ISTRUZIONE OPERATIVA DATA BREACH

L'art. 33 del Regolamento Europeo 679/2016 (GDPR) e la normativa nazionale in vigore, impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (data breach) entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR e della normativa nazionale in vigore.

Per "Violazione di dati" si intende la 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 (Art. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

E' importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

Si possono distinguere tre tipi di violazioni:

violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;

violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;

violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

Rischio assente: la notifica al Garante non è obbligatoria.

Rischio presente: è necessaria la notifica al Garante.

Rischio elevato: In presenza di rischi "elevati", è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

STEP	ATTIVITA'	CHI	A CHI	QUANDO	COME
1	Rilevazione e segnalazione di data breach	Tutto il personale, collaboratori, fornitori, responsabili	Al Responsabile amministrativo della struttura di riferimento (Dirigente, RAD, Direttore Tecnico) o al suo sostituto o all'incaricato privacy e al DPO	Appena se ne viene a conoscenza	Utilizzando le vie più brevi (telefono, di persona, e-mail)
2	Raccolta informazioni sulla violazione	Il responsabile della struttura o il sostituto o l'incaricato privacy, insieme al DPO e ai soggetti coinvolti nella violazione (il responsabile della struttura nel caso non possa essere immediatamente disponibile, deve dare istruzioni precise alla persona che l'ha contattato per iniziare subito la raccolta delle informazioni, indicando dove reperire il modello predisposto a tale scopo)		Immediatamente	Utilizzando il modello fornito e raccogliendo informazioni dai soggetti coinvolti nella segnalazione e nel trattamento dei dati violati
3	Comunicazione del data breach	Il responsabile amministrativo della struttura	Al titolare del trattamento, RPD, esperti ICT	Appena ottenute informazioni di	Utilizzando le vie più brevi (telefono, di persona, e-mail)

		(RAD, Direttore Tecnico, dirigente) o il sostituto o il referente privacy (in mancanza di tali figure la stessa persona che ha rilevato la violazione)		base sulla violazione	
4	Valutazione d'impatto	Titolare, RPD, esperti ICT, soggetti coinvolti		Appena ricevuta la comunicazione	Utilizzando la metodologia indicata nel piano della protezione dei dati personali e gestione dei rischi
5	Individuazione delle azioni correttive	RPD, esperti ITC, soggetti coinvolti		Appena terminata la valutazione d'impatto	Analizzando i risultati della valutazione d'impatto
6	Comunicazione delle valutazioni effettuate e delle azioni da intraprendere	RPD, responsabile della struttura o sostituto o incaricato privacy	Al Titolare		Tramite una breve relazione anche orale
7	Notifica della violazione (se è necessaria)	Titolare	Al Garante	Entro 72 ore dalla rilevazione	Mediante la modulistica predisposta dal Garante
8	Comunicazione agli interessati coinvolti (se è necessaria)	Titolare	Alle persone fisiche i cui dati sono stati violati	Nei termini indicati nella valutazione d'impatto	Comunicazione diretta alle singole persone o mediante pubblicazione in sito a loro accessibile delle eventuali conseguenze della violazione sulle categorie di persone fisiche interessate
9	Disposizioni per l'attuazione delle misure correttive (se individuate)	Responsabili delle strutture coinvolte	Ai soggetti incaricati di svolgere le attività	Nei termini indicati nella valutazione d'impatto	Devono essere indicate in dettaglio le operazioni da svolgere, chi è l'incaricato, i tempi di attuazione; prevedere eventuali operazioni di verifica dell'efficacia delle misure correttive
10	Recepimento della risposta del Garante alla notifica (se effettuata)	Titolare, RPD, responsabili delle strutture coinvolte, esperti ICT			Disposizioni per l'attuazione delle eventuali misure correttive indicate dal Garante; effettuazione di ulteriori indagini per approfondire le informazioni raccolte

Attività relative alla registrazione dell'incidente

STEP	ATTIVITA'	CHI	QUANDO	COME
1	Registrazione della violazione/aggiornamenti	RDP e incaricato privacy	Appena ricevuta la comunicazione	Compilando l'apposito registro con la descrizione della violazione, delle azioni intraprese e annotando i successivi aggiornamenti.
2	Registrazione della risposta del Garante	RDP e incaricato privacy	Al momento della ricezione	Annotando sul registro gli estremi della risposta del Garante e le eventuali prescrizioni in essa contenute
3	Registrazione della prosecuzione/chiusura dell'incidente	RDP e incaricato privacy	In seguito alle indicazioni del RPD	Registra la chiusura dell'incidente se non necessita di ulteriori indagini o riporta le istruzioni per le ulteriori indagini

Attività inerenti la prosecuzione delle indagini

STEP	ATTIVITA'	CHI	A CHI	QUANDO	COME
1	Prosecuzione delle indagini	RPD, responsabile della struttura o sostituto o incaricato privacy, soggetti coinvolti nella violazione e nei trattamenti di dati violati, esperti ICT		A seguito di indicazione da parte del Garante o del titolare; se previsto nella prima valutazione d'impatto; nel caso che le informazioni raccolte risultino incomplete o mancanti	Raccogliendo le informazioni mancanti, o approfondendo quelle note per rilevare eventuali impatti non riscontrati nella prima indagine
2	Esecuzione di una nuova valutazione d'impatto	Titolare, RPD, esperti ICT, soggetti coinvolti		Al momento che si ritiene di aver raccolto tutte le informazioni possibili sulla violazione	
3	Comunicazione dei risultati del proseguimento delle indagini	RPD, responsabile della struttura o sostituto o incaricato privacy	Al Titolare	appena terminato il lavoro	Tramite relazione sintetica sui risultati della valutazione d'impatto e sulle azioni necessarie, allegando il materiale informativo raccolto
4	Aggiornamento della notifica al Garante (se necessario)	Titolare	Al Garante	Appena sono disponibili i nuovi dati o secondo i termini stabiliti	Mediante la modulistica predisposta o come indicato

				dal Garante	dal Garante
5	Comunicazioni agli interessati (se necessario)	Titolare		Nei tempi stabiliti nella valutazione d'impatto	Contattando direttamente gli interessati oppure rendendo nota la violazione e le possibili conseguenze mediante pubblicazione accessibile alle categorie di interessati