Ministero dell'Istruzione e del Merito

Dipartimento per le risorse umane, finanziarie e strumentali
Direzione Generale
per la progettazione organizzativa, l'innovazione dei processi amministrativi, la comunicazione e i contratti
Ufficio III – Protezione dei dati personali del Ministero

All'Ufficio di Gabinetto

SEDE

Al Dipartimento per le risorse umane,
finanziarie e strumentali
SEDE

Al Dipartimento per il sistema educativo
di istruzione e di formazione
SEDE

Ai Direttori Generali dell'Amministrazione centrale
LORO SEDI

Ai Direttori Generali e ai Dirigenti titolari
degli Uffici scolastici regionali
LORO SEDI

e, p.c., Al *Computer Security Incident Response Team* (CSIRT) del Ministero
SEDE

OGGETTO: Obblighi di notifica in caso di violazione dei dati personali (c.d. *"data breach"*) - Novità introdotte dalla versione aggiornata delle Linee Guida n. 09/2022 del Comitato Europeo per la Protezione dei Dati

Con la presente si informano gli Uffici in indirizzo del fatto che, nel primo semestre del 2023, il Comitato Europeo per la Protezione dei Dati, organismo indipendente dell'UE istituito per garantire un'applicazione coerente del Regolamento Generale sulla Protezione dei Dati, noto anche come EDPB (acronimo inglese di "*European Data Protection Board*"), dopo una fase di consultazione pubblica preventiva avviata ad ottobre 2022, ha pubblicato la versione aggiornata delle Linee Guida n. 09/2022 sulla gestione e la notifica delle violazioni di dati personali (c.d. *"data breach*").

La prima versione del documento in questione (all. n. 1) era stata approvata poco dopo l'entrata in vigore del Regolamento UE 2016/679 (di seguito, anche "Regolamento" o "GDPR") ma, con il tempo, si sono rese necessarie talune modifiche al fine di aggiornare, allo stato dell'arte della tecnologia, le indicazioni fornite in passato e di armonizzare la pubblicazione alla casistica sviluppatasi in vigenza del GDPR.

Attraverso tale intervento di aggiornamento, l'EDPB (di seguito, anche "Comitato" o "Board") ha inteso quindi proseguire il percorso iniziato subito dopo l'entrata in vigore del Regolamento, con l'obiettivo di fare chiarezza sugli obblighi di notifica che sussistono, rispetto alle Autorità Garanti e agli interessati, nel caso in cui si verifichi una violazione dei dati personali (di seguito, anche "*data breach*"), allo scopo di supportare i Titolari e Responsabili del trattamento nella gestione degli incidenti di sicurezza eventualmente occorsi all'interno delle proprie organizzazioni.

Nel trasmettere agli Uffici in indirizzo il documento in parola, allo stato disponibile unicamente nella versione in lingua inglese (all. n. 2), si reputa utile offrire di seguito una panoramica delle principali novità introdotte in materia, con un richiamo anche ai più significativi aspetti già affrontati in precedenza dal Comitato e ribaditi nella versione aggiornata della pubblicazione.

Premesse generali in tema di violazione dei dati personali

Analizzando i punti salienti della versione 2.0 delle Linee Guida, emerge innanzitutto la volontà del Board di chiarire alcuni aspetti legati ai principi statuiti dal Regolamento in tema di violazione dei dati personali.

Com'è noto, il GDPR fornisce una definizione precisa della nozione di "*violazione dei dati personali*".

Secondo l'art. 4, n. 12 del Regolamento costituisce violazione di dati personali ogni "*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*".

In sostanza, una violazione di dati personali o *data breach* costituisce un incidente di sicurezza che abbia coinvolto dati personali e dal quale possano derivare rischi per gli interessati.

Da tanto discende che, mentre ogni *data breach* rappresenta sempre la conseguenza più severa di un incidente di sicurezza (*security incident*), non ogni incidente di sicurezza è destinato a sfociare in un'effettiva violazione di dati e, quindi, a dare luogo a un *data breach*.

Ebbene, nel soffermarsi sul punto, il Comitato ha ritenuto utile ricordare come le violazioni di dati personali possano essere classificate in tre diverse tipologie connesse alla sicurezza delle informazioni (c.d. Triade R.I.D.):

- violazione della *riservatezza*, in caso di divulgazione dei dati personali o accesso agli stessi non autorizzato o accidentale;
- violazione dell'*integrità*, in caso di modifica non autorizzata o accidentale dei dati personali;
- violazione della *disponibilità*, in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Ribadendo quanto già osservato nelle precedenti edizioni delle Linee Guida, l'EDPB ha inoltre osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi loro combinazione.

Come rammentato dal Comitato, nel caso in cui si verifichi una violazione dei dati personali è necessario indagare tempestivamente su quanto accaduto, al fine di identificare le caratteristiche dell'evento negativo, per poterlo classificare e valutare.

La classificazione e la valutazione dell'incidente occorso costituiscono, infatti, un passaggio indispensabile per poter affrontare il *data breach* in modo adeguato e conforme alla normativa, perché è sulla base delle valutazioni effettuate dal Titolare che dovranno essere definiti gli *step* successivi da seguire.

Qualora, infatti, dalle verifiche effettuate emerga la sussistenza di un potenziale rischio per i diritti e le libertà delle persone fisiche, l'art. 33 del Regolamento richiede al Titolare del trattamento di notificare la violazione all'Autorità Garante competente senza ingiustificato ritardo e, ove possibile, non oltre le 72 ore dal momento in cui sia venuto a conoscenza della violazione dei dati personali.

Nel caso in cui, poi, la violazione dei dati personali sia suscettibile di presentare un rischio non soltanto probabile, ma elevato per i diritti e le libertà delle persone fisiche, all'onere di notifica all'Autorità di controllo si aggiunge per il Titolare, ai sensi dell'art. 34 del GDPR, anche quello di dare comunicazione della violazione agli interessati, senza ingiustificato ritardo.

L'evento identificato, analizzato ed eventualmente notificato e comunicato deve inoltre essere sempre riportato nel Registro delle violazioni (noto anche come "Registro degli incidenti di sicurezza" o "Registro dei *data breach")*, per poter tenere traccia delle violazioni subite, in un'ottica di responsabilizzazione della organizzazione (c.d. *accountability*).

Il corretto adempimento degli obblighi sopra descritti riveste fondamentale importanza ai fini della protezione dei diritti degli interessati e l'inosservanza delle disposizioni richiamate è sanzionata a norma dell'art. 83 GDPR.

Una violazione di dati personali può, del resto, se non affrontata in modo adeguato e tempestivo provocare agli interessati danni fisici, materiali e immateriali, come la limitazione dei diritti, la discriminazione, il furto o l'usurpazione di identità, un pregiudizio alla reputazione e/o altri nocumenti di natura tanto economica, quanto sociale.

Proprio per tale ragione, nella nuova versione delle Linee Guida, il Board ha ritenuto indispensabile fornire ulteriori chiarimenti e indicare nuovi esempi pratici che possano orientare al meglio i Titolari e i Responsabili del trattamento nella gestione di eventuali *data breach*.

Le principali novità introdotte

I tempi di notifica del *data breach* nelle nuove Linee Guida

Le nuove Linee Guida EDPB mettono innanzitutto alcuni punti fermi in merito ad una circostanza essenziale nello sviluppo diacronico delle procedure relative alla gestione delle violazioni dei dati, ovvero il momento dal quale decorrono i ristretti termini per la notifica all'Autorità Garante (entro 72 ore) e per la comunicazione agli interessati (da effettuarsi senza ingiustificato ritardo).

Come si è avuto modo di anticipare in precedenza, l'articolo 33 del GDPR specifica 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 tempestività, infatti, come sopra accennato, assume rilievo fondamentale nelle procedure di notifica dei *data breach*.

In tale prospettiva, risulta decisivo individuare il momento dal quale decorrono le 72 ore per la notifica della violazione all'Autorità di controllo competente (in Italia, il Garante per la Protezione dei Dati Personali – di seguito, anche "Garante" o "GPDP").

Nell'intervenire sul punto l'EDPB si è preoccupato di sgomberare il campo da possibili usi distorti della normativa, ricordando che i principi generali del GDPR impongono ai Titolari l'adozione di misure tecnico-organizzative a protezione dei dati tali da consentire di venire a conoscenza delle violazioni in tempi rapidi.

In considerazione di ciò è quindi indispensabile scongiurare situazioni di tardiva rilevazione di eventuali violazioni di dati personali intervenute, in quanto le stesse sono considerate indice di scarsa o inadatta organizzazione dell'Ente in termini di conformità alla normativa vigente, nonché di implementazione di misure di sicurezza a tutela dei dati personali

degli interessati e, come tali, si rivelano potenzialmente idonee a costituire autonoma fonte di sanzione.

Tuttavia, resta fermo il principio per cui l'obbligo di notifica sorge in concreto nel momento in cui il Titolare diventi "consapevole" del *data breach.*

La precisa individuazione di questo momento varia da caso a caso, poiché dipende dalle circostanze specifiche della violazione, che possono richiedere ulteriori indagini, nonché notificazioni *follow up* all'Autorità Garante.

Ebbene, al fine di supportare i Titolari e i Responsabili del trattamento nella corretta individuazione di tale momento, il Board, nel puntualizzare che un Titolare o un Responsabile del trattamento può considerarsi "*a conoscenza*" della violazione quando abbia conseguito un "*ragionevole grado di certezza che la violazione si sia verificata*" e che abbia causato una compromissione di dati personali, ha ritenuto utile indicare, a titolo esemplificativo, una serie di "*situazioni-tipo*" reputate idonee a far cogliere con maggiore chiarezza i momenti di conoscenza di eventuali violazioni nella prassi.

Ad esempio, è stato evidenziato come il Titolare e/o il Responsabile del trattamento possa considerarsi "*a conoscenza*" della violazione nel caso in cui:

- abbia ricevuto una e-mail da un utente che lo abbia avvisato di essere stato contattato da un soggetto terzo che impersonava il Titolare e che possa verosimilmente aver avuto accesso ai dati dell'organizzazione del Titolare medesimo;
- sia stata condotta una rapida indagine in grado di suffragare la segnalazione dell'utente, attraverso l'acquisizione di prove puntuali di un'intromissione nel sistema.

Oppure, quando:

- un terzo lo informi di aver ricevuto da suoi dipendenti/operatori, per errore, una comunicazione contenente i dati personali di altri utenti e fornisca la prova dell'intervenuta divulgazione non autorizzata (in tal caso, dal momento che il Titolare del trattamento è stato reso edotto, anche attraverso il supporto di prove evidenti, di una violazione della riservatezza, non possono sussistere dubbi circa il fatto che la stessa si sia verificata e che il Titolare stesso ne sia venuto a conoscenza).

O, ancora:

- in caso di smarrimento di una chiavetta USB contenente dati personali non criptati gestiti dall'organizzazione del Titolare (in tale evenienza, infatti, non essendo effettivamente possibile constatare con assoluta certezza se persone non autorizzate abbiano avuto o meno accesso a tali dati, si deve presumere un accesso non autorizzato possa essersi determinato).

Da quanto illustrato, emerge, dunque, come il momento esatto "di presa coscienza" da parte del Titolare e/o del Responsabile possa variare in base alle circostanze.

La conoscenza dovrà considerarsi immediata in tutti quei casi in cui il Titolare del trattamento dati sia stato informato di una violazione, tramite segnalazione documentata di un terzo, ovvero abbia rilevato, direttamente e/o per il tramite del Responsabile del trattamento eventualmente designato, l'evento.

Diversamente, potrebbero ricorrere situazioni in cui la consapevolezza/conoscenza della violazione non possa dirsi immediata, rendendosi necessario l'espletamento di apposite indagini volte ad appurare se il *data breach* abbia effettivamente avuto luogo.

In tali evenienze, secondo quanto affermato dall'EDPB, il Titolare del trattamento non può considerarsi pienamente "consapevole" *ab origine*. È, tuttavia, necessario che, in siffatte ipotesi, le indagini iniziali vengano avviate dal Titolare il prima possibile e siano quanto più dettagliate possibile per permettere di stabilire rapidamente e con un ragionevole grado di certezza la sussistenza e la gravità della violazione.

Da ultimo, va rammentato come, per quanto il Titolare conservi una responsabilità generale in tema di protezione dei dati personali, un ruolo rilevante nel consentire a quest'ultimo di adempiere ai propri obblighi in materia di rilevazione, verifica e notifica dei *data breach*, sia riconosciuto anche al Responsabile del trattamento (es. fornitore esterno) eventualmente nominato.

L'art. 28, paragrafo 3, del GDPR, nello stabilire che il ruolo del Responsabile del trattamento debba essere disciplinato da un contratto o da un altro atto giuridico, precisa, alla lettera f), che detto contratto o altro atto giuridico deve prevedere che il Responsabile del trattamento "*assista il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento*".

L'articolo 33, paragrafo 2, del GDPR chiarisce inoltre che, se il Titolare ricorre a un Responsabile del trattamento e quest'ultimo viene a conoscenza di una violazione dei dati personali che sta trattando per conto del Titolare, deve notificarla al Titolare "*senza ingiustificato ritardo*".

Va, inoltre, evidenziato che il Responsabile del trattamento non deve valutare la probabilità del rischio sui diritti e le libertà delle persone fisiche prima di notificare la violazione al Titolare. Spetta, infatti, a quest'ultimo effettuare tale valutazione nel momento in cui viene a conoscenza del *data breach*. Il Responsabile del trattamento è tenuto soltanto verificare se sia occorsa una violazione e notificarla al Titolare.

La valutazione del rischio a seguito di *data breach* nelle nuove Linee Guida

In linea con l'orientamento adottato nella versione 1.0 il Comitato, in occasione dell'aggiornamento delle Linee Guida, ha rimarcato anche che il Titolare, una volta che sia venuto a conoscenza di un *data breach*, è tenuto a valutare il rischio che tale violazione comporti per i diritti e le libertà delle persone fisiche coinvolte dal trattamento dei dati e a vagliare, caso per caso, la necessità o meno della notifica al Garante, nonché della comunicazione agli interessati.

Il Titolare è chiamato, dunque, a classificare la violazione, stabilendo se la stessa sia effettivamente suscettibile di comportare o meno un rischio per i diritti e le libertà degli interessati coinvolti e, nel primo caso, se si tratti o meno di un rischio elevato. Laddove, invece, risulti improbabile che la violazione dei dati personali possa generare rischi per i diritti e le libertà delle persone fisiche, il titolare può decidere di non inoltrare la notifica.

In caso di *data breach*, quindi, la misura del rischio va determinata in funzione dei seguenti due distinti elementi:

- **probabilità**: da intendersi come grado di effettiva possibilità che si verifichino uno o più eventi temuti (es. la perdita totale dei dati);
- **gravità**: da intendersi come rilevanza del rischio, in termini di effetti pregiudizievoli che lo stesso è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati).

A seconda della probabilità e del grado del rischio rilevato, il Titolare dovrà quindi:

1. Notificare la violazione dei dati personali all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui sia venuto a conoscenza della stessa, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro le 72 ore, è necessario che la stessa sia corredata dei motivi del ritardo;
2. Comunicare all'interessato la violazione dei dati personali senza ingiustificato ritardo, nel caso in cui la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
3. Riportare l'evento nel Registro delle violazioni (tale ultima attività dovrà essere compiuta a prescindere, sia nel caso in cui il Titolare abbia provveduto alla notifica e/o alla comunicazione dell'incidente di sicurezza, sia quando la violazione subita non presenti alcun rischio per i diritti e le libertà dei soggetti coinvolti - es.: breve

interruzione della fornitura di energia elettrica o compromissione di dati già pubblicamente disponibili).

Al fine di vagliare la gravità del rischio, il Comitato suggerisce ai Titolari di tenere conto dei seguenti fattori:

a. il tipo di violazione occorsa;
b. la natura, la tipologia (es. dati comuni ovvero appartenenti a categorie particolari o relativi a condanne penali o reati) e il volume dei dati compromessi;
c. la facilità per soggetti terzi non autorizzati di identificare gli individui i cui dati sono stati compromessi;
d. le possibili conseguenze per gli individui;
e. le caratteristiche peculiari degli individui coinvolti (es. nel caso di minori o individui vulnerabili);
f. le caratteristiche peculiari del Titolare (es. se si tratta di una struttura sanitaria);
g. il numero di interessati coinvolti.

Ad ogni modo, secondo il Board, sussistono rischi per gli interessati quando il *data breach* possa causare agli stessi un danno fisico, materiale o immateriale. Nell'effettuare quest'analisi, è bene, quindi, che siano considerate e tenute presenti anche tutte le possibili conseguenze secondarie della violazione, che potrebbero produrre impatti significativi nella vita degli interessati.

Suggerimenti per la notifica all'Autorità di controllo

Come sottolineato dal Board nelle Linee Guida, scopo della notifica non è soltanto quello di ottenere indicazioni dall'Autorità Garante circa l'opportunità di comunicare o meno la violazione agli interessati.

In alcuni casi, del resto, può risultare immediatamente evidente, in considerazione della natura della violazione e della gravità del rischio, la necessità di effettuare tale comunicazione, senza indugio, in favore delle persone interessate.

Ad esempio, nel caso in cui sia rilevata una minaccia immediata di furto d'identità, oppure nell'eventualità in cui siano state divulgate *online* categorie particolari di dati personali, non possono sussistere dubbi sul fatto che il Titolare del trattamento debba agire senza ritardo per contenere la violazione e per informare prontamente dell'accaduto le persone coinvolte.

In circostanze eccezionali e di particolare gravità, inoltre, tale comunicazione potrebbe dover essere effettuata addirittura prima della notifica del *data breach* all'Autorità di controllo.

In ogni caso, va tenuto presente che la notifica al Garante non può fungere da giustificazione per la mancata comunicazione della violazione all'interessato, laddove la comunicazione risulti con ogni evidenza necessaria.

Obiettivo precipuo dell'obbligo di notifica è, invero, quello di incoraggiare il Titolare del trattamento ad agire rapidamente in caso di *data breach*, al fine di contenerlo e, se possibile, di recuperare tempestivamente i dati personali compromessi.

Per tale ragione, l'art. 33 del GDPR, al paragrafo 1, richiede al Titolare di procedere alla notifica all'Autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, non oltre 72 ore dal momento in cui sia venuto a conoscenza della violazione.

L'anzidetta disposizione normativa, tuttavia, al successivo paragrafo 4, aggiunge altresì che: "*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*."

Il Regolamento, quindi, prende anche atto del fatto che non sempre sono acquisibili, nel ristretto termine indicato dalla norma, tutte le informazioni necessarie su un incidente di sicurezza.

In considerazione di ciò, il Board, nella nuova versione delle Linee Guida, ha riproposto una serie di indicazioni utili per l'eventualità in cui il Titolare non entri immediatamente in possesso di tutti gli elementi utili per effettuare una descrizione completa ed esaustiva del *data breach* occorso, con un *focus* particolare sull'ipotesi in cui la notifica venga effettuata in ritardo.

L'EDPB ha ricordato, innanzitutto, come il Regolamento, nel prevedere che le informazioni possano essere fornite in fasi successive senza ulteriore ingiustificato ritardo, consenta al Titolare di procedere, laddove necessario, ad una notifica "per fasi", da attuarsi attraverso una prima e rapida notifica di *alert* (in occasione della quale il Titolare del trattamento deve comunque aver cura di informare l'Autorità del contenuto solo parziale della segnalazione), seguita dalla comunicazione di tutte le informazioni aggiuntive acquisite, attraverso l'invio di successive notifiche integrative.

Non va, inoltre, dimenticato che, anche dopo aver completato le attività di notifica, il Titolare ha comunque la facoltà di aggiornare l'Autorità di controllo, fornendo eventuali ulteriori dettagli di cui sia venuto a conoscenza nel tempo. Ciò a maggior ragione nel caso in cui, nel corso dell'indagine, venga appurato che l'incidente verificatosi sia stato contenuto e che non si sia effettivamente verificata alcuna violazione dei dati.

Queste informazioni, infatti, ben possono essere aggiunte a quelle già fornite all'Autorità di controllo, con conseguente registrazione dell'incidente come una non-violazione (o "falso positivo").

Non è prevista, del resto, come precisato dal Board, alcuna sanzione per il caso in cui venga effettuata una segnalazione di un incidente che successivamente, non avendo effettivamente dato luogo ad alcuna violazione, si riveli essere un falso positivo.

Passando poi alle notifiche effettuate in ritardo, il Comitato ha rimarcato come qualora la notifica all'Autorità di controllo non venga effettuata entro le 72 ore indicate dal GDPR, essa debba essere accompagnata dall'indicazione documentata dei motivi del ritardo.

Il Regolamento prevede, altresì, la possibilità di effettuare una "notifica differita" dopo le 72 ore previste dall'articolo 33 nel caso in cui, ad esempio, si subiscano violazioni ripetute, ravvicinate e di simile natura che interessino un numero elevato di soggetti. Al fine di evitare un aggravio di oneri in capo al Titolare e l'invio dilazionato di un numero elevato di notificazioni tra loro identiche, il Titolare è autorizzato ad eseguire un'unica "notifica aggregata" di tutte le violazioni occorse nel breve periodo di tempo (anche se superi le 72 ore), purché la notifica motivi le ragioni del ritardo.

E' stato, inoltre, ribadito che, nel caso in cui il Titolare ometta di notificare una violazione dei dati all'Autorità di controllo o agli interessati, oppure a entrambi, nonostante siano soddisfatte le prescrizioni di cui agli articoli 33 e/o 34 del Regolamento, l'Autorità Garante potrebbe venirsi a trovare nella condizione di dover prendere in considerazione tutte le misure correttive a sua disposizione, tra cui l'irrogazione di una sanzione amministrativa pecuniaria appropriata in associazione a una misura correttiva ai sensi dell'articolo 58, paragrafo 2, del Regolamento, oppure come sanzione indipendente.

La comunicazione del Titolare agli interessati

Un altro degli aspetti chiave da considerare in caso di *data breach* è l'eventuale raggiungimento del livello di "allarme" più elevato, che ricorre nel caso in cui venga rilevato un rischio elevato per le libertà ed i diritti degli interessati e si debba quindi procedere alla comunicazione della violazione agli interessati coinvolti.

L'EDPB, nell'intervenire sul punto, ha fornito talune indicazioni rispetto alla comunicazione che il Titolare deve rivolgere agli interessati vittime di *data breach*.

In particolare, il Board ha precisato che:

- la comunicazione relativa ad un *data breach* deve essere data utilizzando un linguaggio semplice e chiaro, volto a specificare la natura della violazione, i dati di contatto del DPO o di altro punto di contatto da cui ottenere maggiori informazioni, le possibili conseguenze della violazione, le misure messe in atto dal Titolare per contenere danni e rischi (ivi inclusi consigli agli individui interessati per mitigare gli effetti della violazione, come ad esempio un repentino aggiornamento delle credenziali);

- la comunicazione in questione non deve essere confondibile con le comunicazioni "ordinarie" del Titolare. Ad esempio, non è lecito "nascondere" una comunicazione di *data breach* all'interno di una *newsletter* periodica;
- l'avviso deve essere fornito con il mezzo di comunicazione più efficace (a meno che tale soluzione non comporti uno sforzo sproporzionato in capo al Titolare);
- è preferibile utilizzare comunicazioni dirette rispetto a quelle indirette: una e-mail risulta avere maggiore efficacia rispetto ad un comunicato stampa, oltre ad essere uno strumento più idoneo a veicolare la comunicazione ad una pluralità di soggetti;
- in ogni caso, è fondamentale che il Titolare si adoperi per "moltiplicare" gli strumenti utilizzati per far circolare l'informazione, così da garantirne la massima diffusione (ad esempio fornendo la notizia su tutti i canali *social* dell'organizzazione, oltre che sul relativo sito istituzionale e a mezzo stampa).

Il meccanismo dello Sportello Unico (c.d. "*one-stop-shop*")

Le modifiche apportate in sede di aggiornamento del documento hanno interessato inoltre, in particolare, i paragrafi 70 e seguenti delle Linee Guida, che sono incentrati sul meccanismo dello Sportello Unico o del c.d. "*One Stop Shop*".

Con tale espressione si fa riferimento a una delle principali novità introdotte dal GDPR allo scopo di assicurare l'applicazione uniforme delle norme in materia di protezione dei dati personali nel territorio dell'Unione Europea.

Per i trattamenti di dati personali transfrontalieri – ovvero quei trattamenti realizzati da un Titolare che possieda sedi e stabilimenti situati in più Stati membri, ovvero che, pur avendo un'unica sede nel territorio UE, effettui trattamenti che incidono in modo sostanziale su interessati residenti in più di uno Stato membro –, il GDPR, allo scopo di evitare il moltiplicarsi di interventi e di pronunce potenzialmente confliggenti delle varie Autorità di controllo, ha optato per la soluzione dello Sportello Unico.

Per effetto del meccanismo del c.d. "*One Stop Shop*", i trattamenti sopra indicati ricadono, in linea di principio, nella competenza di un'unica Autorità di controllo, da individuarsi nell'Autorità Garante dello Stato membro in cui il Titolare del trattamento abbia stabilito la sua sede principale (amministrazione centrale o sede delle decisioni su finalità e mezzi del trattamento) ovvero la sede unica, che funge da Autorità 'capofila' (c.d."*leading authority*"). Questa Autorità è tenuta a coordinare, nel corso delle indagini, le autorità di controllo degli altri Stati membri interessate allo specifico caso e a coinvolgerle nel processo decisionale. L'obiettivo è giungere a una decisione condivisa, alla quale il destinatario (titolare) dovrà conformare le proprie attività di trattamento nell'Unione.

Ebbene, nella versione aggiornata delle Linee Guida, il Board ha precisato però che, nel caso in cui il Titolare del trattamento non abbia stabilito una propria sede all'interno dell'UE, ma disponga unicamente di un mero rappresentante in uno Stato Membro, il meccanismo dello Sportello Unico o "*One Stop Shop*" non può trovare applicazione. Di conseguenza, in siffatte ipotesi, al Titolare del trattamento si richiede, in caso di *data breach*, di notificare, entro il termine di 72 ore, la violazione della sicurezza dei dati occorsa ad "*ogni singola autorità per la quale gli interessati risiedono nel loro Stato membro*", ossia a tante autorità di protezione dei dati dei Paesi UE quante sono le nazionalità UE degli interessati coinvolti dall'incidente di sicurezza.

Esempi di *data breach*

Pregio della versione aggiornata delle Linee Guida è anche quello di indicare una nuova serie di esempi di *data breach*, utili ad orientare al meglio l'azione dei Titolari e dei Responsabili del trattamento nella classificazione e valutazione delle possibili casistiche di violazione e nella gestione dei processi decisionali conseguenti alla rilevazione di incidenti di sicurezza intervenuti nelle organizzazioni di appartenenza.

Detti esempi vanno, invero, ad ampliare il novero (non esaustivo) di possibili scenari di violazione già delineato in un ulteriore documento di indirizzo diramato in tempi più recenti dall'EDPB in materia di *data breach*.

Va ricordato infatti che, dopo l'emanazione delle già citate Linee Guida del 2017 - ora riproposte nella versione 2.0 -, il Comitato aveva pubblicato un ulteriore documento di indirizzo, ovverosia le Linee Guida 1/2021 su esempi riguardanti la notifica di una violazione dei dati personali (all. n. 3), con l'intento specifico di fornire una serie di indicazioni operative, accompagnate dall'esame di vari tipi di violazioni afferenti a più settori e a più scenari, che andassero a integrare, attraverso la disamina dettagliata di questioni pratiche, gli indirizzi già formulati in precedenza.

Con tale più recente pubblicazione, diffusa allo scopo di aiutare i titolari del trattamento a decidere come gestire le violazioni dei dati e quali fattori prendere in considerazione durante la valutazione del rischio, il Board ha fornito una guida pratica basata su casi concreti tratti dall'esperienza collettiva delle autorità di controllo, rispetto ai quali lo stesso gruppo di Garanti ha presentato delle proprie proposte di valutazione e di analisi delle singole fattispecie considerate, accompagnate da indicazioni specifiche sulle misure corrette da adottare.

Ebbene, nell'aggiornare le Linee Guida del 2017, il Comitato ha ritenuto di dover arricchire la casistica di *data breach* già inclusa nelle Linee Guida del 2021, indicando ulteriori possibili scenari di violazione.

Ad esempio, il Board ha incluso nel novero dei *data breach* anche l'ipotesi di una "*breve interruzione della fornitura di energia elettrica*" che per qualche minuto impedisca il

funzionamento di un call center che abbia, tra le sue funzioni, quella di agevolare il contatto tra clienti e titolare per l'esercizio dei relativi diritti.

Sebbene, come ricordato dallo stesso EDPB, qualsiasi modifica concreta delle circostanze di fatto riferite alle singole fattispecie descritte nel documento possa comportare livelli di rischio diversi o più significativi rispetto a quelli indicati e, quindi, rendere necessarie valutazioni e misure diverse o supplementari rispetto a quelle prospettate, le nuove Linee Guida non prescrivono per la tipologia di incidente sopra indicato, la notifica all'Autorità Garante e la comunicazione agli interessati i cui dati siano stati compromessi, evidenziando unicamente la necessità di aggiornare il Registro delle violazioni, con l'inserimento dell'evento e delle circostanze del caso.

Un altro esempio di *data breach* indicato nella versione aggiornata delle Linee Guida è quello della compromissione di dati già pubblicamente disponibili o, addirittura, di dati adeguatamente crittografati.

Anche in questo caso è stata segnalata unicamente la necessità di provvedere all'aggiornamento del Registro dei *data breach* (e non anche di procedere alla notifica e alla comunicazione).

Il Board, in ogni caso, nell'intervenire sul punto, ha precisato che solo una crittografia "sicura" consente di considerare i dati come non accessibili da terzi non autorizzati e questo richiede una conoscenza specifica in capo ai Titolari e ai Responsabili del trattamento circa i meccanismi di crittografia (es. complessità delle *password*, necessità di variare credenziali di *default*, crittografia durante lo *stand-by* del dispositivo, adeguamento tempo per tempo degli strumenti di crittografia ecc.).

Un dato che, ad ogni modo, è possibile trarre dalle novità introdotte è che il "*Registro dei data breach*" deve diventare un elenco molto dettagliato di ogni violazione dei dati personali eventualmente occorsa, indipendentemente dall'effettiva gravità della stessa e dai reali rischi ai quali abbia esposto gli interessati.

Misure pratiche e consigli tecnici

Nelle nuove Linee Guida viene, infine, riaffermato che è onere del Titolare e del Responsabile del trattamento implementare misure tecniche ed organizzative di protezione idonee ad assicurare la rilevazione tempestiva di eventuali violazioni, in modo tale da consentire all'organizzazione di poter reagire rapidamente e appropriatamente alle stesse.

L'art. 32 del GDPR, in merito alla "sicurezza del trattamento" specifica che nell'implementazione di misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, occorre considerare, tra l'altro, "*la capacità di garantire la riservatezza,*

l'integrità, la disponibilità e la resilienza continue dei sistemi di trattamento e dei dati personali".

Nel pronunciarsi sul punto, l'EDPB ha ricordato innanzitutto che:

- le informazioni relative a tutti gli eventi legati alla sicurezza devono essere rese note dal Titolare ad una o più persone deputate, all'interno dell'organizzazione, ad affrontare gli incidenti di sicurezza, ad appurare l'esistenza di una violazione e a valutare il rischio;
- il rischio derivante dalla violazione – a carico degli interessati – deve essere valutato secondo i seguenti gradi: probabilità di rischio assente, rischio medio o rischio elevato, informando, di conseguenza, le sezioni pertinenti dell'organizzazione;
- se necessario, si deve procedere alla notifica all'Autorità di controllo e alla comunicazione della violazione alle persone interessate;
- allo stesso tempo, il Titolare del trattamento, con il supporto del Responsabile del trattamento ove nominato, deve agire per contenere i pericoli e i danni derivanti dalla violazione;
- è, inoltre, necessario documentare i singoli passaggi della violazione mediante la redazione di apposita documentazione (una relazione, ad esempio, mediante la quale dare atto delle misure correttive approntate - si legga il paragrafo 39 delle Linee Guida).

Nel documento vengono, inoltre, elencati ulteriori consigli tecnici per rilevare ed affrontare una violazione nel migliore dei modi.

In particolare, per individuare alcune irregolarità nel trattamento dei dati, viene suggerito ai Titolari del trattamento di avvalersi di strumenti specifici come analizzatori di flussi di dati e di *log*, grazie ai quali risulta più agevole riconoscere gli eventi e far scattare gli allarmi, puntualizzando come tali misure e meccanismi di rilevazione debbano essere quanto più dettagliati possibile al fine di consentire un maggiore controllo, nonché una migliore gestione nei piani di risposta agli incidenti e/o negli accordi di governance del titolare (paragrafo 37 delle Linee Guida).

Relativamente alle misure organizzative viene posto, poi, l'accento sul tema della "prevenzione", evidenziando come un adeguato livello di protezione dei dati non possa essere assicurato senza l'attuazione di appositi programmi di formazione e sensibilizzazione del personale sugli obblighi di *privacy* e sicurezza.

Oltre all'attivazione di specifici percorsi di formazione e consapevolezza in tema di protezione dei dati personali, le Linee Guida ricordano che può essere particolarmente utile, in tal senso, anche richiamare periodicamente l'attenzione dei dipendenti sui più comuni errori nel trattamento dati e sulle strategie per evitarli, magari trasmettendo l'importanza di una banale

politica di "*clean-desk*" per mantenere l'ordine nell'organizzazione di file e dei documenti o anche di un'attenta azione di riesame dei *file* prima dell'invio.

Passando dalle misure organizzative a quelle più tecniche, è stata evidenziata l'importanza dell'utilizzo di politiche di controllo degli accessi, che prevedano eventualmente misure di autenticazione più rigide per l'accesso a dati sensibili (ad esempio, registrandone tutti gli accessi, da consentire, a seconda dei casi, solo previa specifica motivazione).

Altre misure si focalizzano poi sulla prevenzione di possibili azioni malevole da parte dei dipendenti: la disabilitazione degli *account* istituzionali nel momento in cui un dipendente abbandona l'organizzazione dev'essere certamente tempestiva, ma è possibile anche monitorare (attraverso segnali di *alert*) insoliti flussi di dati tra *server* e postazioni di lavoro degli impiegati, allo scopo di gestire con immediatezza i casi di esfiltrazione.

Ulteriori suggerimenti riguardano, infine, la gestione delle interfacce *input/output* da BIOS (per bloccare o sbloccare l'uso di USB o altri supporti di memorizzazione) e la disabilitazione delle funzioni di stampa dello schermo nel sistema operativo.

In sostanza, viene ribadita la necessità per il Titolare di considerare tutte le possibili soluzioni per evitare o ridurre errori simili.

Il ruolo del Responsabile della Protezione dei Dati (RPD/DPO) nelle nuove Linee Guida

Le Linee Guida si soffermano, infine, sul ruolo del Responsabile della Protezione dei Dati o *Data Protection Officer* (RPD/DPO) che, nel caso di *data breach*, deve fornire assistenza e informazione al Titolare, monitorando il rispetto del GDPR e supportando l'organizzazione nella ricostruzione dell'incidente, per constatare se sia stato gestito in maniera efficiente ed efficace e per individuarne le eventuali cause.

Nella versione aggiornata del documento viene osservato inoltre come, sebbene tale compito non rientri tra quelli "ordinari" del DPO, il Titolare possa anche valutare l'opportunità di affidare al Responsabile della Protezione dei Dati l'incarico di tenere il Registro dei *data breach*, in cui documentare gli incidenti eventualmente occorsi e da esibire all'Autorità di controllo in caso di eventuali verifiche e ispezioni.

Il duplice ruolo del DPO, del resto, emerge con particolare chiarezza in questa delicata fase, in quanto il Titolare, nel notificare una violazione, deve indicare anche i dati e i recapiti del Responsabile per la Protezione dei Dati, cosicché quest'ultimo possa in seguito fungere da tramite fra l'Autorità Garante ed il Titolare.

Da ultimo, nel suggerire a codesti Spett.li Uffici di tenere conto, nell'espletamento dei relativi compiti, dei vari indirizzi dell'EDPB sopra richiamati, appare utile ricordare come

specifiche e dettagliate indicazioni sulle procedure da seguire in caso di eventuali violazioni di dati siano rinvenibili nelle "*Linee Guida per la gestione operativa dei data breach*" appositamente elaborate dal Ministero, che per ogni utilità, nelle more del relativo aggiornamento attualmente in corso, si trasmettono nuovamente (all. n. 4).

In considerazione della rilevanza della materia e della necessità di assicurare che tutto il personale dell'Amministrazione sia adeguatamente informato e istruito in merito agli obblighi da osservare e alle attività da porre in essere in caso di *data breach*, si chiede, infine, agli Spett.li Uffici in indirizzo di invitare, con le modalità ritenute più opportune, tutti i dipendenti in servizio nelle rispettive strutture a prendere visione della documentazione trasmessa, nonché a procedere alla periodica consultazione delle informazioni e dei documenti pubblicati nella sezione "Privacy", rinvenibile all'Area Riservata del sito del Ministero.

Si ringrazia per la consueta e fattiva collaborazione.

Il Responsabile della Protezione dei Dati
Alessia Auriemma

Firmato digitalmente da AURIEMMA ALESSIA
C=IT
O=MINISTERO DELL'ISTRUZIONE E DEL MERITO

Il Direttore Generale
Antonino Di Liberto

Firmato digitalmente da DI LIBERTO ANTONINO
C=IT
O=MINISTERO DELL'ISTRUZIONE

Allegati:

1. Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679, adottate il 3 ottobre 2017 e poi emendate e pubblicate il 6 febbraio 2018, dal Gruppo di Lavoro Articolo 29 (Working Party 29 – WP29, poi divenuto EDPB);
2. Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679, Versione 2.0, adottate il 28 marzo 2023, dal Comitato Europeo per la Protezione dei Dati (EDPB) – versione in lingua inglese;
3. Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali, adottate il 14 dicembre 2021 dal Comitato Europeo per la Protezione dei Dati (EDPB);
4. Linee Guida per la gestione operativa dei *data breach* del Ministero – Versione Agosto 2021;