PROCEDURA DA APPLICARE IN CASO DI DATA BREACH
artt. 33 e 34 Regolamento UE 2016/679
Rev. 02/19

LISTA DELLE REVISIONI

REVISIONE N.	DATA	DESCRIZIONE DELLE MODIFICHE
00	25/5/2018	Prima emissione (in allegato al Registro dei trattamenti)
01	ottobre 2019	revisione del documento e degli allegati: registro delle violazioni; modello notifica al Garante

DEFINIZIONE DEL DATA BREACH
Per "Data Breach" si intende un evento in conseguenza del quale si verifica una "**violazione dei dati personal**i".

L'articolo 4 p.12 del GPDR definisce la "**violazione dei dati personali**" come una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

L'art. 33 del GDPR prevede che "in caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 55 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".

Le violazioni possono essere classificate in tre macro categorie che, a seconda dei casi, possono riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali (anche in combinazione).

1) "**violazione della riservatezza**" in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;

2) "**violazione dell'integrità del dato**" in caso di modifica non autorizzata o accidentale dei dati personali;

3) "**violazione della disponibilità del dato**", in caso di perdita o distruzione accidentali o non autorizzati di dati personali.

A seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

A seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'Autorità di controllo e la comunicazione alle persone fisiche coinvolte.

Il titolare del trattamento, riscontrata una violazione, dovrà pertanto di volta in volta valutare la probabilità e la gravità del conseguente impatto sui diritti e sulle libertà delle persone fisiche e:

a) documentare la violazione nel proprio Registro delle violazioni (sempre);
b) effettuare la notifica al Garante (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
c) comunicare la violazione ai soggetti interessati (laddove possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte).

SCOPO e CAMPO DI APPLICAZIONE
La presente procedura definisce le modalità di gestione del "data breach" che l'Ente, titolare del trattamento, è tenuto ad osservare e far rispettare ai propri preposti.

RESPONSABILITÀ
La responsabilità legata alla presente procedura è del titolare del trattamento.

RIFERIMENTI NORMATIVI
REGOLAMENTO (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di

tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205) e modifica il d.lgs. 196/03;
LINEE GUIDA IN MATERIA DI NOTIFICA DELLE VIOLAZIONI DI DATI PERSONALI (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679.

MODALITÀ' OPERATIVE E GESTIONE DELL'EVENTO
In caso di accertamento di violazione che rientra nella definizione di "data breach" il titolare del trattamento procede come di seguito dettagliato:

1. provvedere all'acquisizione e all'immediata gestione della notizia;
2. compiere un'analisi dell'evento;
3. adottare le misure di riduzione del danno;
4. valutare la gravità dell'evento;
5. notificare il "data breach" al Garante Privacy (laddove necessario);
7. procedere con la comunicazione agli interessati (se necessario);
8. inserire l'evento nel proprio Registro delle violazioni;
9. attivare tutte le azioni correttive per ridurre il ripetersi dell'evento.

Si descrivono di seguito le modalità operative per dare esecuzione a quanto sopra:

1) acquisizione e immediata gestione della notizia (da fonti interne o esterne)
La rilevazione/segnalazione di un data breach può essere di fonte interna o esterna all'Ente.

POSSONO ESSERE FONTI INTERNE: notizie ricevute da parte del personale dipendente; da parte del personale convenzionato/stagisti/tirocinanti; dall'amministratore di sistema (ove presente); dalle figure preposte alla manutenzione degli impianti informatici o alla gestione degli archivi; dagli utenti dei servizi.

SONO FONTI ESTERNE: notizie ricevute da parte delle forze dell'ordine; da parte dei responsabili del trattamento; da parte del DPO; da parte degli interessati; da parte di terzi.

La segnalazione, qualunque sia la forma, deve essere immediatamente messa a conoscenza del legale rappresentante dell'Ente, della Direzione, dell'amministratore di sistema (soggetti che compongono il "**gruppo di gestione del data breach aziendale**") attraverso canali di posta elettronica (pec) e avvertimento verbale/telefonico.

2) analisi dell'evento
Il gruppo di gestione del data breach aziendale è tenuto a compiere un'**analisi dell'evento** riscontrato e/o segnalato verificando che l'episodio rappresenti effettivamente un "data breach" mettendo in atto, laddove possibile, tutte le appropriate misure per l'immediato contenimento del danno.

L'attività di analisi riguarderà:
- una verifica della violazione (se di riservatezza, di integrità o di disponibilità);
- l'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
- l'identificazione degli interessati;
- il livello di gravità dell'evento;
- le misure di sicurezza presenti;
- le immediate azioni di riduzione delle conseguenze.

Tutte le operazioni effettuate devono essere verbalizzate e la rilevazione della violazione deve contenere almeno i seguenti elementi:

Breve descrizione della violazione dei dati personali	
Quando si è verificata la violazione dei dati personali	
Dove è avvenuta la violazione dei dati	
Dispositivo oggetto della violazione	
Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	

Quante persone sono state colpite dalla violazione dei dati personali	
Che tipo di dati sono oggetto di violazione	
Livello di gravità della violazione dei dati personali	
Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future	

Senza ingiustificato ritardo e non oltre 12 ore dall'evento il gruppo di gestione del data breach aziendale comunicherà l'episodio (segnalazione) e la risultanza della prima analisi al DPO mediante le coordinate di posta elettronica pec e avvertimento verbale/telefonico.

3) valutazione della gravità dell'evento
Il gruppo di gestione del data breach aziendale, con il supporto di tutte le risorse competenti, dovrà appurare se l'evento merita di essere notificato al Garante **considerando la probabilità o meno che l'evento possa comportare dei rischi per i diritti e la libertà delle persone.**

Nella fase di valutazione occorre stabilire se nell'incidente sono coinvolti i dati personali. In caso di risposta positiva occorre valutare l'impatto sugli interessati.

La notifica al Garante è necessaria laddove si sia verificata una violazione (distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati, sia che questi dati siano trattati all'interno che all'esterno dell'Ente) caratterizzata da effetti negativi significativi sulle persone fisiche, che possa causare danni fisici, materiali o immateriali (ad esempio la perdita del controllo da parte degli interessati sui loro dati personali), la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo alle persone fisiche interessate.

Nella valutazione si devono prendere in considerazione tanto la probabilità quanto la gravità del rischio per i diritti e le libertà degli interessati.

La ponderazione si basa sui seguenti criteri: natura, carattere sensibile e volume dei dati personali violati; facilità di identificazione delle persone fisiche coinvolte; gravità delle conseguenze per le persone fisiche interessate; caratteristiche particolari dell'interessato; caratteristiche particolari del titolare del trattamento; numero di persone fisiche interessate; aspetti generali della violazione.

Nel caso in cui sussista tale possibilità il titolare effettua la notifica al Garante nei termini prescritti (72 ore) mediante il modello di notifica in allegato alla presente procedura.

Quando la verifica dei fatti renda "improbabile" che la violazione subita comporti un rischio per i diritti e le libertà delle persone fisiche, la notifica non è obbligatoria ed il titolare deve riportare l'episodio occorso e l'attività di gestione dello stesso nel proprio Registro delle violazioni.

4) notifica della violazione al Garante
La notifica, effettuata dal Direttore o dallo stesso legale rappresentante verrà portata a compimento nei termini di legge mediante il Modello reso disponibile dal Garante (in allegato).

5) comunicazione agli interessati
In caso di **elevato rischio per la libertà e i diritti degli individui**, si provvederà ad informare gli interessati tramite i canali istituzionali dell'ente sul fatto avvenuto, sui dati violati e sulle procedure adottate o adottande per ridurre il rischio.

Il titolare del trattamento deve fornire agli interessati almeno le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;

- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

La comunicazione agli interessati non è richiesta laddove:

- il titolare del trattamento ha applicato misure tecniche e organizzative adeguate a proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;
- il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche, immediatamente dopo una violazione;
- contattare gli interessati richiederebbe uno sforzo sproporzionato.

Copia di ogni comunicazione agli interessati dovrà essere conservata nel Registro delle violazioni.

6) inserimento dell'evento nel Registro delle violazioni
Il titolare documenta qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.

Il gruppo di gestione del data breach aziendale è responsabile dell'inserimento di tutte le attività indicate sopra nel registro delle violazioni, che devono essere documentate, tacciabili, e in grado di fornire evidenza nelle sedi competenti.

ALLEGATI

- Registro delle violazioni
- Modello notifica del data breach al Garante