DATA BREACH

COMUNE DI EMPOLI - PROCEDURA PER LA GESTIONE DEGLI EVENTI IN VIOLAZIONE DEI DATI PERSONALI AI SENSI DEGLI ARTT. 33 E SS. DEL REG. ue 679/2016

Premessa

Il ***Data Breach***, ai sensi degli artt. 33 e 34 del Reg. UE 679/2016, è la violazione dei dati personali dell'interessato persona fisica, che può consistere, a titolo esemplificativo e non esaustivo in:

- perdita del controllo dei dati personali che riguardano gli interessati o limitazione dei loro diritti;
- discriminazione, furto o usurpazione d'identità;
- perdite finanziarie, decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale;
- qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Le tipologie di violazione dei dati personali

In linea con la definizione di violazione di dati personali, ex art. 4 p.12 Reg. UE, si distinguono 3 (tre) tipi di violazione, che possono, tuttavia, combinarsi tra loro e che possono compromettere la riservatezza, l'integrità o la disponibilità dei dati:

1) **violazione di riservatezza**, quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.

2) **Violazione di integrità**, quando si verifica un'alterazione di dati personali non autorizzata o accidentale.

3) **Violazione di disponibilità**, quando si verifica perdita, inaccessibilità, o distruzione, accidentali o non autorizzate, di dati personali.

Procedura per la gestione degli eventi

1. Scoperta

1a - L'incaricato al trattamento ravvisa un incidente nella gestione dei dati che astrattamente può determinare un *data breach* ai sensi del regolamento **oppure**

1b - un responsabile "esterno" segnala un evento che astrattamente po' determinare un *data breach*

1c - un interessati segnala un evento che astrattamente po' determinare un *data breach*

2. Avviso

Viene subito informato il Responsabile del Trattamento (Dirigente) che deve avvisare il Titolare (o in sua assenza una persona appositamente designata). Il Responsabile e il Titolare di concerto con

l'amministratore di sistema, nel caso il *data breach* si riferisca al trattamento dati effettuato con strumenti informatici, procedono alla valutazione d'impatto dell'incidente in relazione ai diritti degli interessati.
Il DPO deve essere informato e messo nella condizioni di partecipare

3. Convocazione del "comitato di crisi"

Il Titolare e il Responsabile del trattamento convocano il "comitato di crisi" di cui fanno parte:
i) il DPO;
ii) il responsabile delle risorse umane;
iii) l'amministratore di sistema o il responsabile ITC;
iv) il responsabile della comunicazione;
v) eventuali altri soggetto coinvolti (responsabile esterno etc.)
Il "comitato" verifica l'eventuale sussistenza del rischio per gli interessati.

4. L'esito della verifica

a) se il ***data breach*** non risulta presentare alcun rischio per gli interessati, non si provvede ad alcuna notifica né all'autorità di controllo né agli interessati.
Si procede comunque ad annotare nell'apposito registro l'incidente.
b) Se il ***data breach*** risulta presentare rischi per gli interessati si cerca di stimare la gravità del rischio per procedere alla notifica al Garante mediante il modulo apposito.

5. La notifica al Garante

L'art. 33 del Regolamento UE prescrive che il Titolare, non appena viene a conoscenza di un'avvenuta violazione dei dati personali del trattamento, deve notificare la violazione al Garante della Privacy, **senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza** del *Data breach*.
Se non effettuata entro 72 ore, deve essere fornita una giustificazione per il ritardo
L**a notifica deve contenere**:
a) descrizione della 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) comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrizione delle probabili conseguenze della violazione dei dati personali;

d) 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.

Resta fermo che qualora non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Al fine di semplificare la procedura, l'autorità Garante ha predisposto un Pdf editabile da compilare, firmare digitalmente ed inviare per ottemperare all'obbligo di notifica, scaricabile al seguente indirizzo: www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915835.

Il Regolamento UE consente di non effettuare la notifica se risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Tale evenienza si verifica, per esempio, allorché siano state efficacemente attuate misure tecnologiche di cifratura o pseudonimizzazione che rendano improbabile ricostruire l'origine del dato, oppure quando il dato è inidoneo a rivelare alcunché di pregiudizievole o comunque riservato circa l'interessato.

La qualificazione della violazione del *Data breach* è rimessa sostanzialmente al Titolare, sulla base della valutazione tanto della qualità del dato, quanto dei sistemi tecnologici a presidio dello stesso.

6. La comunicazione all'interessato,

Oltre all'obbligo di notifica al Garante**, il** Regolamento UE prevede l'obbligo di comunicare, in un linguaggio semplice e chiaro, la violazione dei dati personali allo stesso interessato allorché tale violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La comunicazione all'interessato, in forma libera, deve obbligatoriamente contenere:

- indicazione del nome e dei 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 per attenuarne i possibili effetti negativi.