Premessa

Art. 4 – Punto 12) : Definizione

«violazione dei dati personali»:

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 – Punto 12): Conseguenze per l'interessato

Se non affrontata in modo adeguato e tempestivo, può provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie o …

Art. 4 – Punto 12) : Conseguenze per l'interessato

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 alla persona fisica interessata.

Non riguarda le conseguenze per l'azienda

Una eventuale violazione che porti alla divulgazione di informazioni inerenti segreti aziendali ma che non contiene dati personali, non risulta essere un data brech ai sensi del GDPR.

In cosa consiste un data breach ?

Esso include certamente l'attacco a sistemi informatici, l'intrusione o il data leak, dunque eventi in cui l'intervento malevolo di terzi è manifesto, ma comprende anche una serie di ipotesi riconducibili all'inosservanza di norme sulla sicurezza da parte del titolare del trattamento.

In cosa consiste un data breach ?

Anche la semplice associazione o confusione indebita di dati personali all'interno della struttura del titolare o l'accessibilità degli stessi a ruoli interni della struttura del titolare non autorizzati costituisce data breach.
In definitiva, l'area di ciò che rileva in termini di violazione dei dati personali tende a sovrapporsi e a coincidere con ciò che rileva in termini di osservanza delle misure di sicurezza.

In cosa consiste un data breach ?

Tendenzialmente, il concetto di data breach viene a essere equiparato a quello di **rilevante discontinuità** nel normale funzionamento di un sistema informatico.
Il diritto alla protezione dei dati personali va, cioè, correttamente inteso come fondamentale diritto di controllo e decisione riconosciuto all'interessato, diritto rispetto al quale, i dati personali costituiscono unicamente l'oggetto protetto ma non la ratio della tutela.

In cosa consiste un data breach ?

Il WP29 chiarisce che rientra nella categoria dei Data Breach anche un **incidente sulla sicurezza** dal quale deriva una **perdita di disponibilità** dei dati non permanente, ma circoscritta a un limitato periodo temporale, (ad esempio la perdita di accesso temporanea ai dati), in quanto potrebbe comunque comportare un significativo impatto sui diritti e le libertà degli individui (ad es. un blackout elettrico che impedisca all'interessato di accedere ai propri dati).

In cosa consiste un data breach ?

In particolare il Gruppo di lavoro suggerisce che anche la violazione che comporta la perdita temporanea di disponibilità **dovrebbe essere documentata** (così come nel caso di perdita o distruzione permanenti di dati personali).
Viene però precisato che, l'indisponibilità di un dato personale **dovuta dalla manutenzione** programmata del sistema in corso, non può essere considerata una "violazione della sicurezza" ai sensi del GDPR.

Art. 33: Notifica della violazione

Art. 33, comma 1: Notifica della violazione

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 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 presenti un rischio** per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Art. 33, comma 2: Oneri del Responsabile

Il responsabile del trattamento informa il titolare del trattamento **senza ingiustificato ritardo** dopo essere venuto a conoscenza della violazione.

→ *Definizione a livello contrattuale con il Responsabile del tempo massimo entro cui comunicare al Titolare la violazione*

Art. 33, comma 3: Contenuti della notifica

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;

→ *Necessario sapere ex ante dove sono i dati, come è organizzato il db, quanti gli interessati e quali le categorie di dati …*

Art. 33, comma 3: Contenuti della notifica

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;

→ *Pronto intervento del D:P.O., unità di crisi da allertare*

Art. 33, comma 3: Contenuti della notifica

c) descrivere le probabili conseguenze della violazione dei dati personali;

→ *Necessario aver documentato ex ante nella valutazione dei rischi/DPIA eventuali conseguenze alla perdita, modifica o mancata disponibilità dei dati trattati.*

Art. 33, comma 3: Contenuti della notifica

d) 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.

→ *Road map misure ? Che tipo di interventi tampone ? Avviso agli interessati ? Cambiamenti tecnici effettuati ?*

Art. 33, comma 4: Contenuti della notifica

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, **le informazioni possono essere fornite in fasi successive** senza ulteriore ingiustificato ritardo.

→ *Comunicare sempre il possibile entro 72 ore, poi effettuare comunicazioni successive*

Art. 33, comma 5: Contenuti della notifica

Il titolare del trattamento **documenta qualsiasi violazione dei dati personali**, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

→ *Registro delle violazioni, predisposizione modulistica appropriata*

Art. 34: Comunicazione di una violazione dei dati personali all'interessato

Art. 34, comma 1:

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 comunica la violazione all'interessato senza ingiustificato ritardo.

→ *Rischio elevato per gli interessati !!!*

Art. 34, comma 2:

La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un **linguaggio semplice e chiaro la natura della violazione dei dati personali** e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

→ *Dpo o Unità di crisi*
→ *Probabili conseguenze*
→ *Misure adottate per attenuare effetti negativi*

Art. 34, comma 3: non è richiesta comunicazine

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**;

→ *Cifratura e/o pseudonimizzazione*

Art. 34, comma 3: non è richiesta comunicazine

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 di cui al paragrafo 1;

→ *Misure ex post che hanno reso vana la violazione salvaguardando i dati*

Art. 34, comma 3: non è richiesta comunicazine

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a **una comunicazione pubblica** o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

→ *Conviene comunicarlo a tutto il mondo ?*

Art. 34, comma 4: non è richiesta comunicazine

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 o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

→ *Aspettare il garante ?*

Procedura di Data Breach

Procedura:

Predisporre e divulgare in azienda una **Procedura** che vada a spiegare come procedere in caso di data breach

→ *Procedura qualità*
→ *Procedura di gestione 27001*

Procedura:

Ogni incaricato autorizzato a trattare dati, qualora venga a conoscenza di un potenziale caso di data breach, deve avvisare tempestivamente il Rappresentante Legale o altro soggetto da lui delegato o designato (es. Amministratore di Sistema se interno, ICT Manager, Privacy Manager ...).

→ *Definire chi è il responsabile della crisi*

Procedura:

Quest'ultimo valuta col **DPO** (se presente) e con le figure aziendali che ritenga idonee la segnalazione ricevuta, la documenta, ai fini di una corretta classificazione dell'evento, utilizzando un apposito modulo all'uopo predisposto

→ *Modulistica*

Procedura:

Il criterio dirimente per valutare la necessità di avviare una procedura di notifica è la probabilità che la violazione possa **porre a rischio** (per la notifica all'autorità – Garante Privacy) o ad **elevato rischio** (per la comunicazione agli interessati) le libertà e i diritti degli individui

→ *Necessario definirlo ex ante in base alla tipologia di dati*

Procedura: Valutazione del rischio

Si possono presentare le tre seguenti situazioni in caso di violazione dei dati personali:

a) **improbabilità** che la violazione dei dati personali verificatasi presenti un rischio per i diritti e le libertà delle persone fisiche
In tal caso è necessario registrare la violazione e successivamente conservare il registro.
La notifica al Garante della Privacy non è obbligatoria ed è comunque necessario comprovare l'assenza dei rischi.

Procedura: Valutazione del rischio

b) **probabilità non elevata** che la violazione dei dati personali verificatasi presenti un rischio per i diritti e le libertà delle persone fisiche
In presenza di rischi per gli interessati è necessaria **la notifica entro 72 ore** al Garante della Privacy, utilizzando l'apposito o altra procedura resa disponibile sul sito de Garante.

Procedura: Valutazione del rischio

In tale evenienza bisogna:

- Raccogliere tutte le informazioni inerenti al Data Breach
- Inviare la notifica al Garante della Privacy
- Registrare la violazione
- Conservare il registro delle violazioni

Procedura: Valutazione del rischio

La notifica deve comprendere almeno:

- Una descrizione della violazione dei dati, compresi il numero delle persone interessate e le categorie di dati interessati;
- Il nome e i recapiti del DPO (Data Protection Officer o altro punto rilevante del contatto) se nominato;
- Le probabili conseguenze della violazione dei dati;
- Eventuali misure adottate dal titolare per porre rimedio o attenuare l'infrazione.

Procedura: Valutazione del rischio

I principali rischi possono essere ad esempio:

- danni fisici, materiali o immateriali alle persone fisiche
- perdita del controllo dei dati personali
- limitazione dei diritti, discriminazione
- furto di identità
- perdite finanziarie, danno economico
- decifratura non autorizzata della pseudonimizzazione
- pregiudizio alla reputazione
- perdita di riservatezza dei dati personali particolari (sanitari, giudiziari)

Procedura: Valutazione del rischio

Probabile presenza di un **elevato rischio** per i diritti e le libertà delle persone fisiche

In tale situazione bisogna:

- Raccogliere tutte le informazioni inerenti al Data Breach
- Inviare la notifica al Garante della Privacy
- **Comunicare ai diretti interessati del trattamento la violazione verificatasi**
- Gestire i riscontri da parte degli interessati
- Registrare la violazione
- Conservare il registro delle violazioni

Procedura: Valutazione del rischio

La notifica deve comprendere almeno:

- Una descrizione della violazione dei dati, compresi il numero delle persone interessate e le categorie di dati interessati;
- Il nome e i recapiti del DPO (Data Protection Officer o altro punto rilevante del contatto) se nominato;
- Le probabili conseguenze della violazione dei dati;
- Eventuali misure adottate dal titolare per porre rimedio o attenuare l'infrazione.

Procedura: Valutazione del rischio

La comunicazione agli interessati deve comprendere almeno:

- nome e recapiti del DPO (o altro punto rilevante del contatto) se nominato;
- le probabili conseguenze della violazione dei dati;
- eventuali misure adottate dal titolare per porre rimedio o attenuare l'infrazione.

Accountability del Data Breach

Accountability del Data Breach

Il WP 29 punta l'accento sul principio della **responsabilizzazione**.

In particolare precisa come **registrare le violazioni non notificabili, così come quelle notificabili,** è da far risalire tra gli obblighi del titolare del trattamento ai sensi dell'articolo 24, e che l'Autorità Garante possa chiedere di avere visione di tali registri.

Accountability del Data Breach

Nel GDPR non è specificato un **periodo di conservazione** per tale tipologia di documentazione. Laddove tali registrazioni contengano dati personali**, spetta al titolare del trattamento** determinare il periodo appropriato di conservazione in relazione al trattamento dei dati personali, tenendo conto altresì che tale documentazione potrebbe essere idonea prova di conformità ai requisiti del Regolamento e più in generale, al principio di responsabilità del Titolare.

Accountability del Data Breach

Chiaramente, se i “Data Breach record” non contengono dati personali, il principio di limitazione della conservazione del GDPR non si applica.

Ruolo del Responsabile del Trattamento nel Data Breach

Responsabile: non valuta il data breach

Il WP29 chiarisce che il Responsabile del trattamento **non è tenuto a valutare la probabilità di rischio** derivante da una violazione prima di informare il Titolare del trattamento; è infatti quest'ultimo a dover compiere tale valutazione diventando consapevole della violazione. Viene tuttavia raccomandato che il **responsabile avvisi tempestivamente** il Titolare, con ulteriori informazioni sulla violazione, anche fornite in fasi, man mano che ulteriori dettagli diventano disponibili.

Responsabile: deve verificare se vi è stato un data breach

Il Responsabile deve quindi **solo stabilire se si è verificata una violazione** e quindi informare il Titolare.

Il titolare usa il Responsabile per raggiungere i suoi scopi; pertanto, in linea di principio, il titolare del trattamento dovrebbe essere considerato “consapevole” una volta che il Responsabile lo ha informato della violazione

Responsabile: definirne attività nel contratto

Il Gruppo di lavoro precisa che il **contratto** tra il Titolare e il Responsabile del trattamento dovrebbe prevedere i requisiti che quest'ultimo debba rispettare ai fini di una comunicazione tempestiva al primo, a supporto degli obblighi del titolare del trattamento di riferire all'Autorità Garante entro 72 ore.