STUDIO LEGALE PISCINI
Avv. Laura Piscini

Premessa: Il fattore umano nella cyber-security

Sicurezza dei sistemi informatici

Nel 2018, gli attacchi informatici che hanno avuto come obiettivo aziende e imprese nel mondo hanno causato danni per oltre 500 miliardi di dollari. La sicurezza dei sistemi informatici, in questo scenario, è diventata una priorità per tutti. Programmi antivirus e sistemi di controllo della rete sono indispensabili, ma non bastano a proteggere i dati e i sistemi di aziende e uffici. Secondo gli esperti, il 95% degli attacchi informatici sfruttano il fattore umano. Un semplice errore, o la mancata applicazione delle buone pratiche indispensabili per garantire la sicurezza dei sistemi, sono sufficienti per aprire la strada a un attacco che può costare caro.

Cos'è il Data Breach

Il 30 luglio di quest'anno il Garante per la protezione dei dati ha emanato un provvedimento che chiarisce in che modalità e con quali strumenti deve essere notificata una violazione dei dati personali. La violazione in materia di trattamento dei dati personali viene chiamata "Data Breach" e il provvedimento del Garante appena citato, il n. 157, ha lo scopo di riorganizzarne e snellirne la procedura di segnalazione.

Cosa si intende per violazione dei dati personali

Quando si verificano la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali dell'interessato o degli interessati – che siano trasmessi, conservati o semplicemente trattati – siamo in presenza di una violazione dei dati personali.

Un avvenimento insidioso che può compromettere la riservatezza, l'integrità o la disponibilità dei dati.

La violazione può avvenire sia in modo illecito, sia in maniera accidentale: il data breach, perciò, non è soltanto un evento doloso ma, spesso, può essere il risultato di una disattenzione, una leggerezza o una mancata applicazione delle norme di sicurezza idonee. Facciamo qualche esempio. C'è violazione quando:

- un soggetto terzo (che non è l'interessato, il titolare o il responsabile) accede o acquisisce i dati senza averne avuto l'autorizzazione
- un dispositivo, ad esempio un computer o un hard disk, viene rubato o perso
- un malware, un virus o un attacco hacker rendono indisponibili i dati conservati

Come bisogna comportarsi in caso di violazione

Una volta accertata la violazione dei dati personali, il titolare del trattamento (sia esso un soggetto pubblico, un'azienda, un'associazione, un professionista, un partito politico) è tenuto a notificare velocemente l'accaduto al Garante, cioè entro 72 ore dal momento in cui ne è venuto a conoscenza. Quando a venire a conoscenza della violazione è il responsabile del trattamento, questi deve tempestivamente comunicarlo al titolare, così che possa a sua volta segnalarlo al Garante.

La segnalazione al Garante può essere tralasciata solo nel caso in cui sia improbabile che tale violazione comporti un rischio per i diritti e le libertà delle persone fisiche. In caso contrario, se cioè la violazione comporta un rischio elevato per i diritti degli interessati e non sono state già prese adeguate misure che ne riducano l'impatto, il titolare deve comunicarla anche a loro, utilizzando i canali più idonei. Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

Non solo, il titolare del trattamento deve documentare tutte le violazioni dei dati personali di cui è a conoscenza, così che le Autorità, in caso di controlli, possano effettuare le verifiche necessarie sul rispetto della normativa.

Che elementi deve contenere la notifica al Garante

Attraverso un modello allegato al provvedimento, il Garante indica ed individua le informazioni da fornire nella notifica del Data Breach.

L'obiettivo è quello di semplificare il lavoro del titolare e favorire, da parte sua, il corretto adempimento degli obblighi in materia di trattamento dei dati personali.

Il documento di notifica deve essere il più possibile completo e le informazioni fornite devono essere riassunte per sezioni. Anche se il quadro informativo fosse incompleto, la notifica va comunque mandata, con riserva di inviare una seconda notifica ad integrazione della prima. Ecco, qui di seguito, come deve essere costruita la suddivisione in sezioni e cosa devono contenere:

Sez. A – la notifica

- tipologia della notifica
- dati del soggetto che effettua la notifica

Sez. B – il titolare del trattamento

– dati del Titolare del trattamento

– dati di contatto per informazioni relative alla violazione

– dati di ulteriori soggetti coinvolti nel trattamento

Sez. C – informazioni di sintesi sulla violazione

- quando è avvenuta la violazione

– momento in cui il titolare del trattamento è venuto a conoscenza della violazione

- modalità con la quale il titolare del trattamento è venuto a conoscenza della violazione
- in caso di notifica oltre le 72 ore, quali sono i motivi del ritardo
- breve descrizione della violazione
- natura della violazione
- causa della violazione
- categorie di dati personali oggetto di violazione
- volume (anche approssimativo) dei dati personali oggetto di violazione
- categorie di interessati coinvolti nella violazione
- numero (anche approssimativo) di interessati coinvolti nella violazione

Sez. D – informazioni di dettaglio sulla violazione

- descrizione dell'incidente di sicurezza alla base della violazione
- descrizione delle categorie di dati personali oggetto della violazione
- descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione
- misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti

Sez. E – possibili conseguenze e gravità della violazione

- possibili conseguenze della violazione sugli interessati, in caso di perdita di confidenzialità, in caso di perdita di integrità, in caso di perdita di disponibilità
- ulteriori considerazioni sulle possibili conseguenze
- potenziali effetti negativi per gli interessati
- stima della gravità della violazione indicandone le motivazioni

Sez. F – misure adottate a seguito della violazione

– misure tecniche e organizzative adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati

– misure tecniche e organizzative adottate (o di cui si propone l'adozione) per

prevenire simili violazioni future

Sez. G – comunicazione agli interessati

- la violazione è stata comunicata agli interessati?
- numero di interessati a cui è stata comunicata la violazione
- contenuto della comunicazione agli interessati
- canale utilizzato per la comunicazione agli interessati

Sez. H: altre eventuali informazioni

- la violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo ? Se sì indicare quali
- la violazione coinvolge interessati di Paesi non appartenenti allo Spazio

Economico Europeo? Se si indicare quali

- la violazione è stata notificata ad altre autorità di controllo? Se si indicare quali
- la violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative? Se sì indicare quali
- è stata effettuata una segnalazione all'autorità giudiziaria o di polizia?

In che modalità va inviata la notifica al Garante

Il provvedimento, sempre per rendere chiara la procedura di invio della notifica, spiega esattamente come fare: la notifica va infatti inviata al Garante tramite posta elettronica all'indirizzo protocollo@pec.gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata o firma digitale) ovvero con firma autografa. In questo caso, la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario. L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "Notifica violazione dati personali" e, se possibile, la denominazione del titolare del trattamento.

Queste indicazioni, superando ogni precedente dubbio interpretativo, rendono uniforme ciò che prima era differenziato settore per settore, valgono e sono uguali per tutti.

STUDIO LEGALE PISCINI
Avv. Laura Piscini

Quali sono le sanzioni in cui si incorre

Il Garante può prescrivere misure correttive nel caso rilevi una violazione delle disposizioni del GDPR, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare fino a 10 milioni di Euro o, nel caso di imprese, fino al 2% del fatturato totale annuo mondiale.