La gestione del data breach

A domanda risponde Prof. Avv. Michele IASELLI

9 luglio 2024 - dalle ore 11.30 alle 12.30

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione
degli Enti Locali
Email info@dpoinrete.it
Numero Verde 800.16.56.54
Web: www.dpoinrete.it
www.asmel.eu

I dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.

L’art. 33 del Regolamento dispone che in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente ai sensi dell'articolo 51 senza ingiustificato ritardo, 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 non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata di una giustificazione motivata (Data breach).

Tale notifica deve come minimo:
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 Garante per la protezione dei dati personali già per il passato aveva adottato una serie di provvedimenti che introducevano in determinati settori l'obbligo di comunicare eventuali violazioni di dati personali *(data breach*) all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati.

- Provvedimento del Garante n. 161 del 4 aprile 2013 con il quale viene prescritto l'obbligo di comunicazione al Garante (mediante un apposito modello di comunicazione) da parte dei fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli internet point, le reti aziendali).
- Provvedimento n. 513 del 12 novembre 2014 dove viene previsto che entro 24 ore dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

- Provvedimento n. 331 del 4 giugno 2015 dove viene sancito che entro 48 ore dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante (tramite il modello allegato al provvedimento) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.
- Provvedimento del 2 luglio 2015 "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche" con il quale il Garante prescrive, ai sensi dell'articolo 154, comma 1, lett. c), del Codice in materia di protezione dei dati personali, che le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 devono comunicare all'Autorità, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possono avere un impatto significativo sui dati personali contenuti nelle proprie banche dati e che tali comunicazioni dovevano essere redatte secondo uno schema specifico allegato al provvedimento e inviate tramite posta elettronica o posta elettronica certificata.

L’art. 34, invece, prevede un’altra importante incombenza collegata alla precedente e cioè la comunicazione di una violazione dei dati personali all’interessato.
Difatti, 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.

La predetta comunicazione descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e non è richiesta se:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Si ricorda, inoltre, che il Comitato europeo per la protezione dei dati (EDPB) ha predisposto delle Linee guida 1/2021 relative ad esempi di violazioni di dati personali.

Il Comitato ricorda che per violazione dei dati personali – ai sensi dell'art. 4 Regolamento UE 2016/679 (GDPR) – si intende "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".

Fonti di rischio interne

Fonti di rischio esterne

Attacchi informatici

Ransomware

Furti di dati

Misure tecniche

Il Comitato fornisce un elenco (non esaustivo e meramente esemplificativo) di misure tecniche per prevenire e mitigare gli effetti di potenziali attacchi informatici:

- adottare adeguate misure di criptazione dei dati e di gestione delle password, soprattutto quando il trattamento ha ad oggetto dati sensibili o finanziari;
- mantenere costantemente aggiornati i sistemi e tenere traccia di tali aggiornamenti, di modo da poter dimostrare la compliance con il principio di accountability di cui all'art. 5, par. 2 del GDPR;
- fare ricorso a strumenti di autenticazione "forti" (ad esempio l'autenticazione a due fattori) e adeguate policy di gestione e aggiornamento delle password;
- condurre audit e assessment periodici per verificare la costante adeguatezza delle misure;
- mantenere aggiornate le copie di backup in modo assicurarsi la possibilità di procedere rapidamente al recovery dei dati e delle informazioni.

La gestione di un data breach

La soluzione migliore per gestire e prevenire un data breach si divide in sette punti fondamentali:

dpo in rete

- Monitoraggio continuo
- Avviare un processo decisionale e di gestione in situazioni di tranquillità
- Valutare, ridurre e gestire i rischi
- Riduzione dei costi
- Processi definiti senza improvvisazione
- Gestione con compagnie assicurative
- Individuazione di partner esterni

La definizione delle attività da seguire per prevenire un data breach, richiede tempo e calma.
La prima fase comporta la definizione di una policy aziendale, seguita da un organizzazione e formazione dei dipendenti con scadenze ben definite.
Successivamente, bisogna valutare periodicamente le vulnerabilità tramite l'aiuto di consulenti esterni o autonomamente; effettuare test di social engineering (il tutto eseguito tramite le opportune autorizzazioni).
Un'ulteriore attenzione riguarda il costante monitoraggio e aggiornamento dei sistemi e la redazione di una politica rigida sulla gestione delle password.
Infine, è necessario definire i comportamenti "fisiologici" di sistemi e rete monitorando e analizzando il traffico e le performance di rete e sistemi, effettuare l'analisi dei log, e verificare l'efficienza dei backup.

Le violazioni dei dati possono verificarsi per una serie di motivi, anche accidentali, ma gli attacchi mirati sono generalmente effettuati in questi quattro modi:

- Utilizzando le vulnerabilità di sistema
- Password deboli
- Drive-by Download
- Attacchi malware mirati

Le misure preventive da adottare per limitare i rischi di data breach

Al fine di organizzare meglio la procedura di data breach, bisogna strutturare e monitorare costantemente i ruoli e le attività da svolgere.

1. Il primo passo per costruire una procedura efficiente di data breach è assegnare ruoli specifici a tutti i potenziali interessati, questi devono essere dotati di competenza, esperienza, responsabilità ed autorità.
2. Successivamente dovranno essere monitorate le vulnerabilità e i rischi, e ricercare soluzioni e processi per mitigare i rischi.
3. Infine, la figura del DPO o del Referente interno per le attività di privacy, è fondamentale per ricevere le notizie di possibili incidenti, per valutarli e documentarli in collaborazione con il Titolare o Responsabile del trattamento.

Un errore da non commettere, però, è quello di investire quasi tutte le risorse aziendali nella sola fase di prevenzione, dedicando poche o nulle risorse al monitoraggio ed alle azioni di risposta in seguito ad un data breach.
E’, invece, importante sostenere ed investire risorse e tempo in egual misura nella prevenzione, monitoraggio e azioni di risposta al data breach.

L’autovalutazione suggerita dal Garante

Notifica di una violazione dei dati personali (data breach)

art. 33 del Regolamento (UE) 2016/679 - art. 26 del D.Lgs. 51/2018

Auto valutazione per la notifica di una violazione dei dati personali (data breach)

Compilazione della notifica

Istruzioni

Informativa sul trattamento dei dati personali

Pagina informativa - Violazione dei dati personali (data breach)

Fac-simile del modello

La procedura di data breach

Per gestire una violazione dei dati personali è necessario seguire i seguenti cinque step:

Step 1: Identificazione e indagine preliminare
Step 2: Contenimento, recovery e risk assessment
Step 3: Eventuale notifica all'Autorità Garante
Step 4: Eventuale comunicazione agli interessati
Step 5: Documentazione della violazione

Step 1: Identificazione e indagine preliminare

ALLEGATO A – MODULO DI COMUNICAZIONE DATA BREACH

Qualora scopra un Data Breach, è pregato di informare immediatamente il Suo superiore gerarchico, il quale, a sua volta, dovrà compilare la modulistica a seguire e inviarla a mezzo e-mail al seguente indirizzo email: - .....

Comunicazione di Data Breach	**Note**
Data scoperta violazione:	
Data dell'incidente:	
Luogo della violazione (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili):	
Nome della persona che ha riferito della violazione:	
Dati di contatto della persona che ha riferito della violazione (indirizzo e-mail, numero telefonico): *In caso di destinatario esterno indicare la ragione sociale:*	
Denominazione della/e banca/che dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati:	
Categorie e numero approssimativo di interessati coinvolti nella violazione:	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta della violazione:	
Responsabile del dipartimento:	
data:	

Step 2: Contenimento, Recovery e risk assessment

Una volta stabilito che un Data Breach è avvenuto, il Titolare del trattamento o un suo delegato insieme al DPO dovranno stabilire:

- se esistono azioni che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… ecc.);
- una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
- se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

ALLEGATO B – MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL DATA BREACH

Assessment di gravità	**A cura del DPO insieme con l'amministratore di sistema e il Responsabile dell'ufficio coinvolto della violazione**
Dispositivi oggetto del Data Breach (computer, rete dispositivo mobile, file o parte di un file, strumento di back up, documento cartaceo, altro).	
Modalità di esposizione al rischio (tipo di violazione): lettura (presumibilmente i dati non sono stati copiati), copia (i dati sono ancora presenti sui sistemi ma del titolare), alterazione (i dati sono presenti sui sistemi ma sono stati alterati), cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione), furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione), altro.	
Breve descrizione dei sistemi di elaborazione o di memorizzazione dati coinvolti, con indicazione della loro ubicazione.	
Se laptop è stato perso/rubato: quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?	
Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati violata?	
La violazione può avere conseguenze negative in uno dei seguenti settori enteli: operation, research, financial, legal, liability or reputation?	

Qual è la natura dei dati coinvolti? Compilare le sezioni sottostanti:	
○ I dati particolari (come identificati dal Regolamento (UE) 2016/679 relative ad una persona viva ed individuabile: a) origine razziale o etnica; b) opinion politiche, convinzioni religiose o filosofiche; c) appartenenza sindacale; d) dati genetici; e) dati biometrici; f) dati giudiziari; g) relative alla salute o all'orientamento sessuale di una persona.	

o Informazioni che possono essere utilizzate per commettere furti d'identità (i.e. dati di accesso e di identificazione, codice fiscale e copie di carta d'identità, passaporto o carte di credito);	
o Informazioni personali relative a soggetti fragili (i.e. anziani, disabili, minori);	
o Profili individuali che includono informazioni relative a performance lavorative, salario o stato di famiglia, sanzioni disciplinari, che potrebbero causare danni significativi alle persone;	
Altro:	

La violazione può comportare pregiudizio alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro dato economico o sociale significativo?	
Gli interessati rischiano di essere privati dell'esercizio del controllo sui dati personali che li riguardano?	
Quali misure tecniche e organizzative sono adottate ai dati oggetto di violazione? (i.e. La pseudonimizzazione e la cifratura dei dati personali)	
Il Titolare del trattamento ha aderito ad un codice di condotta approvato ai sensi dell'art. 40 Regolamento (UE) o un meccanismo di certificazione di cui all'art. 42 Regolamento (UE)?	
Il Titolare del trattamento ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati successivamente alla violazione?	
Classificazione della violazione (1, 2 o 3) e motivazioni:	
Notificazione del Data Breach all'Autorità Garante	**Si/NO Se sì, notificato in data: Dettagli:**
Comunicazione del Data Breach agli interessati	**Si/NO Se sì, notificato in data: Dettagli:**
Comunicazione del Data Breach ad altri soggetti (i.e. casa madre)	**Si/NO Se sì, notificato in data: Dettagli:**

Step 3: Eventuale notifica all’Autorità Garante competente

Una volta valutata la necessità di effettuare notifica della violazione dei dati subita sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'ente dovrà provvedervi, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.

Step 4: Eventuale comunicazione agli interessati

Una volta valutata la necessità di effettuare la comunicazione della violazione dei dati a coloro dei cui dati si tratta, sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, l'ente dovrà provvedervi, senza ingiustificato ritardo.

Step 5: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente comunicato dai Destinatari attraverso l'Allegato A, l'ente sarà tenuta a documentarlo.

ALLEGATO C – REGISTRO DEI DATA BREACH

Numero Violazione	Data Violazione	Natura della Violazione	Categoria di Interessati	Categoria di dati personali coinvolti	Numero approssimativo di registrazioni dati personali	Conseguenze della Violazione	Contromisure adottate	Notifica Autorità Garante Privacy (S/N)	Comunicazione ai soggetti interessati (S/N)