REGOLAMENTO DATA BREACH

A.S. 2021-2022

Rappresentante legale

Dott.ssa Chiara Di Prima
Via Danimarca, 54
90100 - Palermo (PA)
email: paps010002@istruzione.it

Responsabile per la protezione dei dati personali

DPO Mario Grimaldi
Cell. 3493424766
email: dpo.grimaldi@gmail.com

Sommario

Articolo 1

(Cosa s'intende per "Data Breach ")

Il Regolamento UE 679/2016, all'art. 4,c.12 definisce la violazione dei dati personali: *"Qualsiasi violazione di sicurezza che comporta, anche 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".*

Si tratta di una definizione molto ampia, in quanto comprende qualunque evento che metta a rischio i dati personali trattati (indipendentemente dalla causa che l'ha generata, (i c.d. incidenti informatici, anche accidentali).

Articolo. 2

(Notificazione del Data Breach)

Ai sensi e per gli effetti dell'art.33 del Regolamento UE, in caso di violazione dei dati personali, il titolare del trattamento ha l'obbligo di notificare la violazione all'Autorità di controllo competente 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, devono essere esplicitati chiaramente i motivi del ritardo.

Al riguardo, il considerando 86 del GDPR chiarisce ulteriormente che l'obbligo di notifica interviene qualora la violazione dei dati personali sia suscettibile di presentare un rischio per i diritti e le libertà della persona fisica.

Articolo 3

(Modalità di notifica)

In caso di *Data breach*, tutti i Titolari del Trattamento devono effettuare la notificazione della violazione dati personali al Garante per la Protezione dei Dati.

Il Regolamento distingue due modalità di notifica, a seconda della gravità di rischio; per i diritti e le libertà delle persone fisiche, associato alla violazione:

1. la notificazione dell'avvenuta violazioni di dati all'Autorità nazionale di protezione dei dati personali (prevista dall'art. 33 del regolamento UE);
2. la comunicazione ai soggetti a cui si riferiscono i dati, nei casi più gravi (c.d. soggetti "interessati), prevista dall'art. 34 del regolamento UE.

Articolo 4

(Notifica all'Autorità di controllo e suoi contenuti)

In ossequio a quanto prescritto dall'art. 33 del Regolamento UE, l'Istituto, in qualità di titolare del trattamento, procederà alla notifica all'Autorità di controllo, *"senza ingiustificato ritardo"* e, ove possibile, entro 72 ore da quando ne è venuto a conoscenza, ove risulti probabile che dalla violazione possano derivare rischi per i diritti e le libertà degli interessati.

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, dovranno essere esplicitati e documentati i motivi del ritardo, anche al fine di non incorrere nelle sanzioni previste dal Regolamento Europeo.

La notifica all'Autorità di controllo deve contenere almeno le seguenti informazioni minime:

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, del Responsabile del trattamento 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 del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora non sia possibile fornire tutte le suddette informazioni contestualmente alla notifica, quest'ultima dovrà essere integrata, anche in fasi successive, con i dati e le notizie mancanti, senza ulteriore ingiustificato ritardo.

Articolo 5

(Comunicazione agli Interessati e suoi contenuti)

In ossequio a quanto prescritto dall'art. 34 del Regolamento UE, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Istituto, in qualità di titolare del trattamento, comunicherà, senza ingiustificato ritardo, la violazione all'interessato, anche al fine di consentigli l'adozione di idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione dei suoi dati personali.

La comunicazione all'interessato di dovrà descrive, con un linguaggio semplice e chiaro:

- la natura della violazione dei dati personali;
- 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.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

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 di cui al paragrafo 1;

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.

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 è soddisfatta.

Articolo 6

(Condizioni per la mancata comunicazione agli Interessati)

In attuazione dell'art.34, comma 3 del GDPR, l'Istituto, in qualità di titolare del trattamento, non darà luogo alla comunicazione all'interessato, ove risulti comprova e soddisfatta una delle seguenti condizioni:

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 ad es. 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 di cui al paragrafo 1;

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.

Articolo 7

(Possibili determinazioni dell'Autorità di Controllo)

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'Autorità di controllo può comunque richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda e può decidere che

una delle condizioni di cui alle lett. a), b) o c) dell'articolo risulti soddisfatta.

Articolo 8

(Valutazione preliminare del rischio)

Una violazione dei dati personali può, se non affrontata in modo tempestivo può provocare danni fisici, materiali o immateriali, oltre che reputazionali alle persone fisiche.
In presenza di una avvenuta, accertata violazione dei dati personali, l'Istituto, in qualità di Titolare del trattamento, procederà subito ad effettuare con riguardo alla natura, all'ambito di applicazione, al contesto ed alle finalità del trattamento, una preliminare valutazione oggettiva sulle probabilità e gravità dei rischi, per i diritti e le libertà delle persone fisiche, che possono derivare da trattamenti di dati personali oggetto di violazione, con particolare riguardo ai seguenti aspetti:

1. limitazione o privazione dei diritti delle persone fisiche;
2. perdita dell'esercizio del controllo dei propri dati personali;
3. discriminazione;
4. furto o usurpazione d'identità;
5. perdite finanziarie;
6. decifratura non autorizzata della pseudonimizzazione;
7. pregiudizio alla reputazione;
8. perdita di riservatezza dei dati protetti dal segreto professionale;
9. qualsiasi altro danno economico o sociale significativo alla persona fisica interessata;
10. se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
11. in caso di valutazione di aspetti personali, mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
12. se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
13. se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Inoltre, in sede di valutazione oggettiva dell'effettiva sussistenza del rischio e della sua gravità, ai fini l'eventuale assolvimento dell'obbligo di notifica delle violazioni di dati personali, si terrà debitamente conto anche delle circostanze di tale violazione, quali ad esempio:

a) se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso;

b) se esistono legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.

Articolo 9

(Esiti della valutazione del rischio)

In relazione ai diversi esiti che possono derivare dalla valutazione preliminare del rischio, s1 potranno verificare le seguenti conseguenze:

1. ove risulti probabile che dalla violazione possano derivare rischi per i diritti e le libertà degli interessati, il Titolare del trattamento provvederà a:
   - notificare il *data breach* all'Autorità di controllo (art.33 GDPR), secondo le previsioni di cui all'art 4 del presente Regolamento;
2. ove risulti probabile che dalla violazione possano derivare *elevati* rischi per i diritti e le libertà degli interessati, il Titolare del trattamento provvederà a:
   - notificare il *data breach* all'Autorità di controllo (art.33 GDPR), secondo le previsioni di cui all'art 4 del presente Regolamento;
   - a comunicare il *data breach ai soggetti cui si riferiscono i dati (c.d. "Interessati"* (art.34 GDPR), secondo le previsioni di cui all'art 4 del presente Regolamento;
3. ove, invece, risulti improbabile che dalla violazione possano derivare rischi per i diritti e le libertà degli interessati, il titolare del trattamento non procederà con le notifiche e comunicazioni di cui ai precedenti n.1) e 2).

Conformemente al principio di responsabilizzazione, dunque, l'Istituto è esentato dall'effettuare la notifica solo se è in grado di dimostrare al Garante che la violazione dei dati personali non presenta rischi per i diritti e per le libertà fondamentali delle persone fisiche interessate.

Articolo 10

(Modalità della Valutazione preliminare del rischio)

Ogni Responsabile di Unità Operativa di riferimento (UOR) , in quanto Responsabile del trattamento di pertinenza del proprio settore ha l'obbligo di segnalare immediatamente con la più ampia libertà

di forme e procedure (anche per le vie brevi e/o oralmente), la violazione dei dati personali, procedendo poi alla formale comunicazione entro massimo 24 ore ai soggetti di seguito indicati:

- Titolare del trattamento, in personale del Legale Rappresentante pro-tempore;
- DPO;
- Direttore S.G.A.

Ai fini del rispetto dei tempi prescritti dalla normativa, d'intesa con il Titolare del trattamento, il DPO provvederà - immediatamente, e comunque non oltre le 24 ore successive alla ricezione della comunicazione, inviata anche per posta elettronica all'indirizzo dedicato - a convocare, riunire e presiedere un tavolo tecnico, nella composizione minima di seguito indicata, per effettuare la valutazione preliminare sulle probabilità e gravità dei rischi, per i diritti e le libertà degli interessati, che possono derivare da trattamenti dei dati personali oggetto di violazione

- DPO;
- il Responsabile del trattamento presso il cui servizio si è verificato il data breach;
- Direttore D.S.G.A (responsabile gestione documentale)
- Amministratore di sistema (se previsto in organico)
- Consulente informatico interno/esterno

Il DPO ha pi ena facoltà di convocare altri soggetti che ritiene utili alle necessità del caso.
Il DPO dovrà quindi curare e documentare l'attività istruttoria, acquisendo tutti gli elementi probatori alla base della valutazione.
All'esito delle attività, dovrà essere redatto sintetico verbale, con possibile documentazione di supporto, ricognitivo delle analisi e degli esiti della valutazione effettuata nonché delle conseguenti proposte operative, da sottoporre al Titolare del trattamento per la decisione finale.
Detto verbale, sottoscritto da tutti i convenuti e protocollato, sarà inoltrato al Titolare del trattamento.

Ricevuto il verbale e l'allegata documentazione, in relazione all'esito della valutazione di cm all'art. precedente, il Titolare del trattamento procederà come indicato nell'art art.9.
Gli eventuali atti di notifica all'Autorità di controllo, e la possibile comunicazione all'/agli interessato/i, saranno quindi predisposti e redatti da DPO e presentati al Titolare del trattamento per la sottoscrizione.
Il DPO dovrà garantire che la notificazione, in via telematica tramite posta elettronica certificata- sia effettuata all'Autorità di controllo (anche se in forma generica, e con riserva di integrazione) entro i termini prescritti dal Regolamento UE.
La comunicazione deve essere redatta con cura e attenzione in quanto può dar luogo a un intervento

dell'Autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal Regolamento Ue.

Articolo 11
(Registro cronologico del DPO)

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.
Atteso che tale documentazione consente all'Autorità di controllo di verificare, in qualsiasi momento, il rispetto del GDPR in materia di *Data breach*, la stessa sarà custodita, con la massima cura e diligenza, dal DPO il quale, all'uopo, dovrà tenere altresì apposito registro cronologico, elaborato secondo variabili di interesse, dei casi di violazione dei dati.

Articolo 12
(Sanzioni e responsabilità)

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il Regolamento UE, ha il diritto di proporre reclamo ad un'Autorità di controllo, la quale può infliggere, a seconda dei casi, sanzioni amministrative pecuniarie effettive, proporzionate e dissuasive, ai sensi dell'art.83.
Inoltre, in caso di data breach, l'interessato, ex art.82, che subisce un danno materiale o immateriale causato da una violazione dei dati personali, ha anche il diritto di ottenere il risarcimento del danno dal Titolare del trattamento o dal Responsabile del trattamento, a meno che il Titolare del trattamento non riesca a dimostrare di avere adottato tutte le misure di sicurezza previste dal Regolamento Europeo che l'evento dannoso non gli è in alcun modo imputabile.
Infine, l'art. 83 stabilisce espressamente che la violazione degli obblighi del Titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43 è soggetta a sanzioni.

Articolo 13

(Modalità di notificazione)

La notificazione della violazione dei dati deve essere redatta secondo il modello di cui all'art.11, allegato al presente Regolamento (Allegato 1) e pubblicato sul sito istituzionale, ed inviato telematicamente, tramite posta elettronica certificata, all'indirizzo: databreach.pa@pec.gpdp.it

Articolo 14

(Norma finale)

Per tutto quanto non espressamente previsto nel presente Regolamento si fa rinvio alla vigente normativa legislativa e regolamentare.

L'Istituto si riserva di apportare al presente Regolamento le modifiche, rettifiche e/o integrazioni che si renderanno necessarie, anche alla luce di eventuali innovazioni normative intervenute in materia o pronunciamenti dell'Autorità Garante per la protezione dei dati.

Articolo 15

(Modello allegato per la notifica Data Breach al Garante)

In allegato al presente Regolamento, il modello di notifica *data breach* al Garante (***Allegato 1)***

Il DIRIGENTE SCOLASTICO
Dott.ssa Chiara Di Prima