GDPR: GLI ADEMPIMENTI DEL TITOLARE DEL TRATTAMENTO IN CASO DI ACCERTATA VIOLAZIONE DI DATI PERSONALI

Avv. Francesca Pescatore

Sono ormai note le notizie dei recenti attacchi hacker dello scorso ottobre nei confronti della Siae e della San Carlo, aggredite da un virus *ransomware* di tipo *cryptolocker*, in seguito ai quali sono stati sottratti innumerevoli gigabyte di dati, anche sensibili, poi pubblicati e venduti sul *dark web*.

Il predetto virus, che è solo uno dei tanti in circolazione, non solo ha sottratto i dati ma ha, altresì, inficiato l'accesso dei dispositivi, rendendo inaccessibili i documenti e i fili ivi salvati, con lo scopo di richiedere un riscatto volto a rimuoverne la limitazione.

Sull'onda di quanto accaduto alle malcapitate Siae e San Carlo, partendo dal Regolamento UE 679/2016 (di seguito "GDPR"), facciamo il punto sulle misure, in ambito giuridico, che il Titolare del trattamento deve adottare in caso di accertata violazione della *privacy* aziendale.

Come si accerta un *data breach*?

Perché si possa effettivamente parlare di *data breach*, la violazione di sicurezza deve presentare effetti avversi significativi sui soggetti coinvolti, comportando, in particolare, concreti rischi per i loro diritti e libertà.

Deve, dunque, esservi una violazione di tutte quelle informazioni che identificano o rendono identificabile -direttamente o indirettamente – una persona fisica, e che possano fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stato di salute, la sua situazione economica, ben ricomprendendo anche i dati sensibili, quali, ad esempio quelli inerenti l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, l'appartenenza sindacale, i dati genetici o i dati relativi alla vita sessuale o all'orientamento sessuale.

Per verificare con maggior certezza se la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Garante della Privacy ha stilato delle linee guida, comprensive di esempi.

La suddetta violazione dei dati, accidentale o illecita che sia, deve quindi essere accertata dal Titolare del trattamento. Quest'ultimo, nel verificare l'effettiva violazione, deve prestare particolare attenzione ai tre effetti collaterali che possono svilupparsi:

– violazione della riservatezza dei dati, in caso di divulgazione dei dati o accesso agli stessi non autorizzati o accidentali;

– violazione dell'integrità dei dati, in caso di modifica non autorizzata o accidentale dei dati;

– la perdita della disponibilità dei dati, in caso di perdita o distruzione non autorizzate o accidentali di dati

Il Garante della Privacy ha altresì messo a disposizione una procedura di *self assessment* che permette di effettuare un'autovalutazione tesa ad individuare le azioni e i provvedimenti correttivi da adottare per porre rimedio alla violazione dei dati.

Cosa deve fare il Titolare del trattamento in caso accertata violazione?

Accertata la violazione, così come previsto dall'art 33 GDPR, il Titolare del trattamento, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve effettuare una segnalazione tramite un'apposita procedura telematica, resa disponibile, a far data dal 1° luglio 2021, nel portale dei servizi online dell'Autorità.

Il Garante ha chiarito che il Titolare del trattamento si può ritenersi a conoscenza della violazione solo nel momento in cui è ragionevolmente certo che si sia verificato un incidente di sicurezza che ha comportato la compromissione di dati personali.

Nel caso in cui sia stato designato un Responsabile del trattamento, questo deve, senza ingiustificato ritardo, comunicare la violazione al Titolare del trattamento, il quale dovrà poi procedere come anzi descritto.

La notifica della violazione al Garante

La notifica della violazione deve:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati 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, eventualmente, per attenuarne i possibili effetti negativi.

Nel caso in cui il Titolare non disponesse di tutte le informazioni necessarie, dovrà comunque effettuare la notifica, specificando che si tratta di una notifica preliminare, impegnandosi a comunicare le informazioni mancanti non appena disponibili.

La notifica della violazione agli interessati coinvolti

Se, poi, la violazione rappresenta un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte, anch'esse dovranno essere avvisate ex art 34 GDPR, senza ingiustificato ritardo.

Il rischio elevato deve essere valutato sulla base di diversi elementi, quali:

a) tipo di *data breach*;

b) natura, numero e grado di sensibilità dei dati personali violati;

c) facilità di associazione dei dati violati ad una persona fisica;

d) gravità delle conseguenze per gli interessati;

e) numero di interessi esposti al rischio;

f) caratteristiche del titolare del trattamento.

In tal caso, la comunicazione agli interessati non deve essere generica, ma dovrà contenere tutte le informazioni per consentire loro di comprendere il rischio, tra cui: (i) una descrizione della natura della violazione delle sue possibili conseguenze, nonché (ii) precise indicazioni sugli accorgimenti da adottare per proteggersi da usi illeciti dei dati e per evitare ulteriori rischi.

La documentazione della violazione

Il GDPR prevede poi un ulteriore obbligo per il Titolare, che dovrà documentare le violazioni subite, implementando su un apposito registro le seguenti voci:

a) data e luogo violazione;

b) conseguenze della violazione;

c) data e ora della notifica all'autorità Garante;

d) cause della violazione;

e) provvedimenti correttivi adottati.