Metodologia di identificazione di una violazione dei dati personali

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche. E' bene precisare, tuttavia, che non ogni incidente di sicurezza rappresenta una violazione dei dati personali.
Il presente documento vuole offrire, in maniera pratica, gli strumenti per individuare le dinamiche che possono determinare una violazione.

Individuazione del tipo di violazione

Una violazione dei dati personali può essere definita nei seguenti casi

Violazione di riservatezza
La violazione comporta la divulgazione dei dati personali o l'accesso non autorizzato o accidentale agli stessi. A puro titolo di esempio una violazione della riservatezza può verificarsi nei seguenti casi:

- pubblicazione di un documento nella sua interezza, senza oscurare i dati personali non necessari;
- invio di un messaggio contenente dati a soggetti non interessati al trattamento;
- postazione di lavoro lasciata senza prima prendere le opportune precauzioni, con la possibilità che terze persone possono prendere visione di informazioni;
- dato non pubblico comunicato a terzi in modo non autorizzato;
- accesso non autorizzato a computer, archivi cartacei o database;
- documento contenente dati personali, cestinato senza essere prima distrutto;
- supporto di memoria contenente dati personali non protetti smarrito o rubato (pennetta usb, smartphone).

La violazione di integrità
La violazione si verifica quando avviene un'alterazione (modifica) di dati personali non autorizzata o accidentale.
A puro titolo di esempio:

- archivio danneggiato che non consente il ripristino integrale dei dati;
- supporto di memoria contenente dati personali non protetti smarrito o rubato (pennetta usb, smartphone).

La violazione di disponibilità
La violazione è determinata dalla distruzione o perdita accidentale di dati personali.
A puro titolo di esempio:

- dati cancellati accidentalmente o da soggetti non autorizzati;
- chiave di decriptazione persa;
- dati non ripristinabili dalle copie di sicurezza;
- interruzione significativa di un servizio ("black out" elettrico, attacchi informatici, malfunzionamento di dispositivo informatico);
- supporto di memoria contenente dati personali non protetti smarrito o rubato (pennetta usb, smartphone).

Nota: un singolo incidente può determinare contemporaneamente più violazioni di sicurezza (es. il furto di una pendrive o di uno smartphone può comportare, allo stesso tempo, una violazione della riservatezza, dell'integrità e della disponibilità dei dati).

Determinazione della gravità di una violazione

Al fine di valutare un incidente sui dati personali, bisogna tenere in considerazione anche il livello di gravità della violazione.

Livello di compromissione basso: nel caso di compromissione di dati comuni (es. Nome e Cognome); nel caso in cui sono state applicate misure di sicurezza tali da limitare l'impatto sugli interessati (es. pseudonimizzazione o crittografia); nel caso in cui l'evento riguarda un numero ristretto di individui.

Livello di impatto sugli interessati basso: i soggetti possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).

Livello di compromissione medio: nel caso di compromissione di dati aggregati (es. nome, cognome, data di nascita ed indirizzo), riguardante un numero significativo o una categoria di individui (es. dipendenti, clienti, studenti).

Livello di impatto sugli interessati medio: i soggetti possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).

Livello di compromissione alto: nel caso di compromissione di dati riservati (es. username e password d'accesso, dati personali protetti da segreto professionale, dati che possono rilevare la condizione economica, le preferenze personali, gli interessi, l'ubicazione o gli spostamenti) che possono determinare nei confronti di un elevato numero di interessati la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie.

Livello di impatto sugli interessati alto: i soggetti possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della vita sociale, ecc.).

Livello di compromissione critico: nel caso di compromissione di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Livello di impatto sugli interessati critico: i soggetti possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Valutazione del rischio per il trattamento
Il rischio per il trattamento è uno degli elementi da prendere in considerazione per determinare la gravità di una violazione dei dati personali, e dipende da specifici elementi: - categorie dei dati personali; - categorie di interessati; - numero di individui coinvolti; - probabilità di identificazione degli interessati; - misure di sicurezza applicate al trattamento.

Gli esempi - non esaustivi - che seguono aiuteranno il Titolare e gli altri soggetti coinvolti nel trattamento ad individuare una violazione dei dati personali e a stabilire se è necessaria la notifica all'Autorità Garante. 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	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 chiavetta 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.
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.	Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	A seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata.	
Un titolare del trattamento subisce un attacco tramite *malware* 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.	Sì, effettuare la segnalazione all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	A seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	Se fosse stato disponibile un backup e i dati 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.
La società di *hosting* del sito 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, senza ingiustificato ritardo, la notifica al Titolare del trattamento, che dovrà valutare la violazione e l'eventuale notifica.	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 sempre comunicare al Titolare del trattamento l'avvenuta violazione dei dati. La violazione va obbligatoriamente riportata nei registri delle violazioni, sia del Titolare che del Responsabile del trattamento.

I dati personali di un gran numero di interessati vengono inviati per errore a una mailing list sbagliata.	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.	
Una email viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo email di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se vengono rivelati dati sensibili o se altri fattori presentano rischi elevati.	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.