ISTITUTO ISTRUZIONE SECONDARIA SUPERIORE
"E. GIANNELLI"
Via Fiume, n. 7 - 73052 PARABITA (LE)
C.F. 81002570752 0833593021 0833509756
www.iissparabita.edu.it – leis033002@istruzione.it

REGOLAMENTO

PER LA VIOLAZIONE DEI DATI PERSONALI *-data breach-*

Triennio di riferimento: 2022 – 2025

Approvato dal Consiglio di Istituto nella seduta del 29.09.2022

PREMESSA

Il Ministero dell'Istruzione ha trasmesso il 2 agosto 2023 alle istituzioni scolastiche la nota informativa n. 1248 del 2023 riguardante gli obblighi di notifica in caso di violazione dei dati personali (c.d. "*data breach*") sulla scorta della revisione delle Linee Guida n. 9/2022 elaborato dal Comitato Europeo per la Protezione dei Dati (EDPB) lo scorso 28 marzo 2023.

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali 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 il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Al fine di identificare e, se necessario, notificare correttamente un data breach all'autorità garante competente e/o agli interessati, il Dirigente Scolastico intende definire le procedure da seguire qualora avvenga un presunto data breach all'interno dell'amministrazione. Si ricorda che la mancata notifica, qualora sia essa necessaria, può comportare una sanzione amministrativa fino ad un importo di 10 milioni di euro oppure il 2% del fatturato dell'intera società.

Il presente regolamento di istituto è stato redatto sulla base delle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679, redatto dal gruppo di lavoro art. 29 per la protezione dei dati, adottate il 3 ottobre 2017 e nella versione emendata e adottata in data 6 febbraio 2018. Tali linee guida sono reperibili sul sito del garante per la protezione dei dati personali al link https://www.garanteprivacy.it/regolamentoue/databreach.

Definizione Data Breach

Per poter porre rimedio a una violazione occorre innanzitutto che il titolare del trattamento sia in grado di riconoscerla. In disciplina di GDPR (*General Data Protection Regulation*), un **Data Breach è una violazione di dati personali** accertata.

Si definisce **Data Breach** *ogni violazione della 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,* come da **Regolamento Europeo (art. 4, c. 12).**

Di seguito una descrizione della terminologia, come descritto dal Garante per la Protezione dei Dati personali:

- **Distruzione:** il significato di "distruzione" dei dati personali dovrebbe essere abbastanza chiaro: si ha distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento.

- **Perdita:** Con "perdita" dei dati personali si dovrebbe invece intendere il caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso.

- **Divulgazione o accesso:** un trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del regolamento.

- **Modifica:** si verifica un danno quando i dati personali sono stati modificati, corrotti o non sono più completi.

Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del titolare del trattamento. Un altro esempio può essere il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un *ransomware* (*malware* del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso. Ulteriori esempi possono essere visionati nell'**allegato B** al presente regolamento.

Inoltre, le violazioni possono essere classificate in base ai seguenti tre principi ben noti della 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 dei 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 dellestesse.

Esempi di perdita di disponibilità possono aversi quando i dati vengono cancellati accidentalmenteo da una persona non autorizzata, oppure, in caso di dati crittografati in maniera sicura, quando lachiave di decifratura viene persa. Se il titolare del trattamento non è in grado di ripristinare l'accesso ai dati, ad esempio ricorrendo a un backup, la perdita di disponibilità sarà considerata permanente.

Può verificarsi perdita di disponibilità anche in caso di interruzione significativa del servizio abituale di un'organizzazione, ad esempio un'interruzione di corrente o attacco da "blocco di servizio" (*denial of service*) che rende i dati personali indisponibili.

Tempi di notifica del data breach

Il regolamento impone al **titolare del trattamento** di notificare le violazioni all'autorità di controllo competente, fatta salva l'improbabilità che la violazione presenti il rischio che si verifichino detti effetti negativi. Laddove sia altamente probabile che tali effetti negativi si verifichino, il regolamento impone al titolare del trattamento di comunicare la violazione alle persone fisiche interessate non appena ciò sia ragionevolmente fattibile.

Più nel dettaglio, l'Art. 33, paragrafo 1 del regolamento impone che: In caso di violazione dei dati personali, il titolare del trattamento notifica 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.

Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere postosulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono statieffettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, senecessario.

L'autorità garante riporta alcuni esempi a riguardo:

- In caso di perdita di una chiave USB contenente dati personali non crittografati spesso nonè possibile accertare se persone non autorizzate abbiano avuto accesso ai dati. Tuttavia, anche se il titolare del trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, tale caso deve essere notificato, in quanto sussiste una ragionevole certezza del fatto che si è verificata una violazione della disponibilità; il titolare del trattamento si considera venuto "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB.

- Un terzo informa il titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata. Dato che al titolare del trattamento è stata presentata una prova evidente di una violazione della riservatezza, non vi è dubbio che ne sia venuto "a conoscenza".

- Un titolare del trattamento rileva che c'è stata una possibile intrusione nella sua rete. Controlla quindi i propri sistemi per stabilire se i dati personali ivi presenti sono stati compromessi e ne ottiene conferma. Ancora una volta, dato che il titolare del trattamento ha una chiara prova di una violazione non può esserci dubbio che sia venuto "a conoscenza" della stessa.

- Un criminale informatico viola il sistema del titolare del trattamento e lo contatta per chiedere un riscatto. In tal caso, dopo aver verificato il suo sistema per accertarsi dell'attacco, il titolare del trattamento dispone di prove evidenti che si è verificata una violazione e non vi è dubbio che ne sia venuto a conoscenza.

- Una persona informa il titolare del trattamento di aver ricevuto un'e-mail da un soggetto che si fa passare per il titolare del trattamento, contenente dati personali relativi al suo (effettivo) utilizzo del servizio del titolare del trattamento, aspetto questo che suggerisce che la sicurezza del titolare del trattamento sia stata compromessa. Il titolare del trattamento

conduce una breve indagine e individua un'intrusione nella propria rete e la prova di un accesso non autorizzato ai dati personali. Il titolare del trattamento si considera "a conoscenza" della violazione in questo momento e dovrà procedere alla notifica all'autorità di controllo a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Il titolare del trattamento dovrà prendere le opportune misure correttive per far fronte alla violazione.

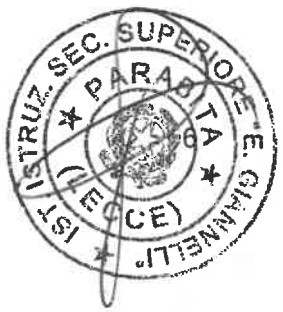
Di conseguenza, il titolare del trattamento dovrebbe disporre di procedure interne per poter rilevare una violazione e porvi rimedio. Ad esempio, per rilevare talune irregolarità nel trattamento dei dati, il titolare o il responsabile del trattamento può utilizzare alcune misure tecniche certe come il flusso di dati e gli analizzatori di registri, dai quali è possibile definire eventi e allerte correlando qualsiasi dato di registro. È importante che quando viene rilevata una violazione, la stessa venga segnalata al livello superiore appropriato di gestione, in maniera da poter essere trattata e, se del caso, notificata in conformità all'art. 33 e, se necessario, all'art. 34.

Doveri del Responsabile del Trattamento

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'art. 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.



Modalità di notifica

In caso di *Data breach,* tutti i Titolari del Trattamento devono effettuare la notificazione dellaviolazione 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 lelibertà delle persone fisiche, associato alla violazione:

1. la notificazione dell'avvenuta violazioni di dati all'Autorità nazionale di protezione dei datipersonali (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.

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 violazionepossano 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 categoriee 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.

La modulistica messa a disposizione dall'autorità Garante per la Protezione dei Dati Personali, per la segnalazione, è scaricabile dal sito dell'istituto e si trova in allegato al suddetto regolamento (Allegato 1).

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 altropunto 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.

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.

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.

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 aspettiriguardanti 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 numerodi 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.

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 peri 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 aprescindere, 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.

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 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 probatorialla 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 cui all'articolo precedente, il Titolare del trattamento procederà come indicato nell'art 9.

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 esibireall'Autorità di controllo in caso di eventuali verifiche e ispezioni.

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 alcunaviolazione, si riveli essere un falso positivo.

Il dirigente scolastico
Prof. Cosimo Preite

ALLEGATI

Vengono di seguito riportate:

-Allegato A: Istruzioni schematiche relative alla notifica della violazione (allegatoA)

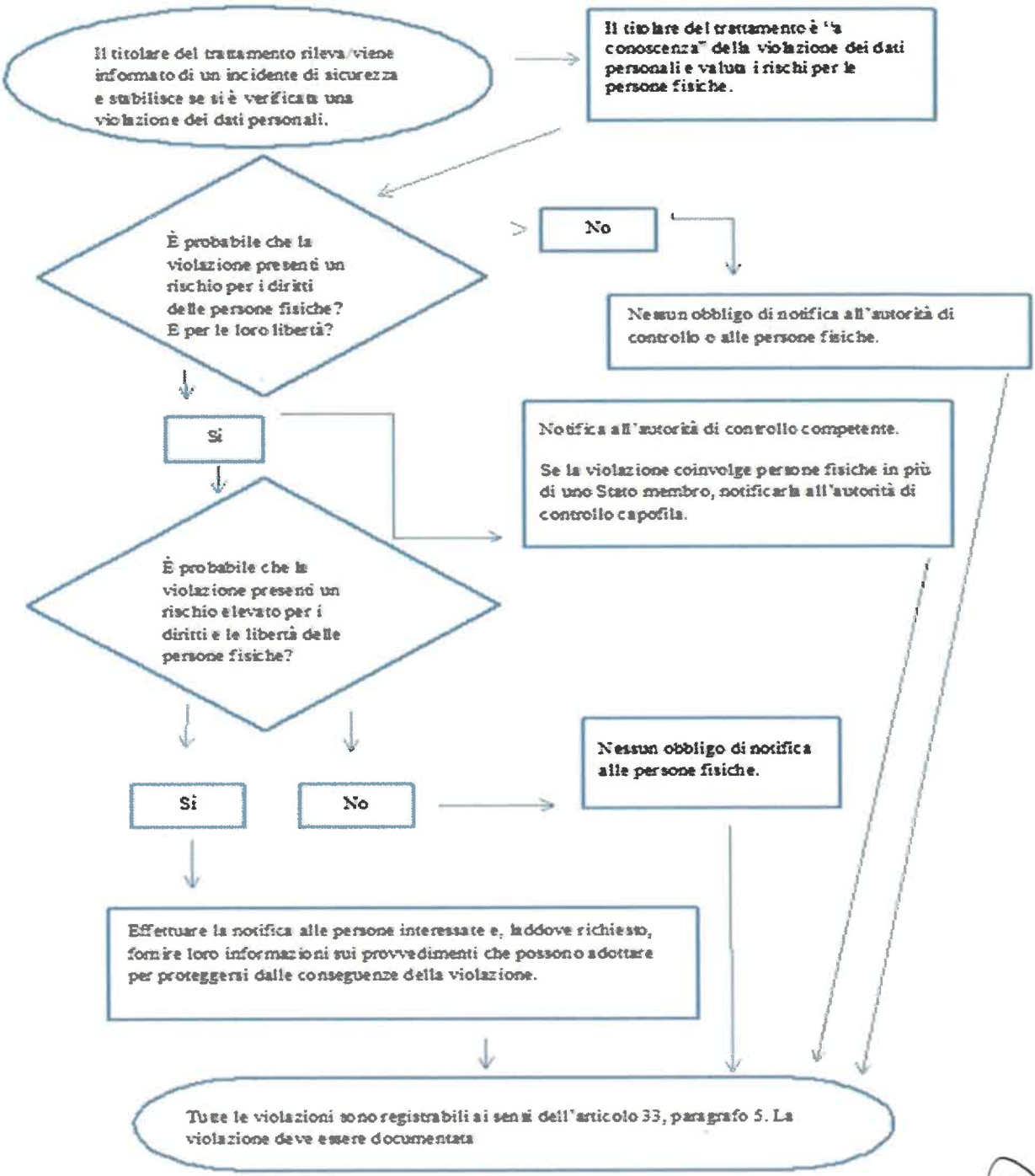
-Allegato B: Lista non esaustiva delle possibili violazioni, come indicato dall'autorità Garante per la Protezione dei Dati Personali.

-Allegato 1: Modello di notifica al garante

-Allegato 2: Referenti della protezione dei dati e gestione della violazione dati personali

Allegato A

Schematizzazione delle procedure di valutazione delle violazioni di dati personali



Esempi di violazioni dei dati personali e dei soggetti a cui notificarle

I seguenti esempi non esaustivi aiuteranno il titolare del trattamento a stabilire se deve effettuare la notifica in diversi scenari di violazione dei dati personali. Questi esempi possono altresì contribuire a distinguere tra rischio e rischio elevato per i diritti e le libertà delle persone fisiche.

Esempio	Notifica all'autorità di controllo?	Comunicazione all'interessato?	Note/raccomandazioni
Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica

ii. Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati. Il titolare del trattamento ha clienti in un solo Stato membro.	Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata.	
iii. Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del trattamento e accedere alle proprie registrazioni.	No.	No.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'art. 33, paragrafo 5. Il titolare del trattamento deve conservare adeguate registrazioni in merito.
iv. Un titolare del trattamento subisce un	Sì, effettuare la segnalazione	Sì, effettuare la segnalazione alle	Se fosse stato disponibile un backup e i dati

attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa evidente che l'unica funzionalità dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.	all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente con altri mezzi, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'art. 32.
v. Una persona telefona al call center di una banca per segnalare una violazione dei dati. La persona ha ricevuto l'estratto conto mensile da un soggetto diverso. Il titolare del trattamento intraprende una breve indagine (ossia la conclude entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e che vi è una potenziale carenza sistemica che potrebbe comportare il coinvolgimento già occorso o potenziale di altre persone fisiche.	Sì.	La comunicazione va effettuata soltanto alle persone fisiche coinvolte in caso di rischio elevato e se è evidente che altre persone fisiche non sono state interessate dall'evento.	Se dopo ulteriori indagini si stabilisce che l'evento ha interessato un numero maggiore di persone fisiche è necessario comunicare questo sviluppo all'autorità di controllo, e il titolare del trattamento deve informarne le altre persone fisiche interessate se sussiste un rischio elevato per loro.

vi. Un titolare del trattamento gestisce un mercato online e ha clienti in più Stati membri. Tale mercato subisce un attacco informatico a seguito del quale i nomi utente, le password e la cronologia degli acquisti vengono pubblicati online dall'autore dell'attacco.	Sì, segnalare l'evento all'autorità di controllo capofila se la violazione riguarda un trattamento transfrontaliero.	Sì, dato che la violazione potrebbe comportare un rischio elevato.	Il titolare del trattamento dovrebbe prendere delle misure, ad esempio forzare il ripristino delle password degli account interessati, e altri provvedimenti per attenuare il rischio. Il titolare del trattamento dovrebbe altresì considerare qualsiasi altro obbligo di notifica, ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali.

vii. Una società di *hosting* di siti web che funge da responsabile del trattamento individua un errore nel codice che controlla l'autorizzazione dell'utente. A causa di tale vizio, qualsiasi utente può accedere ai dettagli dell'account di qualsiasi altro utente.	In veste di responsabile del trattamento, la società di *hosting* di siti web deve effettuare la notifica ai clienti interessati (i titolari del trattamento) senza ingiustificato ritardo. Supponendo che la società di *hosting* di siti web abbia condotto le proprie indagini, i titolari del trattamento interessati dovrebbero essere ragionevolmente certi di aver subito una violazione e pertanto è probabile che vengano considerati "a conoscenza" della violazione nel momento in cui hanno ricevuto la notifica da parte della società di *hosting* (il responsabile del trattamento). Il titolare del trattamento deve quindi effettuare la notifica all'autorità di controllo.	Qualora non vi siano probabili rischi elevati per le persone fisiche non è necessario effettuare una comunicazione a tali persone.	La società di *hosting* di siti web (responsabile del trattamento) deve prendere in considerazione qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali). Qualora non vi sia alcuna prova che tale vulnerabilità sia sfruttata presso uno dei suoi titolari del trattamento, la violazione potrebbe non essere soggetta all'obbligo di notifica, tuttavia potrebbe essere una violazione da registrare o essere il segno di un mancato rispetto dell'art. 32.

viii. Le cartelle cliniche di un ospedale sono indisponibili per un periodo di 30 ore a causa di un attacco informatico.	Sì, l'ospedale è tenuto a effettuare la notifica in quanto può verificarsi un rischio elevato per la salute e la tutela della vita privata dei pazienti.	Sì, informare le persone fisiche coinvolte.	
ix. I dati personali di un gran numero di studenti vengono inviati per errore a una mailing list sbagliata con più di 1 000 destinatari.	Sì, segnalare l'evento all'autorità di controllo.	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	
x. Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e- mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se è interessato un numero elevato di persone, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, il messaggio di posta elettronica contiene le password iniziali).	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.

ALLEGATO 1

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal Regolamento europeo 2016/679, i titolari di trattamento dei dati personali sono tenuti a comunicare al Garante le violazioni dei dati personali (data breach) che possono comportare un rischio elevato per i diritti e le libertà delle persone fisiche, (cfr. Art 33.1 del predetto Regolamento Ue 2016/679).

La comunicazione deve essere effettuata entro 72 ore dalla conoscenza del fatto, compilando il modulo che segue.

Titolare del trattamento

Denominazione o ragione sociale _____

Provincia _____ **Comune** _____

Cap _____ **Indirizzo** _____

Nome persona fisica addetta alla comunicazione _____

Cognome persona fisica addetta alla comunicazione _____

Funzione rivestita _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

Eventuali Contatti (altre informazioni) _____

Natura della comunicazione

_____

_____

_____

Breve descrizione della violazione dei dati personali trattati mediante il *dossier* sanitario

Quando si è verificata la violazione dei dati personali trattati?

- ☐ Il _____
- ☐ Tra il _____ e il _____
- ☐ In un tempo non ancora determinato
- ☐ E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio

Tipo di violazione

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ Altro:

Dispositivo oggetto della violazione

- ☐ Computer
- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di *backup*
- ☐ Documento cartaceo
- ☐ Altro :

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione dei dati personali trattati mediante il *dossier* sanitario?

- ☐ N. _____ persone
- ☐ Circa _____ persone
- ☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- ☐ Dati anagrafici
- ☐ Indirizzo di posta elettronica
- ☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)
- ☐ Dati idonei a rivelare lo stato di salute
- ☐ Dati relativi a minori
- ☐ Dati facenti parte di categorie particolari (es. rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica o alla vita sessuale o all'orientamento sessuale della persona)
- ☐ Copie per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro :

Livello di gravità della violazione dei dati personali trattati mediante il *dossier* sanitario (secondo le valutazioni del titolare)?

- ☐ Basso/trascurabile
- ☐ Medio
- ☐ Alto
- ☐ Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il _____

☐ No, perché _____

Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

Luogo, data

Firma

_____

_____

ALLEGATO 2

REFERNTI DELLA PROTEZIONE DEI DATI E
GESTIONE DELLA VIOLAZIONE DATI PERSONALI (data breach)

Il Regolamento sulla privacy dell'IISS "Giannelli" è stato aggiornamento come da nota informativa trasmessa dal Ministero dell'Istruzione il 2 agosto 2023 riguarda gli obblighi di notifica in caso di violazione dei dati personali, noti come "data breach", in conformità con le Linee Guida n. 9/2022 elaborate dal Comitato Europeo per la Protezione dei Dati (EDPB) il 28 marzo 2023. Il Dirigente Scolastico, rappresentante legale dell'istituzione scolastica titolare del trattamento, per garantire le misure organizzative più idonee a tutelare i dati personali trattati ha definito le linee guida per la gestione delle violazioni privacy di cui il presente documento è un estratto con la sintesi delle procedure adottate per la gestione dei data breach.

Cosa è una violazione di dati personali (data breach)

All'art. 4, punto 12, del Regolamento Europeo 679/2016 (GDPR) definisce il data breach come "la 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".

Esempi di data breach:

- sottrazione o copia non autorizzata di un documento cartaceo od informatico contenente dati personali
- perdita o furto di una pen drive, di un notebook o di qualunque altro dispositivo contenente dati personali
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- dati e documenti criptati da un ransomware (malware del riscatto)
- dati e documenti criptati dal titolare del trattamento mediante una chiave non più in suo possesso
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali;
- una e-mail che viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e- mail di altri destinatari che non abbia dato il consenso.

Cosa deve fare l'amministrazione in caso di violazione

L'art. 33 del Regolamento Europeo 679/2016 (GDPR) impone al titolare del trattamento di notificare all'autorità di controllo (Garante privacy) la violazione di dati personali entro 72 ore dal momento in cui ne viene a conoscenza. L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche; qualora non

rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

La valutazione dell'opportunità della comunicazione al Garante o agli interessati spetta al titolare del trattamento (nella persona del dirigente scolastico) sentito il parere del Responsabile Protezione Dati e di altre eventuali figure che forniscono servizi di assistenza e consulenza.

Cosa deve fare il personale della scuola in caso di violazione

Il contenimento dei rischi associati ad una violazione di dati personali è strettamente legato alla tempestività e all'adeguatezza degli interventi atti a limitare ogni possibile conseguenza. E' allora necessario che qualora un dipendente dell'amministrazione rilevi una possibile violazione dei dati personali ne dia immediata comunicazione al Dirigente Scolastico o, qualora esso non sia immediatamente disponibile, al Responsabile della Protezione dei Dati o ad altre eventuali figure che gestiscono i sistemi informatici o che forniscono servizi di assistenza e consulenza informatica e normativa in modo da consentire la massima tempestività di intervento.

A questo proposito forniamo i seguenti riferimenti:

Responsabile Protezione Dati:

Direttore S.G.A.
Vice Direttore S.G.A.
Collaboratori del Dirigente Scolastico
Referenti di sede
Docenti di sostegno
Referenti BES
Applicati di segreteria

Modulo segnalazione violazione dei dati personali (*data breach*)

La modulistica messa a disposizione dall'autorità Garante per la Protezione dei Dati Personali, per la segnalazione, è scaricabile dal sito dell'istituto e si trova in allegato al suddetto regolamento (Allegato 1).

Attività successive alla segnalazione

Il dirigente scolastico, di concerto con l'RPD ed altre eventuali figure tecniche o consulenziali di cui si avvale la scuola per la gestione della privacy e dei sistemi informatici, provvederà ad effettuare una prima indagine interna e a definire la gravità dell'eventuale violazione. In particolare procederà a identificare i possibili rischi derivanti dalla violazione e a definire qualunque azione da intraprendere per la loro minimizzazione. In questa fase il dirigente scolastico dovrà valutare l'opportunità o la necessità di fare la comunicazione al Garante, che dovrà intervenire entro le 72 ore ore dalla conoscenza del fatto, ed eventualmente alle persone fisiche minacciate nei loro diritti dall'evento. In merito alla scelta dovranno essere coinvolti ed esprimeranno il proprio parere il RPD ed eventuali altri consulenti informatico/normativi ma la decisione finale dovrà essere del dirigente scolastico che sarà responsabile in base al principio della responsabilizzazione.

La comunicazione al Garante

Qualora il dirigente scolastico ritenga di dover fare la segnalazione al Garante dovrà effettuarla entro le 72 dalla venuta a conoscenza della violazione salvo motivare opportunamente il ritardo. La notifica della violazione al Garante dovrà avvenire dalla casella PEC istituzionale dell'amministrazione e dovrà essere indirizzata a protocollo@pec.gpdp.it. La mail dovrà avere come oggetto **"notifica data breach"** e dovrà avere allegata una relazione effettuata sulla base del modello messo a disposizione dal Garante a questo link. La relazione dovrà essere firmata digitalmente dal dirigente scolastico, titolare del trattamento, ma è opportuno che alla sua redazione partecipi attivamente il RPD.

Il registro delle violazioni

La violazione, che sia o no comunicata al Garante o agli interessati, dovrà essere annotata nel registro delle violazioni che dovrà essere tenuto costantemente aggiornato dall'amministrazione.