PROCEDURA DATA BREACH

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

Già attualmente sussiste l'obbligo di notifica delle violazioni di dati personali per particolari categorie di titolari (società telefoniche ed internet provider; pubbliche amministrazioni) o per particolari categorie di trattamenti (sistemi biometrici, dossier sanitario).

La novità del GDPR, che diverrà applicabile dal 25 maggio 2018, è l'estensione dell'obbligo a tutti i titolari.

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, settantadue 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, il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Occorre in ogni caso tenere conto che, la mancata notifica e/o comunicazione, possono rappresentare per l'autorità di controllo un indizio di carenze più profonde e strutturali quali ad esempio carenze od inadeguatezza di misure di sicurezza, in tal caso, trattandosi di ipotesi separate ed autonome, l'autorità procederà per l'ulteriore irrogazione di sanzioni.

Il rispetto degli obblighi di notifica (art. 33) e di comunicazione (art.34), in situazioni già mediamente complesse (in termini di dimensioni ed articolazione dell'organizzazione del titolare e/o in termini di numero di interessati di cui sono trattati i dati personali e/o in termini di operazioni di trattamento, o di quantità, varietà, natura dei dati trattati), richiede al Titolare di strutturare il trattamento dei dati personali avvalendosi di un sistema di conformità e gestione del rischio che preveda un sotto-sistema per la gestione degli incidenti e la continuità operativa.

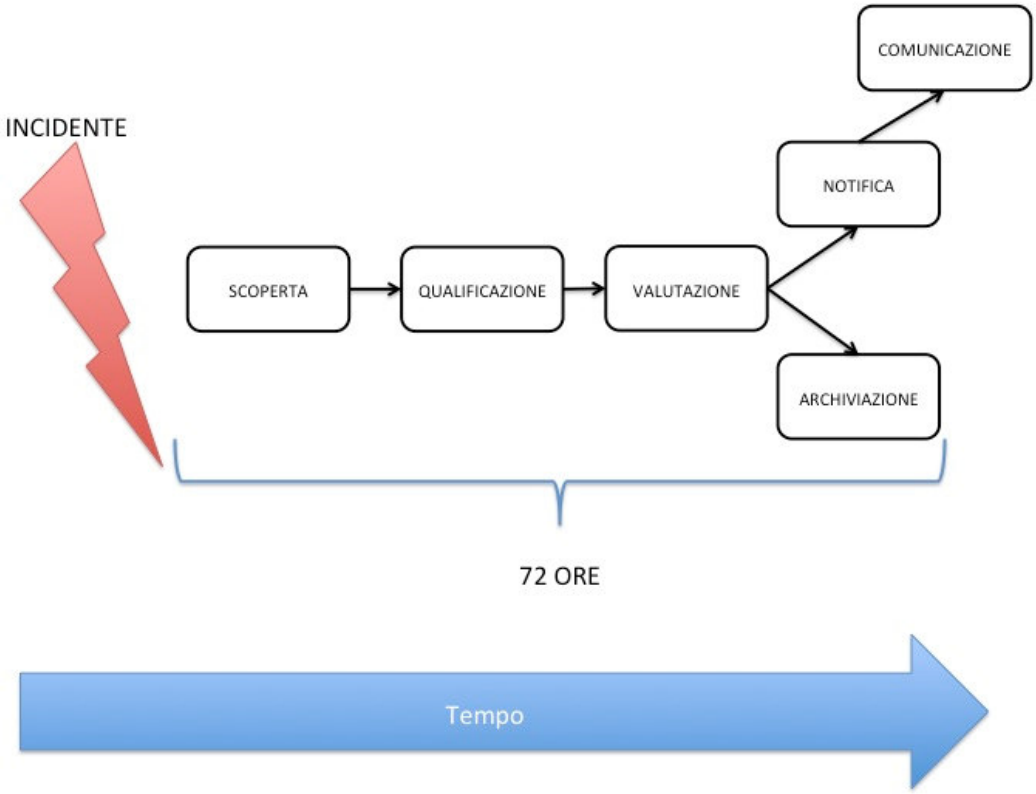
Questo sistema deve essere in grado di rispettare i requisiti di trasparenza, evidenza e responsabilità prescritti dal GDPR; si ricorda che l'art.24 punto 1 del GDPR richiede al titolare di "mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR".

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 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.
Ne discende che le generali attività di scoperta dell'incidente, come le successive di trattamento, devono essere documentate, adeguate (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi), tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti.

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



Il considerando 85 del GDPR spiega che lo scopo della notifica è di limitare i danni che possono derivare per effetto di una violazione a carico degli interessati e che l'efficacia di questo dovere di limitazione dipende dalla tempestività e dall'adeguatezza con cui la violazione è affrontata.
Il gruppo "Article 29 Data Protection Working Party" (WP29)[1], chiarisce ulteriormente che la responsabilità del titolare deve essere commisurata secondo la sua capacità di scoprire tempestivamente un incidente ed indagarlo al fine di valutare l'obbligatorietà della notifica.
Dato che l'obbligo di notifica spetta al titolare, è molto importante che, nell'affidare servizi a responsabili del trattamento, questi, preliminarmente, si accerti della capacità del fornitore nel gestire tempestivamente e adeguatamente un incidente di sicurezza (art. 28 p.1 GDPR) e, quindi, preveda idonee clausole contrattuali (art. 28 p.3 GDPR) che regolino il rapporto di fornitura in modo da garantire il rispetto del GDPR.
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.
Scoprire l'incidente non è sufficiente, il titolare deve essere in grado di valutare la portata di questo in termini di impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati.

Si possono distinguere tre tipi di violazioni:

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

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

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

In particolari circostanze le violazioni potrebbero essere combinate tra loro.
Particolarmente "insidiosa" è il terzo tipo di violazione in considerazione dell'eventualità in cui l'indisponibilità sia solo temporanea: deve essere considerata una violazione? In caso positivo quando scatterebbe l'obbligo di notifica?

L'art. 32 del GDPR richiede al titolare di mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; in particolare:

– la lettera b) richiede: "la capacità di assicurare su base permanente la disponibilità dei sistemi e dei servizi di trattamento;

– la lettera c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

Da quanto sopra si ricava che un incidente che determini la non disponibilità di dati per un periodo di tempo deve essere comunque considerato violazione e, dunque, deve essere comunque documentato.
L'obbligo di notifica e quello aggiuntivo di comunicazione devono essere valutati caso per caso in relazione ai diritti ed alla libertà degli interessati.

Per esempio: la temporanea indisponibilità di dati personali per un ospedale potrebbe comportare rischi per i diritti e la libertà delle persone fisiche quando determina la cancellazione di un intervento; mentre, nel caso di una società di comunicazioni un'indisponibilità temporanea di dati che determinasse un ritardo nell'invio di una newsletter non sarebbe causa dell'obbligo di notifica.

Il considerando 85 offre utili elementi per determinare i rischi che possono determinare l'obbligo di notifica, in particolare, occorre valutare la possibilità che la violazione possa causare danni fisici, materiali o immateriali alla persona fisica. La disposizione a titolo d'esempio elenca: perdita del controllo dei dati personali che li riguardano; limitazione dei loro diritti; discriminazione; furto o usurpazione di identità; perdite finanziarie; decifratura non autorizzata della pseudonimizzazione; pregiudizio alla reputazione; perdita di riservatezza dei dati personali protetti da segreto professionale, o qualsiasi altro danno economico o sociale significativo per la persona interessata.

L'art. 34 del GDPR stabilisce che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve comunicare la violazione all'interessato senza ingiustificato ritardo.

Il considerando 86 del GDPR chiarisce che l'obbligo di comunicazione risponde allo scopo di consentire all'interessato, qualora sussista una violazione che presenta rischi elevati, di prendere le precauzioni necessarie.

La comunicazione ha un contenuto pressoché identico a quello della notifica.

Notifica di Data Breach - Art. 33 p.3 GDPR

a) Descrivere la 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) Comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.

c) Descrivere le probabili conseguenze della violazione dei dati personali.

d) Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

INDIRIZZO PEC DEL GARANTE DELLA PRIVACY:

databreach.pa@pec.gpdp.it

Comunicazione di Data Breach - Art. 34 p.2 GDPR

a) Descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali.

b) Comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.

c) Descrivere le probabili conseguenze della violazione dei dati personali.

d) Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

INDIRIZZO PEC DEL GARANTE DELLA PRIVACY:

databreach.pa@pec.gpdp.it

La comunicazione dovrebbe essere data direttamente e personalmente agli interessati coinvolti dalla violazione, a meno che ciò comporti sforzi sproporzionati. In tal caso, si procede invece ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con la medesima efficacia.

La comunicazione deve essere distinguibile rispetto altre diverse comunicazioni che vengono fatte dal titolare agli interessati, in altri termini, la comunicazione deve essere chiara, inequivocabile e richiamare l'attenzione dell'interessato.

Il rispetto di questi requisiti richiede che il titolare, già prima che si verifichi una causa di comunicazione, considerati i dati che tratta e le categorie di interessati, predisponga un piano specifico di comunicazione.

La comunicazione, pur sussistendo la condizione di rischio elevato, si ritiene soddisfatta quando:

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.
Mentre per far scattare l'obbligo di notifica è sufficiente che sussista una violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche, per la comunicazione occorre che tale rischio sia elevato.

Il titolare è dunque tenuto non solo ad individuare e qualificare i rischi connessi a violazioni di dati personali, ma, qualora tali rischi riguardino i diritti e le libertà delle persone fisiche, deve anche procedere ad una valutazione del livello di rischio.

Il considerando 76 del GDPR chiarisce che la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

Il WP29 suggerisce ulteriori criteri per permettere una valutazione più accurata[2]

1) Tipo di violazione

2) Natura, sensibilità e volume dei dati personali

3) Facilità di riconoscimento degli interessati

4) Serietà delle conseguenze per le persone fisiche

5) Caratteristiche specifiche delle persone fisiche

6) Quantità di persone fisiche coinvolte

7) Caratteristiche specifiche del titolare

La valutazione dei rischi non sempre è semplice[3], il WP29 raccomanda al titolare, in caso di dubbio, di scegliere la strada di maggior tutela procedendo alla notifica.

Alla luce di quanto detto ci si domanda come e cosa possa fare il titolare per rispettare gli articoli 33 e 34 del GDPR in vista dell'imminente applicabilità fissata al 25 maggio 2018.

I presidi della notifica e della comunicazione seppure richiedono adempimenti specifici, non possono essere letti ed interpretati correttamente senza considerare la loro correlazione con l'intero GDPR, quali organi di un medesimo corpo.

In particolare sono fondamentali gli articoli 24 e 32 del GDPR, essi impongono ad ogni titolare di:

1) mettere in atto misure tecniche e organizzative adeguate per garantire il rispetto del GDPR;

2) essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR;

3) riesaminare ed aggiornare tali misure quando necessario;

4) garantire un livello di sicurezza adeguato al rischio.

Gli obblighi di cui sopra devono essere valutati tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche propri di ciascun titolare.

E' chiaro che, pur essendo uguali per tutti i titolari europei, questi obblighi assumono aspetti diversi a seconda del titolare. Per esempio: se per il titolare di una piccola organizzazione che tratta piccole e limitate quantità di dati personali non è richiesta una particolare attività di formalizzazione, per il titolare di una organizzazione vasta e complessa che tratta dati personali su larga scala, aventi natura sensibile, è invece richiesta la strutturazione di un vero e proprio sistema di gestione dei dati personali (PDMS) che operi interattivamente e sinergicamente con gli altri sistemi di gestione attivi (Per esempio: i sistemi qualità, ambiente, 231, ecc…).

Il trattamento degli incidenti di sicurezza presuppone, a monte, l'esistenza di un sistema di sicurezza delle informazioni che offre tutti gli strumenti necessari.

Ad esempio, la scoperta dell'incidente presuppone un sistema di monitoraggio che a sua volta presuppone l'organizzazione della sicurezza all'interno dell'ente (definizione degli obiettivi, politiche, compiti e responsabilità, classificazione di dati e processi, individuazione e definizione dei rischi, individuazione dei rimedi).

La valutazione dell'incidente presuppone la definizione dei criteri di valutazione, la formazione del personale incaricato, la predisposizione di procedure.

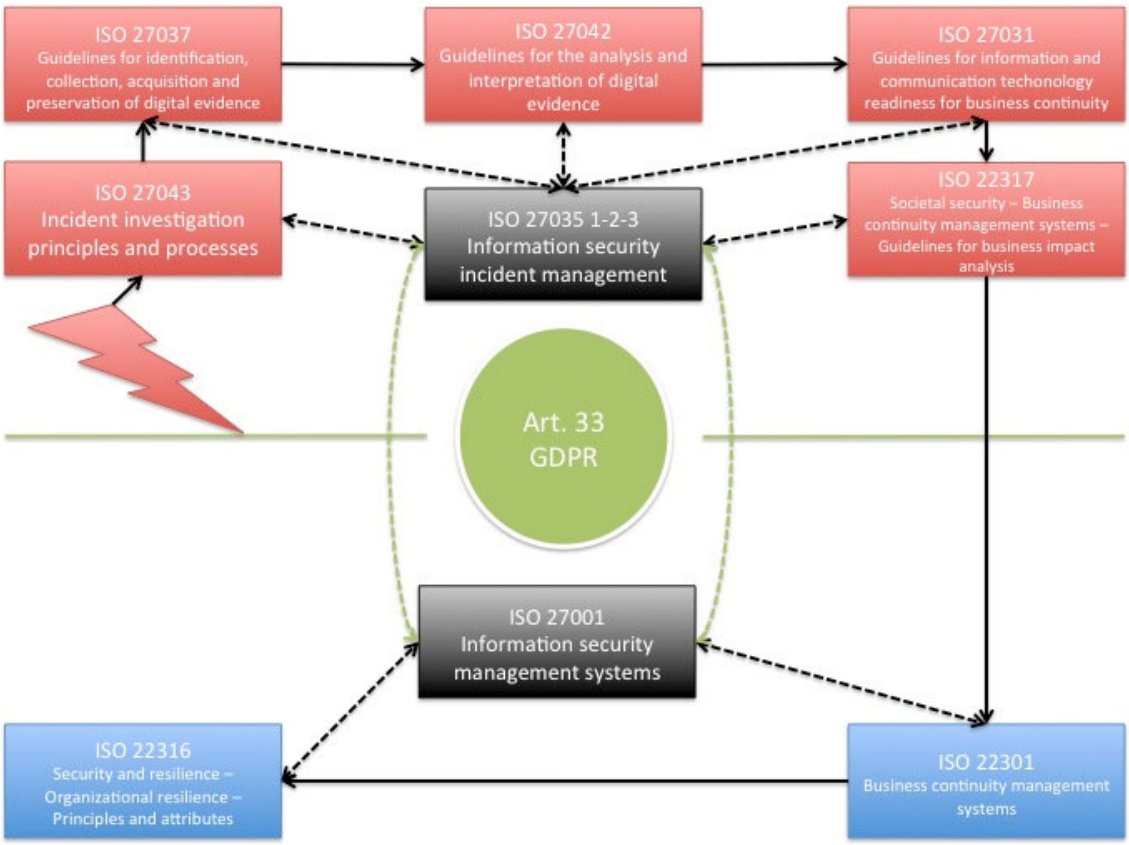
La tempestività nella notifica può essere assicurata se preesiste un sistema di comunicazione interno adeguato e tutti coloro che operano per il titolare abbiano ricevuto adeguata formazione.

La stessa comunicazione può essere fatta solo se sono disponibili le informazioni necessarie, aspetto possibile solo se precedentemente è stato strutturato un sistema di report dell'incidente, è stata fatta una ricognizione adeguata dell'organizzazione del titolare, sono state condotte le Valutazioni di impatto sui dati personali (DPIA).
Infine, la stessa documentazione delle violazioni che la norma prescrive di conservare (anche per quelle che non determinano obbligo di notifica), è possibile se è stato strutturato un sistema di gestione degli incidenti.

L'aderenza del PDMS a standard e buone prassi, riconosciute (per esempio: UNI – EN – ISO) è certamente un elemento prezioso che aiuta il titolare e ne attesta sia la diligenza che la sensibilità, per titolari che gestiscono organizzazioni complesse, questo passo è fortemente suggerito.
Gli standard internazionali che aiutano a gestire la notifica e la comunicazione sono molteplici, tra questi si segnala:

ISO 27001: Information security management systems – Requirements.
ISO 27035 parti 1 e 2: Information security incident management.
ISO 27043: Incident investigation principles and processes.
ISO 22301: Business continuity management systems – Requirements.

Lo schema che segue illustra una possibile combinazione degli standard ISO nella gestione della notifica delle violazioni dei dati personali prevista dall'art. 33 del GDPR.



Concludendo, il titolare deve costruire il proprio PDMS estrapolando dagli standard i principi più adatti alle proprie specifiche circostanze, ricordando che il DPMS, pur essendo documentato, non si risolve in tale aspetto, ma rappresenta uno strumento di guida e controllo da utilizzare nella gestione della propria organizzazione.

REGISTRO DATA BREACH

Numero	Data	Descrizione	Categorie di interessati (utenti, dipendenti, fornitori, altro)	Categorie dei dati (comuni, particolari, giudiziari)	Numero degli interessati	Probabili conseguenze della violazione	Misure adottate per attenuare i rischi	Esito della valutazione del rischio	Comunicazione al garante Si/no	Comunicazione agli interessati Si/no