comunica l'avvenuta violazione anche all'abbonato o all'altra persona*".

Pertanto, il responsabile del trattamento deve procedere alla notifica ove la stessa risulti necessaria alla luce dei possibili effetti negativi, indipendentemente dal numero degli interessati.

Come si devono trattare i dati che potrebbero essere pubblici?

Due punti meritano di essere presi in considerazione.

1. Il termine "pubblico" può implicare livelli diversi di disponibilità: i dati possono essere liberamente accessibili su Internet, pubblicamente disponibili nell'ambito di un servizio in abbonamento, pubblicamente disponibili offline su richiesta, ecc.

[12] Secondo studi recenti, tra il 55 e l'80% degli utenti di Internet utilizza la medesima password per account diversi.

Ad esempio, in Francia, in occasione delle elezioni, le liste elettorali vengono affisse ai muri del palazzo comunale e qualsiasi elettore o partito politico può ottenerne copia, ma la legge non ne consente la pubblicazione online.
Pertanto, l'invio accidentale della versione elettronica delle liste a un elettore non autorizzato a riceverle o lo smarrimento di una versione cartacea della stessa non costituirebbe una violazione della riservatezza, a differenza della pubblicazione delle liste su Internet, che andrebbe notificata.

2. Alcuni dati possono essere pubblici per alcune persone interessate, ma non per altre.
Ad esempio, una lista di numeri telefonici collegati a un cognome può contenere sia numeri accessibili al pubblico attraverso gli elenchi telefonici, sia numeri riservati.

In sintesi, se la violazione comporta una modifica del grado di disponibilità o di pubblicità dei dati, va considerata come una violazione della riservatezza e deve essere notificata (sempre che la violazione rischi di ledere gli interessati).

Come si possono informare gli interessati quando i dati di contatto sono insufficienti o ignoti?

Vi sono casi in cui il fornitore, pur essendo legato all'utilizzatore finale da un rapporto contrattuale diretto, non dispone di dati sufficienti per garantire un'adeguata informazione. In tali circostanze, sebbene la notifica possa essere effettuata attraverso annunci sui mezzi di comunicazione, rimane comunque l'obbligo di compiere ogni ragionevole sforzo per informare gli interessati individualmente[13].

Sebbene il fornitore debba assolvere l'obbligo di compiere ogni ragionevole sforzo mettendo in atto qualsiasi ragionevole meccanismo idoneo a garantire che tutti gli interessati siano informati della violazione, ciò non esclude tuttavia che esso possa chiedere l'assistenza di altri fornitori o responsabili del trattamento che detengano i dati di contatto. Pertanto, considerando il caso 4, il responsabile del trattamento che non disponga dei dati necessari per informare i titolari delle carte interessati potrebbe rivolgersi all'intermediario del pagamento, il quale potrebbe facilmente contattarli. In altri casi potrebbe essere necessaria la collaborazione delle autorità competenti, le quali andrebbero informate, in ogni caso, del fatto che il fornitore non è in grado di garantire notifiche individuali.

È necessario informare gli interessati che non sono stati lesi dalla violazione?

No, sempreché tali persone possano essere individuate in modo attendibile. Ad esempio, qualora si possa dimostrare che gli interessati appartenenti a una determinata sottocategoria non sono stati lesi dall'incidente di sicurezza, potrebbe non essere necessario informarli. Tuttavia, ai fini della decisione, il responsabile del trattamento deve tenere conto di tutti i

[13] Ai sensi dell'articolo 3, paragrafo 7, del regolamento (UE) n. 611/2013, il fornitore che, malgrado i ragionevoli sforzi profusi, non sia in grado di individuare entro il termine applicabile tutte le persone che potrebbero essere lese dalla violazione di dati personali, informerà tali persone entro lo stesso termine attraverso annunci pubblicitari nei principali mezzi di comunicazione nazionali o regionali negli Stati membri interessati. Sulla stessa linea, la suddetta disposizione prevede altresì che il fornitore continui a compiere tutti gli sforzi ragionevoli per identificare tali persone e informarle non appena possibile.

possibili effetti negativi. A seconda della natura della violazione, anche la mancata notifica può provocare disagi agli interessati.