Premessa

Il Regolamento (UE) 2016/679 del 27 aprile 2016 "Regolamento generale sulla protezione dei dati" – indicato anche come GDPR, acronimo del titolo in inglese General Data Protection Regulation –, obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri ed entrato in vigore il 24 maggio 2016, si applica a decorrere da 25 maggio 2018.

Il sistema di trattamento e protezione dei dati personali che esso prevede si basa sul concetto di accountability, cioè, superata una logica meramente incentrata ad un adempimento formale, quale era quella che permeava la disciplina precedente, che in Italia era dettata dal decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", regola la materia in una logica di responsabilità del risultato, che rappresenta il parametro di valutazione di ogni comportamento e attività in relazione a obiettivi definiti. Insieme al concetto di responsabilità, l'accountability comprende quelli di trasparenza, intesa come accesso alle informazioni concernenti ogni aspetto dell'organizzazione, delle attività, dei comportamenti e dei risultati, e di compliance, intesa come rispetto delle norme e quindi come garanzia dell'adeguamento e dell'adeguatezza dell'azione alle leggi, ai regolamenti e altre norme, e quindi di legittimità.

Si basano su questa logica tutti gli istituti giuridici che il GDPR disciplina tra i quali sono previsti:

- la notifica di una violazione dei dati personali all'autorità di controllo, comunemente detta "data-breach" (art.33);
- la comunicazione di una violazione dei dati personali all'interessato (art. 34).

Il Data-Breach

Il data-breach era già previsto dalla normativa precedente ma con il Regolamento (UE) 2016/679 ne viene estesa la disciplina, che da settoriale (servizi di comunicazione accessibili al pubblico, oltre ad altre ipotesi regolate da fonti diverse) si trasforma in generale e quindi applicabile a tutti i titolari di trattamento indipendentemente dalla tipologia di attività svolta.

La definizione del data-breach è contenuta nell'art. 4 punto 12) del GDPR ed individuata come 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*".

L'art. 33 del GDPR, nell'ambito della sicurezza dei dati personali, definisce i presupposti e la procedura del data-breach, imponendo l'obbligo di notificare all'Autorità nazionale di controllo – nel caso dell'Italia al Garante per la protezione dei dati personali – qualsiasi violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato a dati personali, indipendentemente dalla causa che l'ha generata. La stessa norma dispone che il data-breach vada notificato all'Autorità nazionale di controllo entro 72 ore dal momento in cui la violazione è conosciuta. Entro questo termine i titolari devono essere in grado di identificare la violazione, revisionare eventuale documentazione, adottare procedure e/o atti che mitighino il danno arrecato e notificare il data-breach all'Autorità nazionale di controllo. Per garantire il rispetto di tale termine, occorre predefinire come in concreto nella propria Amministrazione vada attivata e gestita la procedura per non trovarsi impreparati nel caso in cui ricorrano le condizioni di cui all'art 33 del GDPR. La procedura del data-breach va inoltre aggiornata e testata regolarmente per adottare tutte le misure tecniche e organizzative più appropriate e, se occorre, adeguarle alla luce delle criticità evidenziate dai fatti.

Rientrano nella fattispecie del data-breach gli eventi e i comportamenti atti a danneggiare i dati, a comprometterne la disponibilità o l'integrità indipendentemente da finalità o interventi fraudolenti. Fatti simili si verificano spesso e sono considerati fisiologici nella gestione e conservazione di dati con supporti informatici e tecnologici ma assumono rilevanza per l'art. 33 del Regolamento (UE) 2016/679 quando la violazione dei dati personali presenta un rischio per i diritti e le libertà delle persone fisiche.

Le linee guida del 6 febbraio 2018 in materia di data-breach

Il Gruppo di lavoro articolo 29 - istituito dall'art. 29 della direttiva dell'Unione Europea 95/46 e composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione europea -, nelle sue linee guida adottate il 6 febbraio 2018 in materia di data-breach, individua tre categorie di eventi rilevanti ai sensi degli artt. 33 e 34 del GDPR:

a) quando vi è un accesso incidentale o abusivo a dati personali;
b) quando vi è una perdita o distruzione accidentale o non autorizzata del dato personale;
c) quando vi è un'alterazione accidentale o non autorizzata del dato personale.

Nel caso concreto l'accaduto può corrispondere anche a più di una di queste categorie.
Il Gruppo di lavoro articolo 29 ha inoltre individuato alcuni parametri utili per valutare la rilevanza e la gravità di un data-breach. Tra gli aspetti da valutare per individuare la presenza di un rischio per i diritti e le libertà delle persone fisiche evidenzia:

- il tipo di violazione;
- la natura, il numero e il grado di sensibilità dei dati personali violati;
- la facilità di associare i dati violati a una persona fisica;
- la gravità delle conseguenze per gli interessati;
- il numero di interessati esposti al rischio;
- le caratteristiche del titolare del trattamento come, per esempio, le dimensioni dell'ente, il tipo di attività svolta, la qualità e quantità di dati trattati.

Infatti l'art. 33 del GDPR in ordine al contenuto della notifica all'Autorità nazionale di controllo stabilisce che essa deve almeno:

- 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;
- 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;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere 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.

Lo stesso articolo prevede che la notifica possa non essere fatta ove sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
L'art. 34 del GDPR stabilisce invece che quando la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. Ciò al fine di consentire all'interessato di proteggersi da eventuali conseguenze dannose derivanti da un data-breach. A volte, per esempio, il semplice cambio di una password può servire a evitare gravi danni, anche economici, derivanti dalla diffusione o uso improprio dei dati personali da parte di terzi.
La comunicazione deve contenere:

- descrizione della natura del data breach;
- individuazione delle categorie e del numero approssimativo degli interessati e delle registrazioni dei dati personali coinvolti;
- nome e contatti del DPO (Data Protection Officer, cioè il responsabile della protezione dei dati), se designato;
- descrizione delle probabili conseguenze del data-breach;
- descrizione delle misure di sicurezza adottate o da adottare per porre rimedio al data-breach e, se del caso, per attenuarne i possibili effetti negativi.

La comunicazione all'interessato deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le informazioni e le misure di cui all'art. 33, paragrafo 3, lettere b), c) e d).
Il titolare è esonerato dal comunicare il data-breach all'interessato nel caso in cui:

- il titolare abbia implementato misure di sicurezza adeguate e tali misure erano già state applicate ai dati personali oggetto del data-breach (per esempio la cifratura);
- dopo il data-breach il titolare abbia adottato misure di sicurezza atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione all'interessato richiederebbe sforzi sproporzionati e quindi si può procedere a una comunicazione pubblica.

Infine l'art. 33 del GDPR obbliga il titolare del trattamento a conservare la documentazione attestante tutti i data-breach avvenuti, che l'Autorità nazionale di controllo potrà esaminare per verificare il rispetto delle norme in materia. Tale adempimento si sostanzia nella tenuta e conservazione di un registro che deve riportare:

- le circostanze relative a qualsiasi violazione dei dati personali e le sue conseguenze;
- i provvedimenti adottati per porvi rimedio.

Inoltre il titolare deve motivare le decisioni assunte, in particolare nel caso in cui abbia deciso di non procedere alla notifica; oppure abbia ritardato nella procedura di notifica; oppure abbia deciso di non comunicare il data-breach agli interessati, motivazioni da riportare nel registro.

Comitato Data-Breach

Il data-breach richiede valutazioni e interventi di rilevanza giuridica, organizzativa, tecnica e tecnologica e di opportunità adeguati anche per prevenire o evitare eventuali conseguenze di carattere economico-finanziarie dovute a pretese risarcitorie e danni di valenza reputazionale per l'Ente.

Le attività di competenza dell'Amministrazione connesse a un data-breach richiedono quindi il coinvolgimento di diversi soggetti che, ciascuno per l'ambito di pertinenza, intervengano e collaborino in modo coordinato ed efficace a seguito del verificarsi di una violazione dei dati personali sia nella valutazione del fatto e delle iniziative da adottare sia nella predisposizione di misure atte a scongiurare il ripetersi di eventi analoghi.

Per quanto sopra esposto si rende necessario prevedere e definire una procedura che individui i soggetti da coinvolgere in considerazione delle funzioni svolte nell'ambito dell'amministrazione.

Occorre quindi individuare un gruppo di lavoro – che per brevità viene denominato **Comitato Data-Breach** – formato dai seguenti soggetti:

- il Titolare del trattamento (nella persona del suo Legale Rappresentante o suo delegato);
- Responsabile interno del trattamento dei dati personali interessato dalla violazione;
- Responsabile della sicurezza informatica ovvero l'Amministratore di Sistema;
- DPO (Data Protection Officer) del Titolare del Trattamento;
- Responsabile esterno del trattamento dei dati interessato dalla violazione;
- DPO (Data Protection Officer) del Responsabile esterno del trattamento dei dati interessato dalla violazione, se nominato.

Procedura gestione Data-Breach

La procedura di data-breach si articola nelle seguenti fasi:

a. comunicazione di fatti o circostanze che evidenziano o fanno supporre una violazione dei dati personali: il responsabile interno/esterno del trattamento o altro soggetto/dipendente incaricato del trattamento o il responsabile della sicurezza che venga a conoscenza di un fatto che determini o possa determinare una violazione dei dati personali informa il titolare del trattamento senza ingiustificato ritardo, inviando una segnalazione tramite posta elettronica a un indirizzo dedicato corrispondente a una lista di distribuzione che include i componenti del Comitato Data-Breach;
b. accertamento della violazione dei dati personali: i componenti del Comitato Data-Breach, ricevuta la segnalazione informano tempestivamente il Responsabile del trattamento interno ed esterno competente; a seconda del tipo di violazione dei dati personali e delle proprie competenze, acquisiscono ogni ulteriore informazione utile all'accertamento della violazione;
c. valutazione della violazione: il Comitato Data-Breach valuta il fatto descritto sulla base degli elementi acquisiti. Gli esiti della valutazione vengono formalizzati in apposito verbale sottoscritto in forma autografa o con firma digitale con marca temporale.

Tali esiti si possono così sintetizzare:

- **ipotesi I** - il rischio per i diritti e le libertà delle persone fisiche non è elevato: il titolare non deve notificare al Garante per la protezione dei dati personali né dare comunicazione agli interessati. Deve solo tenere traccia dell'evento e dell'analisi del rischio effettuata per future consultazioni compilando il registro;
- **ipotesi II** - il rischio per i diritti e le libertà delle persone fisiche è probabile ma non elevato: il titolare del trattamento notifica la violazione al Garante per la protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Se non è rispettato il termine delle 72 ore, il ritardo dev'essere giustificato adducendo una adeguata motivazione. La notifica è effettuata tramite l'invio di una mail con firma digitale e marca temporale, utilizzando l'apposito modulo;
- **ipotesi III** - il rischio per i diritti e le libertà delle persone fisiche è probabile ed elevato:
  a. il titolare del trattamento notifica la violazione al Garante per la protezione dei dati personali (art. 33);
  b. il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo e in maniera chiara e trasparente, tramite l'invio di una mail con firma digitale e marca temporale o, in mancanza, altra forma di comunicazione diretta (per es. nota cartacea protocollata). Nel caso in cui ci siano più interessati e la comunicazione diretta richiederebbe sforzi sproporzionati si procede a una comunicazione pubblica, o misura simile, tramite la quale gli interessati sono informati con analoga efficacia, per es. pubblicazione di un piccolo banner evidente nella home page del portale istituzionale per un congruo numero di giorni oppure notifica sempre tramite il portale istituzionale (art. 34).

c. compilazione del registro: il titolare del trattamento, oltre a conservare la documentazione attestante tutti i data-breach avvenuti, li documenta in un registro che deve contenere informazioni relative a:
   - le circostanze relative a qualsiasi violazione dei dati personali le sue conseguenze;
   - i provvedimenti adottati per porvi rimedio;
   - la motivazione delle decisioni assunte, in particolare nel caso in cui abbia deciso di non procedere alla notifica; oppure abbia ritardato nella procedura di notifica; oppure abbia deciso di non comunicare il data-breach agli interessati.

d. notifica della violazione al Garante e/o eventuale comunicazione agli interessati: il titolare del trattamento provvede alla notifica al Garante per la protezione dei dati personali e all'eventuale comunicazione agli interessati.

Per la notifica di violazioni dei dati personali il Garante per la protezione dei dati personali verrà utilizzata la modulistica adottata dal Garante medesimo e pubblicata nel relativo portale.

Compensi del Comitato Data-Breach

I componenti del Comitato Data-Breach svolgono l'attività suindicata a titolo gratuito essendo le stesse da intendersi quali attività già ricomprese nel mandato ovvero posizione ricoperta. Pertanto, la costituzione del Comitato Data-Breach è da intendersi ad invarianza di spesa.

Durata, revisione e validità del documento

Il presente documento è applicabile dal giorno solare successivo alla sua approvazione e fino a comunicazione contraria; è soggetto a valutazione periodica circa la sua efficacia ed è soggetto ad eventuale revisione delle forme e nei modi identici alla sua approvazione.