PROCEDURA DEL DATA BREACH o VIOLAZIONE DEI DATI PERSONALI

COSA É UN *DATA BREACH*?

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.

Per **violazione dei dati personali (***data breach*) si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati dal titolare del trattamento o dai responsabili o dagli incaricati/autorizzati.

Un *data breach* non è solo un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto di un notebook di un dipendente), siano essi dati cartacei o informatici.

COSA FARE QUANDO ABBIAMO UN *DATA BREACH*

Le azioni da intraprendere sono 3:

a) Rendicontazione (adempimento obbligatorio)

b) Notificazione al Garante (adempimento eventuale – Da Valutare caso per caso)

c) Comunicazione al soggetto o ai soggetti interessati (adempimento eventuale – Da valutare caso per caso)

A) Rendicontazione *Data Breach*

In ossequio al principio dell'accountability, il titolare dovrà rendicontare (immediatamente o il prima possibile) ogni forma di *data breach* ma anche ogni tentativo di *data breach* verificatesi nella propria struttura, con il supporto del Responsabile IT e dei Referenti.

In particolare il titolare deve documentare qualsiasi violazione dei dati personali comprese:

- le circostanze a essa relative

- le sue conseguenze

- i provvedimenti adottati per porvi rimedio

Tale rendicontazione *"Data Breach Accountability"* resterà a disposizione del DPO (se esistente) e dell'Autorità di controllo.

B) Notificazione

In caso di violazione dei dati personali, il titolare del trattamento notifica (con il Modello Allegato) la violazione all'autorità di controllo competente 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.

Quando si notifica?

Quando non sia "improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche". Ciò significa che il titolare dovrà valutare, caso per caso, se, dalla violazione dei dati, ci sia un effettivo rischio per i diritti delle persone fisiche. Tale scelta di notificare o di non procedere alla notifica dovrà essere oggetto di rendicontazione.

Cosa si notifica?

La notifica 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.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Come di notifica?

Utilizziamo il Modello Allegato che andrà inviato al Garante Privacy.

C) Comunicazione di una violazione dei dati personali all'interessato

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 comunicazione all'interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le seguenti informazioni misure:

- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

- descrizione delle probabili conseguenze della violazione dei dati personali;

- descrizione delle 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.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

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

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.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda.

Modalità di comunicazione all'interessato in caso di data breach

Per la comunicazione all'interessato sono state previste le seguenti modalità:

a) Notificazione personale all'interessato a mezzo PEC o raccomandata a/r;

b) In caso di un numero di interessati eccessivamente numeroso, si potrà procedere ad una pubblicazione della Comunicazione a mezzo internet o a mezzo stampa.

Colle di Val d'Elsa (SI), xx/xx/xxxx

Il Titolare del trattamento