Data breach e GDPR: gestire la crisi con procedure corrette

LA GUIDA COMPLETA

Diego Padovan
Data Protection Officer, Amministratore DPO Compliance Consulting

Tra i nuovi adempimenti in materia di protezione dei dati personali introdotti dal GDPR, c'è quello relativo al data breach. Ecco come procedere all'analisi dei rischi per reagire correttamente ad una eventuale emergenza.

Al fine di ottemperare ai nuovi adempimenti in materia di violazione dei dati personali (il c.d. data breach), introdotti dal nuovo Regolamento (UE) 2016/679, in particolare con gli Articoli 33 e 34 del GDPR, ogni azienda è chiamata, nell'ambito della gestione delle proprie attività e processi organizzativi, ad incorporare un ulteriore modello di analisi dei rischi, quello relativo al data breach.

GDPR, analisi data breach, notifica violazione dati personali al garante privacy

Il Modello di analisi del data breach è essenziale per poter valutare la necessità o meno di notificare la violazione dei dati personali al Garante e agli interessati qualora il rischio per gli stessi risulti elevato, al fine di consentirne la mitigazione attraverso l'adozione di precauzioni e rimedi, ma non rappresenta l'unico elemento da tenere in considerazione per una risposta efficace in caso di violazione dei dati personali.

In quest'ottica, la risposta all'evento di data breach è da considerarsi come un vero e proprio processo aziendale, con referenti specifici, fasi ben delineate, metodologie di analisi testate e output chiari, che consistono non solo nel decidere in 72 ore "se notificare", ma anche quali sono le misure di mitigazione da porre in essere, per l'azienda e per l'interessato, al fine di ridurre il rischio e le conseguenze del breach a cui i dati personali sono stati esposti.

Vale la pena ricordare che non è possibile eliminare il rischio, ma con un approccio metodologico e organizzativo strutturato è possibile ridurre la probabilità legata ad esso e mitigarne le conseguenze.

Un processo di data breach ben strutturato prevede 4 fasi:

1) Preparazione.
2) Reazione.
3) Comunicazione.
4) Registro.

Prima del data breach: analizzare il livello di rischio

È la fase temporale di maggior importanza, infatti se ben affrontata consente di reagire e mitigare le conseguenze del data breach con la massima efficienza.

Analizzare il livello di rischio a cui l'Azienda (o Ente) è esposta in termini di dati personali gestiti, comporta non scordare mai cosa è possibile fare prima che il processo sia eventualmente messo alla prova. Investire in prevenzione significa ridurre il rischio di costi esorbitanti conseguenti i danni prodotti dalla violazione subita in azienda e per far ciò è necessario tenere a mente che un processo di data breach deve essere preceduto da un'analisi delle vulnerabilità del proprio sistema IT, unico modo per capire dove l'azienda può incorrere

con maggiore rischio nei data breach. Si tratta nella pratica di simulare un attacco da parte di un hacker e lavorare sui piani di remediation con questi concordati.

Inoltre, è necessario costituire un "comitato per il data breach", che deve poter contare almeno sulle seguenti competenze: GDPR, IT, Marketing e Comunicazione, Finance, Responsabili del Trattamento (se coinvolti). In effetti, si tratta proprio di competenze poiché, considerando la composizione delle PMI italiane, spesso queste possono coincidere in pochissimi soggetti. Un Comitato efficace deve dunque poter contare su un approccio trasversale, che coinvolga l'azienda nelle sue diverse funzioni, ed avere compiti e responsabilità ben precisi, ma per poter essere esaustivi, questo punto merita un approfondimento a parte.

Il processo per la valutazione del data breach

È necessario quindi costituire un processo per la valutazione del data breach, tenendo presente le tre macro-categorie di data breach delineate dal WP29:

"Confidentiality Breach", in caso di accesso accidentale/abusivo ai dati personali;

"Availibility Breach", se vi è una perdita/distruzione accidentale o non autorizzata di dati personali;

"Integrity Breach", se siamo in presenza di alterazioni accidentali o non autorizzate dei dati personali.

Il processo dovrà permettere una valutazione del rischio effettivo a cui sono esposti i dati personali, e quindi degli impatti nel caso si verificasse una particolare violazione, calcolato in base alle misure di sicurezza adottate sui sistemi, tipologia dei dati trattati ed il livello di identificabilità della clientela. Tramite questi risultati potranno essere definite le priorità di interventi di comunicazione e mitigazione.

Riassumendo, per il processo di valutazione del data breach sarà necessario:

- Identificare e definire una scala di valori di criticità associata alle differenti tipologie di dati personali trattati dai sistemi e dalle infrastrutture informatiche aziendali.
- Identificare i punti di vulnerabilità a cui gli stessi potrebbero essere esposti.
- Valutare rischio e impatti in caso di occorrenza del data breach, considerando lo stato delle misure e delle soluzioni di sicurezza in essere.
- Stabilire una soglia di accettazione del rischio.
- Stabilire le contromisure in funzione delle tipologie di data breach, della soglia di rischio e delle risorse, in senso lato, necessarie per investire nelle contromisure stesse, infatti è importante tenere sempre presente che l'Art.34, comma 3 del GDPR, alla lettera b) prevede che non è richiesta la comunicazione all'interessato se 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;

Formazione in azienda e comitato data breach

Inoltre, affinché il processo non si riduca ad un formalismo sterile presente nella documentazione aziendale, è necessario creare all'interno dell'azienda un livello di formazione e consapevolezza adeguati tra le persone autorizzate al trattamento e prevedere un processo di segnalazione specifico al Comitato data breach da parte dei dipendenti e dei processors.

La formazione è gestibile attraverso corsi ed aggiornamenti periodici, policy sul trattamento dei dati personali adeguati, nonché sulle modalità di utilizzo della strumentazione informatica.

La consapevolezza invece è raggiungibile attraverso un forte commitment dei vertici aziendali nelle attività di trattamento e quindi nella volontà da parte di chi gestisce l'Azienda di far permeare nei processi aziendali i principi di privacy-by-default e privacy-by-design promossi dal GDPR.

Infine, ma non di minore importanza, è necessario stabilire i ruoli e le responsabilità dei processor cui si avvale il titolare del trattamento, affinché nelle clausole contrattuali o nelle relative nomine, siano presenti delle garanzie a supporto dell'attività di detection e reazione al data breach; altrimenti, in assenza di un'adeguata collaborazione tra processor e controller, tutto il processo è semplicemente inutilizzabile e la reazione al breach inattuabile.

Reagire correttamente ad un data breach (in 72 ore!)

Reagire al data breach significa avere consapevolezza che la violazione sia occorsa. L'avvio del conto alla rovescia delle 72 ore parte infatti dal momento in cui l'azienda sia venuta a conoscenza della violazione dei dati personali, pertanto la base sottostante questa fase è il rapporto e la comunicazione tra controller e processor, tra controller e persone autorizzate al trattamento o, auspicabilmente in misura ridotta, poiché può implicare negligenza nella fase di "controllo", tra controller ed interessati.

Nel primo caso, come detto nel paragrafo precedente, è essenziale che siano chiari i ruoli, le responsabilità e le modalità di comunicazione, possibilmente attraverso clausole contrattuali specifiche. Nel secondo caso è essenziale la consapevolezza Aziendale in tema privacy, ossia che i principi di privacy-by-default e privacy-by design siano permeati all'interno di ogni processo Aziendale e che le persone autorizzate al trattamento siano state adeguatamente formate al fine di eseguire tempestivamente le indicazioni per la segnalazione al comitato data breach. Infine, è necessario che attraverso un'adeguata informativa, gli interessati al trattamento siano in grado di trovare, in modo facile e intuitivo, i contatti del titolare, o del DPO se presente, al fine di segnalare l'evento anomalo.

Ad avvenuta segnalazione, il comitato eseguirà in collaborazione e coordinato dal DPO se presente, la procedura di valutazione del data breach e ne analizzerà i risultati, in funzione del rischio e delle possibilità di mitigazione e rimedi perseguibili dall'azienda o dagli interessati. In particolare, dovrà prontamente porre in essere le misure di mitigazione dei rischi già previste in fase di preparazione all'evento del data breach, in quanto in sua assenza, l'eventuale valutazione da parte dell'Autorità sarà sicuramente meno indulgente e la sanzione eventualmente imposta più elevata. Quest'ultimo aspetto però non deve essere ciò che spinge l'azienda nell'adozione di un corretto modello di valutazione del data breach, bensì lo sono le conseguenze derivanti la perdita dei dati, che costituiscono un asset strategico per l'azienda. Infatti, la loro perdita determina, in termini di danni reputazionali, un costo elevatissimo, soprattutto in caso di esposizione al web, evenienza che può portare un'azienda a dover terminare la propria attività o nei casi più "felici" a cambiare brand.

Come comunicare il data breach in modo corretto (spiegato dal GDPR)

La terza fase del data breach consiste nella necessità di gestire il delicato processo di comunicazione della violazione. Difatti, come spiega il GDPR, se la probabilità del rischio per gli interessati è elevata, si dovrà informare delle violazioni anche gli interessati senza ingiustificato ritardo. Fanno eccezione le circostanze indicate al paragrafo 3 dell´art. 34, in via generale i contenuti della notifica alla Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del regolamento ed approfonditi nelle linee-guida in materia di notifica delle violazioni di dati personali del Gruppo "Articolo 29".

Tale fase risulta delicata poiché implica il rischio di inidonea comunicazione al Garante o agli interessati. Nel primo caso, potrebbe accadere la necessità di approfondimenti successivi o di rettifica, nel secondo caso potrebbe comportare una perdita della brand reputation.

Ridurre tali rischi è possibile, agendo preliminarmente (vedi fase Prima del data breach) con una procedura interna di comunicazione al Comitato (nel caso presente al DPO) e impostando correttamente il rapporto Controller-Processor. In questo modo il flusso di informazioni verso il Garante e verso gli Interessati per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi sarà più efficiente e le informazioni correttamente circostanziate, per descrivere le probabili conseguenze della violazione dei dati personali, le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento o che si invita a intraprendere da parte degli interessati.

Vale la pena approfondire brevemente la gestione della comunicazione agli interessati. Questa infatti si configura come vera e propria comunicazione c.d. di crisi. Nessuna organizzazione (o istituzione) può ritenersi al riparo di un data breach, e quindi dall'evento di crisi, non può astenersi dalla necessità di gestirlo sotto il profilo comunicativo, poiché se l'opinione pubblica viene a conoscenza di un fatto che ritiene inaccettabile, quale può essere la perdita del controllo sui propri dati personali, ciò mette in discussione la fiducia nei confronti dell'organizzazione stessa e ne minaccia la sopravvivenza.

Affrontare un evento di crisi come il data breach, pertanto, comporta la valutazione da parte di professionalità interne o esterne all'Azienda (o Ente) specializzate nei processi comunicativi di crisi, ma ciò, come descritto nella prima fase, deve avvenire preliminarmente alla violazione dei Dati, in modo di poter essere pronti alle fatidiche 72 ore.

Registro delle violazioni: come concludere il processo di data breach

Il processo di data breach si conclude con la tenuta del Registro delle violazioni.

L'Art. 33, paragrafo 5 del Regolamento prescrive che tutti i Titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate alla Autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

Come è possibile intuire, le misure adottate nelle fasi precedenti sono di estremo aiuto in tale adempimento. Basterà prevedere una procedura per il recepimento delle informazioni necessarie a documentare eventuali violazioni e poter così rispondere e fornire tale documentazione, su richiesta, al Garante in caso di accertamenti. Tale procedura potrà essere correttamente impostata durante la prima fase, prevedendo specificatamente, tra le responsabilità del Comitato, del DPO laddove nominato, e dei Controller anche la compilazione e la tenuta del registro stesso.