REGOLAMENTO DATA BREACH

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).

Le violazioni di dati personali possono essere classificate in base a tre diverse tipologie connesse alla sicurezza delle informazioni:

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

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Articolo. 2
(Notificazione del Data Breach)

La notifica ha la funzione di consentire all'autorità di controllo di applicare le misure correttive a sua disposizione (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ecc.)

previste dall'articolo 58 del Regolamento e di adottare misure di tutela immediate a favore dei soggetti coinvolti. Elemento centrale della procedura di notificazione è la sua tempestività.
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.

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;
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 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)

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.

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 dati personali (DS)
- Responsabile protezione dati personali (DPO)
- Direttore S.G.A

Ogni Responsabile del trattamento che viene a conoscenza di una violazione dei dati personali che sta trattando per conto del Titolare, deve notificarla al Titolare "senza ingiustificato ritardo".
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.

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/videoconferenza, 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:

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

Il DPO ha piena 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.

Articolo 11
(Registro degli incidenti di sicurezza)

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 Titolare, il quale, all'uopo, dovrà tenere altresì apposito registro degli incidenti, elaborato secondo variabili di interesse, dei casi di violazione dei dati.
Il Titolare può 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.

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. 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.

Articolo 13
(Modalità di notificazione)

In caso di violazione, il Titolare al Trattamento dati personali notifica il data breach al Garante per la protezione dei dati personali, utilizzando l'apposita procedura telematica disponibile al seguente link https://servizi.gpdp.it/databreach/s/ con la quale vengono richieste le informazioni contenute nel modello v.2021-04 pubblicato sia sul portale del Garante[1] sia nella sezione privacy del sito istituzionale.

Articolo 14
(Norma finale)

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

1 Notifica di una violazione dei dati personali art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

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.

Il Dirigente Scolastico