ISTITUTO COMPRENSIVO STATALE CINISI

Via Sacramento, snc - 90045 CINISI (PA)
C.M. PAIC846007 - C.F. 97163700822 - C.U. UF53BN - Tel. 091.8664046
www.istitutocomprensivocinisi.edu.it - E-mail: paic846007@istruzione.it - paic846007@pec.istruzione.it

REGOLAMENTO DATA BREACH

Titolare del trattamento

Istituto Comprensivo Statale Cinisi

email: paic846007@istruzione.it; PEC: paic846007@pec.istruzione.it

Rappresentante legale

Prof. Benedetta Lidia Bartolotta
Via Sacramento snc – Cinisi (PA)
Tel. 091/8664046
email: paic846007@istruzione.it

Responsabile per la protezione dei dati personali

Mario Grimaldi
Cell. 3493424766
email: dpo.grimaldi@proton.me

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.

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;

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.

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