Data breach: come prevenirli e gestirli correttamente

INDICE – Data breach: come prevenirli e gestirli correttamente

[Introduzione: definizione di Data breach](#)

[Notifica](#)

[Comunicazione all’interessato](#)

[Gestione Data breach](#)



Introduzione: definizione di Data breach

Con l’espressione “data breach” si intendono tutte quelle ipotesi di violazione di sicurezza che comportano

accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali raccolti, trasmessi, conservati o comunque trattati. Si tratta sostanzialmente di un fallimento delle misure di sicurezza adottate per la protezione dei dati personali trattati.

Nel momento in cui si verifica la violazione, il Titolare deve attivare tutte le misure necessarie per gestire la crisi, dandone al contempo tempestiva comunicazione al Garante della privacy e all'interessato a cui si riferiscono i dati.

Compito delle aziende, è dunque quello di dotarsi di modelli organizzativi atti a: pianificare le misure preventive per individuare e contenere una violazione; valutare il rischio per gli individui, stabilendo se sia necessaria o meno la notifica all'Autorità Garante e comunicare la violazione dei dati alle persone interessate.

Il Gruppo di lavoro Articolo 29

Il Gruppo di lavoro Articolo 29 (di seguito WP29) ha adottato delle linee guida con l'obiettivo di chiarire le modalità di applicazione delle disposizioni del Regolamento UE 2016/679, relativi alla notifica della violazione dei dati personali. In particolare, il WP29, ha suddiviso la violazione dei dati personali in tre categorie:

- Violazione di riservatezza: si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
- Violazione dell'integrità: si verifica un'alterazione dei dati non autorizzata o accidentale;
- Violazione della disponibilità: si verifica la perdita, l'inaccessibilità o la distruzione, accidentale o non autorizzata, delle informazioni personali.

Una violazione dei dati personali può avere delle conseguenze estremamente pesanti sugli individui, conseguenze che possono comportare danni fisici, materiali o non materiali. Ai sensi del considerando 85 GDPR, tra i danni che possono esserci sono compresi:

- Perdita di controllo sui propri dati personali;
- Limitazione dei propri diritti;
- Discriminazione;
- Furto di identità o frode;
- Perdita finanziaria;
- Inversione non autorizzata di pseudonimizzazione;
- Danni alla reputazione;
- Perdita di riservatezza dei dati personali protetti dal segreto professionale;
- Qualunque svantaggio economico o sociale significativo a quegli interessati.

Uno degli obblighi più importanti del Titolare è quello di valutare i rischi che possono esservi per i diritti e le libertà degli interessati, attuando misure tecniche e organizzative adeguate ad affrontarli. Di conseguenza, il GDPR (ai sensi degli artt. 33 e 34) richiede al Titolare di:

- Documentare eventuali violazioni dei dati personali, compresi i fatti relativi alle violazioni, gli effetti causati e le azioni collettive intraprese;
- Notificare la violazione dei dati personali all'autorità di controllo, a meno che non sia improbabile che la violazione dei dati comporti un rischio per i diritti e le libertà delle persone fisiche;
- Comunicare la violazione dei dati personali all'interessato nel caso in cui la violazione comporti un rischio elevato per i diritti e le libertà delle persone fisiche.

I data breach rappresentano un sintomo di un regime di sicurezza dei dati vulnerabile o comunque obsoleto.

Notifica

L’obbligo di notifica e l’obbligo di comunicazione devono essere valutati caso per caso, in base ai diritti e alle libertà degli interessati.

La notifica di una violazione dei dati personali è disciplinata dall’art. 33 GDPR, che al par. 1 prevede: *“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.”*

Non esiste dunque un obbligo di notifica in presenza di una violazione: la notifica vi è nel solo caso in cui la violazione comporta un rischio per i diritti e le libertà delle persone fisiche.



Se il rischio è particolarmente elevato, il Titolare è tenuto anche a dare comunicazione all'interessato.

La notifica ha il pregio di attenuare i danni che possono derivare da una violazione, in dipendenza della tempestività e dell'adeguatezza con cui questa è affrontata. I Titolari possono non essere in possesso di tutte le informazioni relative alla violazione nelle 72 ore successive al suo verificarsi. Tuttavia, il WP29 ha chiarito che i Titolari hanno la possibilità di fare più comunicazioni in momenti successivi all'Autorità Garante, spiegando i motivi del ritardo. L' Autorità Garante terrà in debito conto anche la capacità di individuare tempestivamente l'esistenza di un incidente e i criteri di valutazione attinenti all'obbligatorietà di una notifica.

Ma quali sono le informazioni da fornire all'Autorità di vigilanza?

L'art. 33 par. 3 del GDPR stabilisce che la notifica di cui al paragrafo 1 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 WP29 sottolinea che il Titolare del trattamento dovrà documentare tutte le violazioni che si sono verificate, al fine di dimostrare la conformità al GDPR del trattamento effettuato. L'art. 33 par. 5 del GDPR prevede infatti che il Titolare deve registrare i dettagli riguardanti la violazione, le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Il GDPR non specifica un periodo di conservazione per tale documentazione.

Se queste registrazioni contengono dati personali, spetterà al Titolare determinare il periodo appropriato di conservazione, conformemente ai principi relativi al trattamento dei dati personali.

Comunicazione all'interessato

Nel momento in cui la violazione dei dati presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve comunicare la violazione ai soggetti interessati i cui dati sono stati violati. Questo adempimento è previsto dall'art. 34 GDPR, il cui paragrafo 1 prevede: *"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".*

Tale comunicazione è obbligatoria, salvo che non sia improbabile che vi sia un rischio per i diritti e le libertà delle persone a seguito di una violazione. Nel caso in cui vi sia un rischio elevato per i diritti e le libertà degli individui come risultato di una violazione, occorre informare anche gli interessati.

La comunicazione di una violazione agli individui dovrebbe essere fatta senza ingiustificato ritardo, ovvero il più presto possibile. L'obiettivo della comunicazione è quello di fornire specifiche informazioni sui passi da adottare per proteggere sé stessi, con l'obiettivo di diminuire i rischi e i danni. Infatti, in alcuni casi, una comunicazione tempestiva aiuterà le persone a prendere le misure per proteggersi da eventuali conseguenze negative della violazione.



La comunicazione agli interessati deve avere un linguaggio semplice e chiaro, e deve contenere le seguenti informazioni:

- Una descrizione della natura della violazione;
- Il nome e le informazioni di contatto del responsabile della protezione dei dati o di altri punti di contatto;
- Una descrizione delle probabili conseguenze della violazione;
- Una descrizione delle misure adottate o proposte dal controllore per affrontare la violazione, comprese, se del caso, misure atte a mitigarne gli eventuali effetti nocivi.

Il Titolare del trattamento deve fornire consigli specifici agli interessati per proteggersi da eventuali conseguenze negative della violazione, ad esempio reimpostando la password nel caso in cui le credenziali di accesso siano state compromesse.

La violazione deve essere comunicata direttamente ai soggetti

interessati, salvo il caso in cui questo comporti uno sforzo sproporzionato. In questo caso, sarà possibile procedere a una comunicazione pubblica oppure con una misura analoga, attraverso cui le persone interessate vengono informate in modo efficace (art. 34 par. 3, lett. C).

L'art. 34 par. 3 stabilisce tre condizioni che, se soddisfatte, non richiedono comunicazione agli interessati in caso di violazione. Queste condizioni sono:

"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."

La responsabilità di dimostrare l'omessa o tardiva comunicazione all'Autorità di vigilanza spetta ai Titolari. Se un Titolare decide di non comunicare una violazione all'interessato. L'art. 34 par. 4 GDPR, prevede che l'Autorità di vigilanza possa comunque richiederla, se ritiene che la violazione dei dati possa provocare un rischio elevato.

Gestione Data breach

Per prevenire e gestire episodi di violazione di dati personali è necessario adottare una serie di misure, quali:

- Adottare un protocollo di risposta: il protocollo di risposta consiste in una serie di procedure atte a gestire e risolvere eventuali casi di violazione dei dati personali.
- Effettuare test periodici per controllare la validità del protocollo: tali test sono fondamentali per comprendere se le procedure adottate per prevenire e gestire i casi di data breach siano efficienti e funzionanti. È altresì importante ottenere una copertura assicurativa per eventuali casi di data breach, ottenendo così un indennizzo in presenza di eventuali violazioni di dati.
- Tenere un registro dei casi di data breach: il DPO deve promuovere la tenuta di un registro dei casi di data breach, per identificare il tipo e la natura dei casi più ricorrenti.
- Compiere attività di indagine per individuare la natura la portata della violazione: tali attività possono essere estremamente utili per individuare e controllare i fattori di rischio, misurare l'efficacia delle policy adottate e per elaborare un piano di conformità per essere compliant rispetto alla normativa in vigore.

Avv. Anna Minichiello

Dott. Niccolò Morandi

Hanno parlato di noi

CORRIERE DELLA SERA

la Repubblica

Il Sole 24 ORE

il Giornale

ItaliaOggi

Libero Quotidiano.it

fanpage.it

PANORAMA

TGCOM24

TG5

Rai News 24

Rai 1

Rai 2

Rai 3



CORRIERE DELLA SERA

la Repubblica

Il Sole 24 ORE

il Giornale

ItaliaOggi



fanpage.it

PANORAMA













Contattaci

- Orari

Lunedì – Venerdì: 9.00 – 13.00 / 14.30 – 19.00

Lunedì – Venerdì:
9.00 – 13.00 / 14.30 – 19.00

- Email

info@alassistenzalegale.it

- Telefono

+39 02 5450823

Chiamaci
Contattaci
□
□
□
□
☐ Ho letto e accetto i termini dell'Informativa sulla Privacy
Invia