**ANALISI TECNICA DELL'EVENTO**

I Riceventi, dopo un'analisi preliminare, attivano il Gruppo di Gestione, sotto la supervisione del Coordinatore del Gruppo Privacy. Il Gruppo che gestisce gli incidenti, è responsabile, sulla base delle rispettive competenze, in base alla tipologia della violazione, dell'analisi tecnica dell'evento, delle azioni da mettere in atto tempestivamente per il contenimento del danno, avvalendosi della collaborazione delle figure indicate nella matrice (allegato B).

In particolare, una volta verificato che l'evento segnalato si configuri effettivamente come un "Data Breach" (Analisi Preliminare), verranno svolte tutte le operazione necessarie a raccogliere gli elementi per una valutazione dell'evento (Analisi Approfondita) ai fini della notifica al Garante della Privacy. È importante sottolineare che, anche nel caso in cui dall'Analisi Preliminare emerga che la segnalazione non ha i caratteri del Data Breach, è necessario registrarla nel Registro delle Violazioni.

Durante l'Analisi Approfondita, dovranno essere accertate le circostanze della violazione, le conseguenze e i relativi rimedi.

Si precisa che l'art. 33 paragrafo n. 4 del DGPR recita "Qualora nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo". Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni e, anche in caso queste non siano per il momento ritenute esaustive, effettuare la notificazione.

Nello specifico verrà effettuato, in un tempo consigliabile non superiore a 8 – 10 ore:

- Il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento (cfr Linee Guida sulla notifica delle Violazioni dei dati personali ai sensi del Regolamento UE 2016/79 WP 250 Par. 1 . punto 2)
- L'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
- L'identificazione degli interessati;
- Il contenimento del danno come di seguito descritto:

 Limitazione degli effetti dell'incidente,

 Raccolta delle prove forensi nel caso sia ipotizzato un reato,

 Determinazione delle azioni possibili di ripristino,

 Valutazione delle eventuali vulnerabilità collegate con l'incidente,

 Individuazione delle azioni di mitigazione delle vulnerabilità individuate,

 Valutazione dei tempi di ripristino,

 Gestione della comunicazione con i Clienti, con CERT e con i media,

 Ripristino dei dati, dei sistemi, dell'infrastruttura e delle configurazioni,

 Verifica dei sistemi recuperati.

Tutte le operazioni effettuate devono essere tracciate e riconducibili a specifiche persone, sulla base della matrice allegato B.

**VALUTAZIONE DELLA GRAVITÀ DELL'EVENTO**

Secondo la matrice dell'allegato B, il Coordinatore del Gruppo Privacy, con il supporto dei soggetti competenti, dovrà appurare se l'evento merita di essere notificato al Garante della Privacy e con quali modalità (notifica unica o per fasi).

Insieme ai soggetti interni di ausilio alla fase di analisi tecnica, si dovrà:

- Informare il RPD;
- Accertare la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà delle persone (cioè quando si è verificato una 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);
- Effettuare la notifica al Garante, se necessaria;
- Verificare, successivamente, se sia necessaria una seconda notifica più approfondita, di conseguenza ad una analisi tecnica supplementare;
- Effettuare una comunicazione all'Autorità giudiziaria competente, se necessaria.

L'art. 33 paragrafo n. 1 chiarisce che non vi è obbligo di notifica della violazione

quando è “improbabile” che questa comporti un rischio per i diritti e le libertà delle persone fisiche, ovviamente il giudizio che determina l’improbabilità del rischio deve essere riportato nel Registro delle Violazioni.

A questo proposito, i Garanti europei nelle loro linee guida, precisano che la mancata comunicazione può essere sanzionata ma che nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria.

Nella fase di Valutazione, sulla base delle informazioni predisposte in fase di Pianificazione, occorre innanzitutto stabilire se nell’incidente sono coinvolti i dati personali. In caso di risposta positiva occorre valutare l’impatto sugli interessati. Se si tratta di una violazione di riservatezza occorre verificare che le misure di sicurezza (es.: cifratura dei dati) in vigore rendano improbabile l’identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note). In caso di perdita di integrità o disponibilità di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati.

Se in tale modo i rischi per gli interessati sono trascurabili, la procedura può terminare, dopo aver documentato il processo e le scelte operate: le misure messe in atto sono state adeguate alla minaccia. La fase di Miglioramento può essere innescata per incrementare ulteriormente la protezione del dato, ma non è obbligatoria.

Nel caso che i rischi per l’interessato non siano trascurabili occorre procedere come di seguito:

1. Si ha il dovere di notificare al Garante, questo può presentarsi in 3 sottocasi:

a. L’organizzazione è Titolare del/i trattamenti dei dati coinvolti nell’incidente

b. L’organizzazione è contitolare del trattamento con delega alla notifica

c. L’organizzazione è Responsabile del trattamento con delega alla notifica.

2. L’organizzazione non ha nemmeno potenzialmente il dovere di notificare all’Autorità Garante: questo quando l’ASL TO4 agisce come Responsabile del trattamento per conto di altro Titolare, senza delega alla notifica al Garante.

Nella seconda ipotesi l'organizzazione deve comunicare al Titolare la sospetta violazione e/o l'incidente di sicurezza riguardante dati personali al Titolare stesso nei modi convenuti con la massima tempestività e mettersi a disposizione di quest'ultimo per approfondimenti e contenimento dei danni.

Nella prima ipotesi occorre valutare, seguendo le indicazioni dei documenti sopracitati, se il rischio per gli interessati è probabile. In questa fase come prima indicazione occorre assumere come rischio il massimo risultante dall'analisi fatta in fase di Pianificazione. L'analisi del caso specifico deve portare ad una valutazione specifica. L'analisi dei rischi per gli interessati deve dare le giuste priorità agli sforzi di contenimento dell'incidente, nonché fare proseguire la procedura nel caso in cui la soglia sia superata. In ogni caso va condotta la fase di Miglioramento.

Qualora i contorni della compromissione non siano chiari si può attendere fino ad un massimo di 72 ore prima di effettuare una notifica. Alla scadenza delle 72 ore è opportuno fare una comunicazione significando che questa è l'inizio di una notifica in fasi. Si può valutare di fare una notifica cumulativa se una stessa compromissione ha riguardato la stessa tipologia di dati con le stesse modalità.

Per completare la comunicazione, se temporalmente fattibile, occorre individuare:

- Le misure di contenimento adottate
- Il numero anche approssimativo di interessati
- Il periodo di violazione
- Se si ritiene di informare o meno gli interessati e le relative motivazioni
- Le misure di contenimento del danno da suggerire agli interessati
- Il carattere transfrontaliero e la nazionalità degli interessati o meno
- Le azioni di miglioramento intraprese.