**Le nuove Linee Guida del Garante europeo sul Data Breach**

Il Garante europeo (*European Data Protection Board* – EDPB) il 28 marzo 2023 (*Guidelines 9/2022 on personal data breach notification under GDPR)*[1], terminata la fase di consultazione pubblica aperta lo scorso ottobre[2] che ha raccolto numerosi spunti, ha emanato la versione 2.0 delle nuove Linee Guida riguardanti la notifica dei *Data Breach*, che, di fatto, superano le disposizioni emanate in materia dal *Working Party ex art.29* poco dopo l'entrata in vigore definitiva del Regolamento UE sul trattamento dei dati delle persone fisiche (GDPR)

Tale intervento normativo è stato considerato opportuno sia per coordinare le linee guida e i *cases* derivanti dall'applicazione del GDPR sia per poter aggiornare la situazione sotto un profilo tecnologico.

Questo nuovo provvedimento si è reso particolarmente necessario perché erano sorte perplessità a livello europeo sulla modalità di notifica del *data breach* ai Garanti nazionali soprattutto in relazione al c.d. *"one-stop-shop"* che è un meccanismo secondo il quale la notifica è possibile ma solamente nei confronti di un'unica Autorità di controllo, cioè del Garante nazionale.

La modifica ha riguardato il paragrafo 70 e seguenti (in particolare il paragrafo 73) del precedente provvedimento che disciplinavano la situazione relativa ad un titolare del trattamento che non ha una sede all'interno dell'UE (pensiamo, per esempio a soggetto statunitense che non ha stabilito una propria rappresentanza nell'Unione europea) e la normativa prevedeva che, in questo caso, per un eventuale *data breach*, il Garante al quale andava inviata la notifica era quello dei cittadini i cui dati erano stati oggetto della violazione.

Per questi titolari, in base alle nuove linee guida, si esclude l'applicazione del principio di *one-stop-shop* per l'individuazione dell'autorità di controllo capofila, previsione coerente con quanto era già previsto dalle linee guida WP244[3] e EDPB 3/2018[4].

La novità, quindi, consiste nell'obbligo di notificare il *data breach*, non più ad una sola Autorità di controllo (appunto l'*"one-stop-shop"*) come sopra ricordato, ma a tutti i Garanti dei vari paesi i cui cittadini sono stati coinvolti nella violazione dei dati.

Questa nuova indicazione ha delle conseguenze sui tempi di notifica della violazione in quanto presuppone che il titolare sia in grado di distinguere immediatamente dall'analisi dell'accaduto, e quindi entro le 72 ore, come vedremo successivamente, la riferibilità territoriale relativi ai dati delle persone fisiche raccolti e trattati ma che sono stati oggetto del data breach.

Le nuove linee guida modificano anche il diagramma del flusso operativo (Allegato VII precedente e rappresentato in calce) che deve essere rispettato dagli operatori al momento in cui avviene una *data breach.*

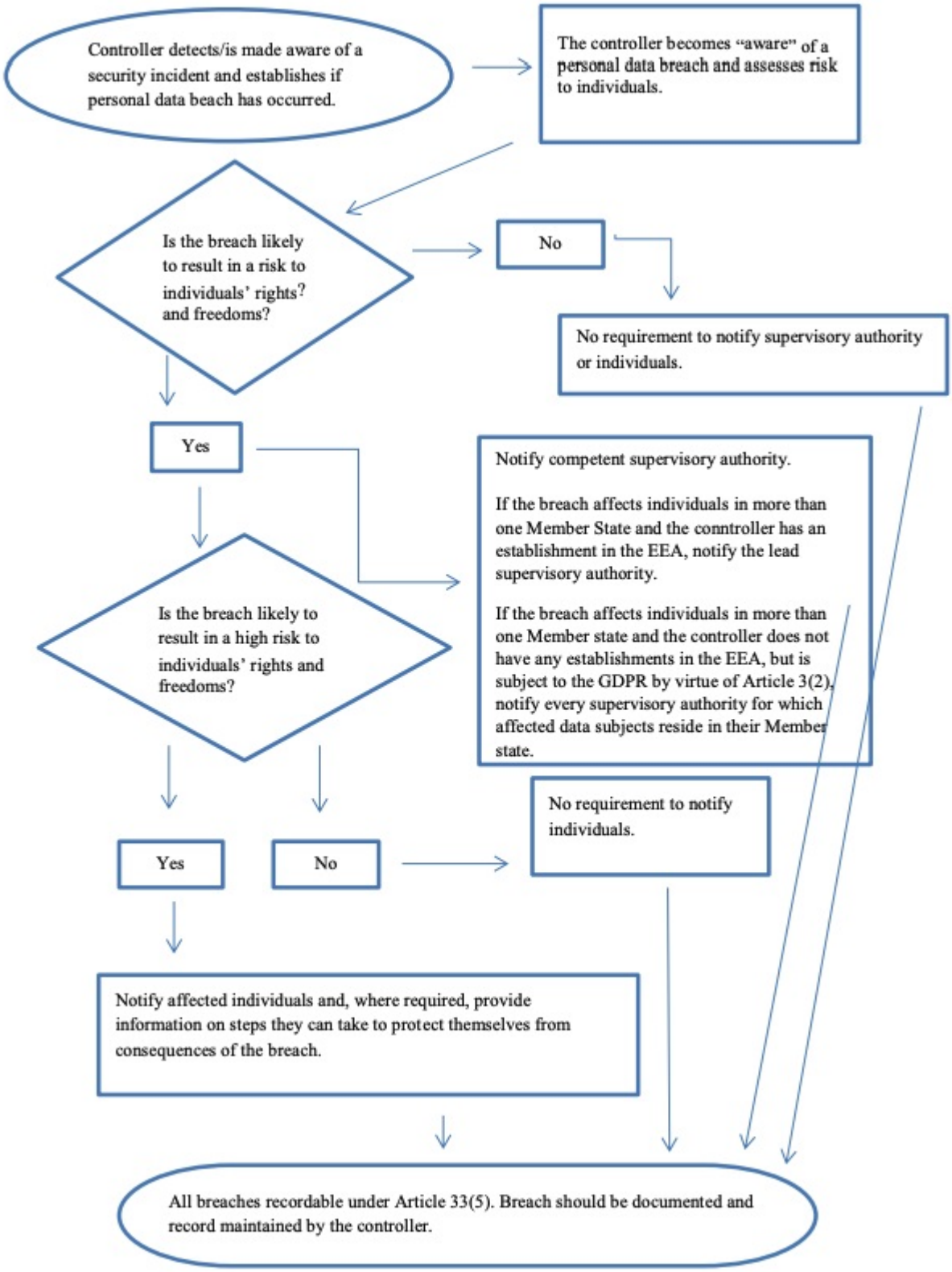
---

*[1] - "Adoption of the Guidelines following the targeted public consultation on the subject of data breach notification for controllers not established in the EEA."*

[2] - 10 October 2022 - "*Adoption of the Guidelines (updated version of the previous guidelines WP250 (rev.01) adopted by the Working Party 29 and endorsed by the EDPB on 25 May 2018) for a targeted public consultation."*

*[3] - Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - Adottate il 13 dicembre 2016 - Versione emendata e adottata in data 5 aprile 2017.*

[4] - *Linee-guida 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3)*




**I tempi di notifica di un *Data Breach***

Come è noto l'art. 33 GDPR (*"Notifica di una violazione dei dati all'autorità di controllo"*) stabilisce che *"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"*.

La problematica che è stata sollevata nel corso di questi anni ha riguardato, in modo particolare, l'inizio del periodo delle 72 ore, cioè da quando decorre il tempo per notificare al garante e ai soggetti interessati l'avvenuto *data breach* ed in proposito i Garanti europei individuano dei punti fermi.

Innanzitutto, le Linee guida considerano la situazione in cui il titolare avendo predisposto *"misure tecnico-organizzative a protezione dei dati*", ha immediata conoscenza dell'avvenuta violazione dei dati, che secondo i Garanti europei è la fattispecie *standard* per dimostrare di essere *compliance* con le norme regolamentari.

Diversa è invece la situazione in conseguenza della quale il titolare viene a conoscenza dell'accaduto in un tempo più lungo da quando è avvenuto il *data breach*, e in questo caso, secondo l'organismo europeo, siamo di fronte ad un *"indice di scarsa o inadatta organizzazione aziendale in termini di conformativa normativa e implementazione di misure tecniche a protezione dei dati"*: in buona sostanza il titolare non è *compliance* e quindi non rispettando il "*principio di accountability*", termine che nel nostro ordinamento ha assunto il significato di "*responsabilizzazione*", può incorrere anche in eventuali sanzioni.

Quindi, secondo le nuove Linee guida, il momento da cui inizia a decorrere il periodo di 72 ore *ex* art. 33 GDPR, è quello in cui il titolare ha, di fatto, rilevato con certezza la violazione dei dati.

Il provvedimento dei Garanti europei, include anche una sorta di elenco di violazione dei dati sia essa formale o sostanziale. Come esempio viene indicata una ipotesi di una *"breve interruzione della fornitura di energia elettrica"* che per qualche minuto potrebbe, di fatto, impedire la normale attività con la conseguenza di un rischio di perdita accidentale di dati.

Un ulteriore esempio contenuto nelle Linee guida riguarda dati già disponibili o dati crittografati, a proposito dei quali l'*European Board* ricorda che solo l'utilizzo di una crittografia *"sicura"* impedisce l'accesso ai dati a soggetti non autorizzati all'accesso stesso, ma questo è possibile solo se i titolari, hanno una specifica conoscenza dei sistemi di crittografia. Relativamente a quest'ultima affermazione credo che ogni commento sia inutile!!!

**La procedura per la segnalazione all'Autorità di controllo**

Un adempimento importante nel procedimento che può concludersi con la segnalazione della violazione al Garante consiste nella registrazione del fatto nel registro data breach in relazione al quale il Garante europeo mantiene una linea rigida e ferma imponendo l'iscrizione nel registro di tutte le violazioni dei dati personali da quella più formale a quella più significativa.

Ricordando l'esempio di cui sopra relativo ad una breve interruzione di energia elettrica, l'EDPB non prescrive in questo caso né la notifica all'Autorità né la comunicazione agli interessati i cui dati siano stati compromessi, ma stabilisce che sia necessario inserire tale situazione nel registro dei *data breach* indicando le relative circostanze.

Nel momento in cui il titolare è a conoscenza dell'avvenuta violazione deve attivarsi per comprendere ed essere il più sicuro possibile se il *data breach*

- possa produrre un rischio per i diritti e le libertà dei soggetti che sono interessati dalla violazione, circostanza che comporta la semplice registrazione della compromissione dei dati nel registro dei *data breach*.
- possa produrre un rischio per i diritti e le libertà dei soggetti coinvolti dalla violazione, circostanza che comporta la registrazione della compromissione dei dati nel registro dei *data breach* e la notifica al Garante.
- nel caso in cui produca un rischio elevato per i diritti e le libertà dei soggetti interessati, si ha come conseguenza la registrazione della compromissione nel registro dei *data breach*, la notifica all'autorità garante e la comunicazione agli interessati coinvolti nella compromissione.

Considerando, altresì, che la eventuale comunicazione agli interessati i cui dati possono esseri stati compromessi deve avvenire senza ingiustificato ritardo.

Inoltre, secondo l'EDPB, il titolare deve tenere anche conto:

- del tipo di violazione avvenuta, la sua natura, la tipologia dei dati (per esempio dati comuni oppure dati appartenenti a particolari categorie o dati giudiziari), e la quantità dei dati che sono stati eventualmente violati e compromessi
- della facilità che hanno avuto i soggetti terzi che hanno violato i dati di accedere agli stessi e, eventualmente, anche di identificare i soggetti i cui dati sono stati oggetto di violazione.
- di quali possono essere le possibili conseguenze per i soggetti interessati.
- delle caratteristiche particolari relative ai soggetti coinvolti (per esempio se i dati sono relativi a minori oppure a soggetti vulnerabili) e di quelle del titolare (per esempio un ospedale)
- del numero dei soggetti interessati che sono coinvolti nel *data breach.*

Ma oltre alla valutazione del rischio, il titolare deve anche individuare quale siano le procedure da mettere in atto per contenere il rischio stesso, sia relativamente alla violazione in essere cercando di contenere il più possibile il rischio per gli interessati coinvolti nel *data breach*, ma anche per evitare che un incidente che attiene alla sicurezza dei dati possa ripetersi nel futuro.

Da questo punto di vista, l'*European Board* sottolinea come anche una violazione rivelatasi innocua, può rendere necessario un intervento correttivo molto incisivo.

**La comunicazione agli interessati**

Come sopra ricordato, qualora il titolare, a causa della violazione dei dati di persone fisiche, sia di fronte ad un rischio elevato per le libertà ed i diritti degli interessati, deve procedere alla comunicazione della violazione agli interessati coinvolti.

Ma cosa deve essere comunicato agli interessati che sono stati vittime della violazione dei dati? E come deve avvenire tale comunicazione?

Secondo il Garante europeo per comunicare, agli interessati coinvolti, il *data breach*, bisogna usare un linguaggio semplice e chiaro (*"describe in clear and plain language"*), per indicare loro:

a. la natura della violazione dei dati personali;
b. i dati di contatto del DPO (*Data Protection Officer* o Responsabile della protezione dei dati, nella traduzione italiana, identificato con l'acronimo RPD) o di altro punto di contatto da cui ottenere maggiori informazioni;
c. le probabili conseguenze della violazione;
d. le misure intraprese o da intraprendere per contenerne gli effetti negativi, comprese le indicazioni per gli individui interessati quale, per esempio se necessario, l'immediato reset delle proprie credenziali di autenticazione informatica.

Il Garante europeo, inoltre, al fine di evitare una minimizzazione della situazione, precisa che:

- bisogna evitare che le comunicazioni di *data breach* non siano simili alle comunicazioni ordinarie, per esempio mediante *newsletter* a cadenza regolare una comunicazione di questo tipo;
- meglio utilizzare comunicazioni dirette che indirette, per esempio inviando specifiche e-mail piuttosto che un comunicato stampa. Tale osservazione è condivisibile ma si deve tener conto, anche per esperienza professionale, che ciò non è sempre possibile soprattutto quando i soggetti interessati sono un numero rilevante (nel caso di specie, si trattava di un *data breach* di dati relativi ai bambini iscritti in numero elevato ad una mensa scolastica). In questo caso può essere utile utilizzare più mezzi di comunicazione per garantire una diffusione significativa.

**E il DPO?**

Le Linee guida definiscono anche quale sia il ruolo del DPO in caso di eventuale *data breach.* In particolare, il problema si ha in relazione alla compatibilità fra la di *Data Protection Officer* e quella del rappresentante di un titolare

con sede *extra-Ue*. Secondo l'European Board le due funzioni non sono compatibili e quindi chi deve notificare il *data breach* è il titolare del trattamento e il DPO "europeo" al massimo può essere coinvolto nel procedimento di notifica nel caso in cui questa funzioni rientri nelle sue competenze.

Questa figura, come è noto, svolge un ruolo fondamentale (non sempre compreso dai titolari) per garantire il rispetto della normativa sulla *privacy*, e, in caso di *data breach* deve fornire assistenza, consulenza e informazione al titolare per essere *compliance* anche in questa situazione e, se del caso, anche fornendo pareri specifici in relazione alla violazione dei dati soprattutto per quanto attiene l'eventuale impatto sull'organizzazione dell'ente.

Il ruolo che ha il DPO nell'eventualità di un *data breach* è del tutto evidente anche per il fatto che in caso di violazione del trattamento dei dati, il titolare quando notifica al proprio Garante tale accadimento deve indicare sempre i dati di contatto con il DPO in modo che questo possa essere il punto di congiunzione fra titolare e Autorità di controllo.

Infine, secondo quanto prevedono le Linee Guida qui in commento, è possibile affidare al DPO la tenuta del registro dei *data breach*, anche se tale compito non è previsto dal Regolamento Ue che invece individua le funzioni specifiche del DPO.

In relazione a quest'ultima ipotesi sarebbe opportuno un intervento legislativo a livello comunitario perché si rischia di avere un possibile "contenzioso" allorché un ente volesse affidare tale funzione al proprio DPO e questi si rifiuti in quanto ritiene che tale compito non è previsto dal GDPR.

**Stefano PAOLI**