PROCEDURA GESTIONE DATA BREACH

1. Che cos'è il Data Breach

Il *data breach* consiste nella violazione dei dati personali gestiti da una organizzazione 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.

Il Regolamento UE sulla protezione dei dati personali, GDPR n. 2016/679, disciplina il *data breach* prevedendo espressamente un obbligo di notifica e comunicazione in capo al titolare del trattamento in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati, quali quelli relativi ai dati sensibili e giudiziari previsti dall'art. 9 del GDPR.

2. Rilevazione identificazione e classificazione degli eventi

La fase di rilevazione, identificazione e classificazione dell'evento è particolarmente critica in quanto comporta o il riconoscimento dell'incidente, e quindi la sua gestione, oppure l'archiviazione dell'evento.

Relativamente alla rilevazione dell'evento, la segnalazione di un evento potenzialmente identificabile come incidente può provenire da diverse fonti, quali:

- personale interno;
- terze parti;
- sistemi di monitoraggio della sicurezza fisica o logica.

Le segnalazioni possono provenire dal servizio di Help Desk, dai sistemisti o dagli utenti stessi. Tutte queste segnalazioni indirizzate vengono analizzate e classificate.

Una volta che l'incidente è identificato e classificato, vengono determinate le seguenti variabili:

- l'urgenza dell'intervento;
- l'impatto dell'evento sull'operatività dell'Amministrazione (es. importanza del servizio impattato);
- nel caso l'evento non presenti conseguenze, esso deve essere comunque tracciato;
- nel caso l'evento venga classificato come incidente di sicurezza deve essere comunicato al Titolare del trattamento, al DPO-RPD Responsabile della protezione dei Dati, al Responsabile del servizio, al CED ove esistente, al fine di avviare la fase di gestione.

Successivamente all'identificazione e classificazione dell'evento, il Titolare del trattamento, nel caso l'evento venga classificato come incidente di sicurezza, può prevedere la creazione di un IRT (Incident Response Team) al fine di avviare la fase di gestione.

Nel caso in cui non sia creato l'IRT, il Titolare del trattamento, sentito il DPO, dà disposizioni affinché si provveda alla registrazione dell'evento, secondo opportune modalità, in funzione della tipologia di evento segnalato.

3. Gestione degli incidenti

Il processo di gestione degli incidenti è un processo di tipo reattivo. A seguito del verificarsi di un incidente occorre procedere con le attività nel seguito descritte:

- Rilevazione, identificazione e classificazione degli incidenti.
- Gestione degli incidenti.
- Chiusura degli incidenti.

Sulla base delle informazioni raccolte durante la fase di rilevazione, identificazione e classificazione dell'evento, nel caso in cui sia stato classificato come incidente, il Titolare del trattamento o l'IRT se nominato, esegue tutte le procedure necessarie per provvedere alla gestione dello stesso.

Nella gestione di un qualunque incidente di sicurezza devono essere considerate le seguenti due **priorità**:

- Prima Priorità: proteggere tutti gli asset dell'Ente/Azienda, incluse le risorse colpite dall'incidente, fino al ripristino della normale operatività;
- Seconda Priorità: raccogliere informazioni e prove per supportare le eventuali e appropriate azioni correttive, disciplinari o legali.

Ulteriori attività da svolgere collegate all'incidente di sicurezza rilevato:

- nel caso di eventi con livelli di gravità estremamente rilevanti sui dati gestiti dal Sistema informativo l'Ente/Azienda provvederà ad attivare il processo di Data Breach;
- tutte le attività di gestione devono essere tracciate e documentate per quanto possibile a partire dal momento della rilevazione.

4. Processo di Data Breach

Nel caso in cui l'incidente di sicurezza abbia un impatto significativo sui dati personali contenuti nelle banche dati (Data Breach) di titolarità dell'Ente/Azienda, in conformità a quanto previsto dall'art. 33 del GDPR n. 2016/679.

Il flusso inizia con l'identificazione di un Data Breach nell'ambito della gestione di un incidente di sicurezza e si conclude, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, con l'invio al Garante, di una notifica da parte del Titolare del trattamento **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 comporti un **rischio** per i diritti e le libertà delle persone fisiche.

Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta** tutte le violazioni dei dati personali, ad esempio predisponendo un **apposito registro**. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

Vanno notificate unicamente le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali.

Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti

dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

5. Descrizione del flusso

Il flusso di comunicazione al Garante da parte dell'Ente prevede i seguenti passi:

1. Il Titolare del trattamento o l'IRT, se nominato, nel corso della gestione di un incidente di sicurezza informatica, riscontra una compromissione di dati personali (Data Breach).
2. Gli uffici impattati, valutano l'effettiva perdita o diffusione di dati personali e le informazioni contenute nel modulo compilato.
3. In caso di valutazione con rilevamento di violazione dei dati personali, che presenti un probabile rischio per i diritti e le libertà delle persone fisiche, gli uffici impattati informano il Titolare del trattamento o l'IRT, se nominato, inviando le informazioni raccolte.
4. il Titolare del trattamento o l'IRT, se nominato, di concerto con il DPO/RPPD Responsabile della protezione dei dati, valutano il livello di gravità della violazione in funzione della significatività dell'impatto della violazione avvenuta sui dati personali contenuti nelle banche dati di propria titolarità eseguendo un'autovalutazione attraverso il tool messo a disposizione sul sito web del Garante della protezione dei dati personali accessibile dal seguente link: https://servizi.gpdp.it/databreach/s/self-assessment .

Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali

Questo strumento, a disposizione di ciascun titolare del trattamento di dati personali, consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Mediante alcuni semplici quesiti, il titolare viene guidato nell'assolvimento degli obblighi in materia di **«Notifica di una violazione dei dati personali all'autorità di controllo»** (art. 33Apertura sito esterno in una nuova scheda per l'articolo 33 del Regolamento (UE) 2016/679 del Regolamento (UE) 2016/679 o art. 26 del D.Lgs. 51/2018) e di **«Comunicazione di una violazione dei dati personali all'interessato»** (art. 34Apertura sito esterno in una nuova scheda per l'articolo 34 del Regolamento (UE) 2016/679 del Regolamento (UE) 2016/679 o art. 27 del D.Lgs. 51/2018). Questo strumento è da considerarsi esclusivamente quale ausilio al processo decisionale del titolare del trattamento e non rappresenta il pronunciamento dell'Autorità sull'applicazione del Regolamento (UE) 2016/679 o del D.Lgs. 51/2018. Le informazioni fornite durante il suo utilizzo non saranno conservate.

Nel caso in cui la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, ai sensi dell'art. 33 del GDPR, la notifica all'autorità di controllo deve essere effettuata entro 72 ore, diminuite a 48 ore per gli Enti della Pubblica Amministrazione secondo quanto previsto dal Provvedimento del 27 maggio 2021 - Procedura telematica per la notifica di violazioni di dati personali (data breach).

Qualora la notifica all'autorità di controllo sia effettuata oltre i termini previsti, è corredata dei motivi del ritardo.

Eventuali richieste di ulteriori informazioni necessarie o modifiche alla comunicazione al Garante, durante le attività di risoluzione dell'evento, saranno concordate sentito il DPO, Responsabile della Protezione dei Dati, con i responsabili degli uffici coinvolti.

6. Come inviare la notifica al garante

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ in attuazione del: Provvedimento del 27 maggio 2021.

Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante.

7. Comunicazione della 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, ai sensi dell'art. 34 del GDPR, 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:

- il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- 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.

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 a una comunicazione pubblica (Es. pubblicazione sul sito web dell'Ente/Azienda) o a una misura simile, tramite la quale gli interessati sono informati della violazione 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.

La presente procedura sarà oggetto di periodiche revisioni e adeguamenti in relazione alle norme di armonizzazione che saranno emanate, a variazioni nelle misure di sicurezza da adottare e conseguenti modifiche procedurali.

8. Chiusura degli incidenti

A seguito dell'implementazione delle contromisure e della valutazione della loro efficacia, l'Ente/Azienda dichiara l'incidente chiuso in modo formale, verificando che siano state prodotte dall'IRT, se nominato, le seguenti evidenze:

- l'analisi relativa alle modalità di gestione dell'evento al fine di valutare i tempi di risposta, la metodologia utilizzata, ecc. ed al fine di verificare la necessità di modifiche od integrazioni nella procedura e/o policy in essere;
- la stesura di un rapporto relativo all'incidente di sicurezza, da condividere con i dirigenti responsabili delle strutture coinvolte, in modo da riportare le problematiche di sicurezza verificatesi e tenerne traccia.
  Il rapporto deve essere consegnato tempestivamente e deve contenere, necessariamente, i seguenti punti:
  - descrizione dell'evento, dalla sua segnalazione al ripristino dell'operatività;
  - esposizione di tutte le prove raccolte e di tutte le ricerche effettuate con i relativi risultati;
  - ipotesi sulle cause dell'incidente;
  - proposte di miglioramento e azioni correttive;
  - l'esecuzione delle azioni correttive proposte ed approvate.

A conclusione dell'incidente l'IRT (Incident Response Team), se nominato, deve trasmettere una dettagliata relazione al Titolare del Trattamento.

Data 02/08/2023

Il Titolare del trattamento