MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
Istituto Comprensivo "A.Stradella" - Nepi.
Via Romasnc - 01036 - Nepi (VT) - C.F. 90056760565
✉vtic81400x@istruzione.it ✉vtic81400x@pec.istruzione.it
☎ ***0761/556092***

PROCEDURA PER LA GESTIONE DELLE

VIOLAZIONI DEI DATI PERSONALI

"DATA BREACH"

AI SENSI DEL REGOLAMENTO EUROPEO 679/2016

L'art. 33 del Regolamento generale sulla protezione dei dati 679/2016 G.D.P.R. ha introdotto l'obbligo in capo al Titolare del trattamento di notifica all'Autorità di controllo – Autorità Garante per la protezione dei dati personali (d'ora in poi per brevità Autorità Garante) - delle violazioni dei dati personali (c.d. data breach). Una violazione dei dati personali (c.d. data breach) se non affrontata in modo adeguato e tempestivo può provocare danni fisici, materiali o immateriali alle persone fisiche: quali la perdita del controllo dei dati personali che li riguardano o la 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.

Per prevenire o mitigare tali pregiudizi, il Titolare del trattamento deve notificare la violazione, senza ingiustificato ritardo e, ove possibile entro 72 ore da quando ne è venuto a conoscenza all' Autorità Garante. L'obbligo di comunicazione viene meno solo qualora il Titolare ritenga che la violazione dei dati personali presenti un rischio improbabile in termini di pregiudizio per i diritti e le libertà delle persone fisiche.
Nel caso di rischio elevato, oltre alla notifica all'Autorità Garante, il Titolare è tenuto a dare comunicazione della violazione anche all'interessato ai sensi dell'art. 34 del G.D.P.R.
Qualora la notifica non sia effettuata entro 72 ore, essa dovrà essere corredata dei motivi del ritardo. A fronte del mancato rispetto dell'obbligo di notifica l'Autorità Garante può:

- applicare misure correttive previste dall'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati);
- oppure in aggiunta o in luogo delle misure correttive di cui all'art. 58 GDPR irrogare sanzioni amministrative pecuniarie ai sensi dell'art. 83 GDPR (fino a 10.000,000 Euro e per le imprese fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore).

SCOPO/FINALITA' DELLA PRESENTE PROCEDURA

L'Istituto A. Stradella di Nepi, nella persona del Dirigente scolastico, nella sua qualità Titolare del trattamento dei dati personali, ha predisposto la presente procedura interna per una corretta e rapida gestione delle violazioni dei dati personali al fine di:
- assicurare il rispetto delle prescrizioni del G.D.P.R.;
- garantire la migliore tutela dei diritti e libertà degli interessati (alunni, docenti, collaboratori, assistenti amministrativi, famiglie);
- salvaguardare il proprio patrimonio informativo istituzionale.

NORMATIVA E DOCUMENTI DI RIFERIMENTO

La presente procedura è stata redatta sulla base della seguente normativa e documentazione:

• Regolamento UE 679/2016, considerando n. 85, 86, 87, 88 artt. 33, 34;

• Decreto legislativo 196/2003, modificato dal decreto legislativo del 10 agosto 2018, n. 101

• Linee Guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE 2016/679 elaborate dal Gruppo di lavoro articolo 29 per la protezione dei dati personali, adottate il 3 ottobre 2017- versione emendata e adottata in data 6 febbraio 2018.

In particolare si riportano integralmente gli artt. 33 e 34 del G.D.P.R.

Art. 33 del GDPR "Notifica di una violazione dei dati personali all'autorità di controllo"

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, 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, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

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 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.

e) Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

f) 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. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

<u>Articolo 34 del GDPR “Comunicazione di una violazione dei dati personali all'interessato”</u>

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 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.

4. 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 di cui al paragrafo 3 è soddisfatta.

DEFINIZIONI GENERALI

- «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4, punto 1 GDPR);

- “categorie particolari di dati personali”: dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 G.D.P.R.);

- “Dati relativi a condanne penali e reati”: dati personali relativi a condanne penali e a reati o connessi a misure di sicurezza (art. 10 G.D.P.R.);

- trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi

altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, punto 2 GDPR);

- «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, punto 7 GDPR);

- «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4, punto 8 GDPR);

- "autorizzato al trattamento": persona fisica, espressamente designata che opera sotto l'autorità del Titolare del trattamento (art. 29 GDPR e art. 2- quaterdecies D.lgs. n. 196/2003, modificato dal D.Lgs. 10 agosto 2018, n.101,

- «violazione dei dati personali»: 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 (art. 4, punto 12 GDPR);

- «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 (art. 4, punto 21 GDPR- art. 2 bis D.lgs. n. 196/2003, modificato dal D.Lgs. 10 agosto 2018, n. 101);

Strumenti informatici:

- "Dispositivi Fissi": si intendono gli strumenti informatici non facilmente removibili dal perimetro della sede dell'istituto quali personal computer, server locali, stampanti affidati alle persone autorizzate per uso professionale;

- "Dispositivi Mobili": in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili, quali chiavette USB, SD cards, hard disk esterni, tablet e smartphone.

DATA BREACH E POTENZIALI SCENARI

Il GDPR definisce violazione dei dati personali o Data Breach "*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*" (art. 4, n. 12). Le indicazioni di cui alla presente sezione della Procedura valgono per qualsiasi tipologia di Dato personale.

Eventi di Data Breach possono riguardare sia casi cui è connesso un rischio marginale (es. perdita di una chiavetta USB di un dipendente), che casi più critici di furto o perdita di intere basi dati, quali, a titolo esemplificativo, le banche dati gestite dal Titolare del trattamento.

Nel caso si verificasse una delle casistiche riportate di seguito, o un analogo scenario, è fondamentale chiedersi se e quale tipo di Dati personali sono coinvolti nell'evento, e, di conseguenza, procedere alla segnalazione:

1. furto o smarrimento di laptop, smartphone, tablet contenenti Dati personali;
2. furto o smarrimento di documenti cartacei contenenti Dati personali;
3. furto o smarrimento di dispositivi portatili di archiviazione non criptati, come chiavette USB e hard disk esterni, contenenti Dati personali;
4. perdita o modifica irreparabile di archivi contenenti Dati personali in formato cartaceo o digitale (ad esempio, a causa di una errata cancellazione o modifica dai sistemi o dagli archivi digitali che non possa essere ripristinata attraverso l'uso di un backup);
5. diffusione impropria di Dati personali, per mezzo di:

   - invio di e-mail contenente Dati personali al destinatario errato;

   - invio di e-mail con un file contenente Dati personali allegato erroneamente; o esportazione fraudolenta o errata di Dati personali dai sistemi scolastici;

6. richiesta di invio di documenti e file contenenti Dati personali da parte di un esterno che si finge fraudolentemente un collega, collaboratore e/o altro soggetto e conseguente invio allo stesso di tali documenti e file;
7. segnalazione da parte di un fornitore di un evento di Data Breach sui propri sistemi che ha interessato o potrebbe potenzialmente interessare Dati personali del Titolare del trattamento.

GESTIONE DATA BREACH

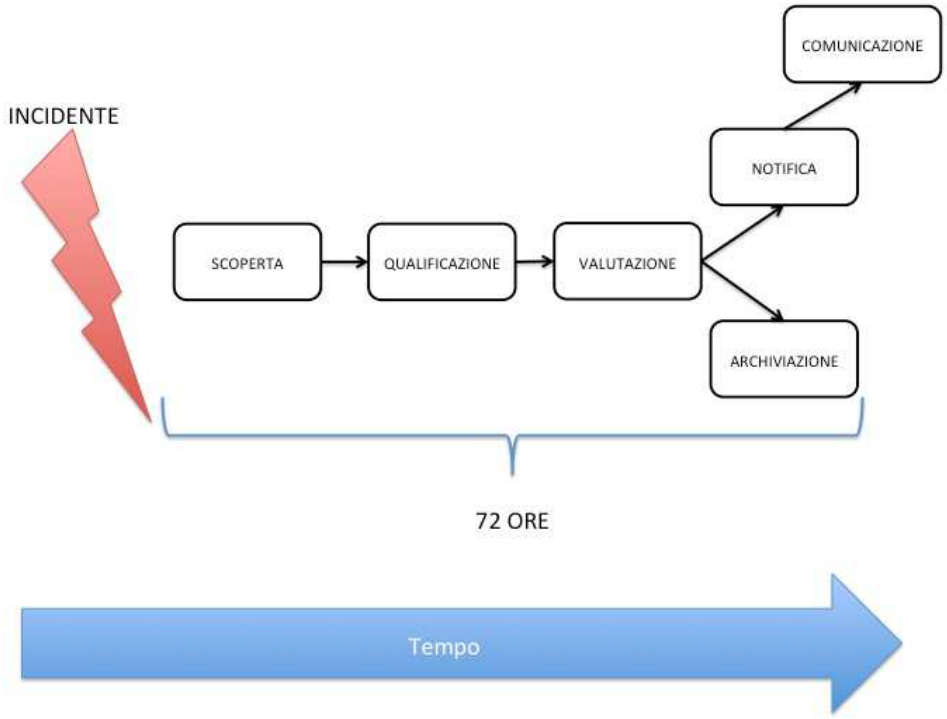
AMBITO DI APPLICAZIONE DELLA PROCEDURA

La presente procedura è rivolta:

- ai **docenti, assistenti amministrativi, DSGA, Dirigente Scolastico e suoi Collaboratori, alunni,** che durante lo svolgimento delle attività scolastiche possono venire a conoscenza di una violazione dei dati personali;
- alle **famiglie** qualora anch'esse vengano a conoscenza di una violazione dei dati personali.

Al fine di consentire una gestione efficace e tempestiva delle violazioni dei Dati personali, il Titolare del trattamento adotta un processo strutturato per la gestione dei casi di Data Breach che prevede:

- Rilevazione e segnalazione del Data Breach;
- Analisi del Data Breach;
- Risposta e notifica del Data Breach;
- Registrazione del Data Breach.



Rilevazione e segnalazione del Data Breach

La rilevazione e segnalazione del Data Breach è un obbligo per tutti i dipendenti e/o collaboratori del Titolare del trattamento.

Nel caso in cui si verifichi uno degli eventi sopradescritti descritti o in tutti gli altri casi in cui il soggetto che tratta dati personali sia consapevole di altri eventi potenzialmente rischiosi per i documenti e gli archivi, è tenuto a informare immediatamente il Dirigente Scolastico il quale provvede – senza indugio – a darne notizia al responsabile per la protezione dei dati personali (DPO).

Nel caso di un incidente informatico, dovrà essere compilata scheda su apposito registro informatico la cui struttura è nella disponibilità del Titolare e del personale amministrativo (Registro Data Breach).

Al registro andranno allegate tutte le comunicazioni relative all'incidente (ad es. denuncia all'autorità giudiziaria, notifica al Garante Privacy e relativa corrispondenza, comunicazioni agli interessati, ecc.).

In tale Registro dovranno essere inseriti tutti gli eventi che determinano o configurano anomalie rispetto alla normale gestione dei sistemi informatici (ad esempio: Virus, perdita di dati, alterazione di dati, attacchi alla rete, furti di credenziali, ecc.).

Analisi del Data Breach

A seguito della rilevazione e/o segnalazione, il Dirigente Scolastico – sentito il Responsabile per la protezione dei dati personali - effettua una valutazione al fine di verificare che nell'incidente rilevato siano stati effettivamente violati Dati personali trattati dall'Istituto.

La suddetta analisi è finalizzata alla raccolta ed identificazione delle seguenti informazioni:

- categorie di Interessati cui i Dati personali violati si riferiscono (ad esempio, utenti, dipendenti, fornitori, etc.);
- categorie di Dati personali compromessi (ad esempio, Dati personali, Dati sensibili, Dati giudiziari);
- tipologia di Data Breach: violazione della riservatezza, disponibilità o integrità (ad esempio, accesso non autorizzato, perdita, alterazione, furto, disclosure, distruzione, etc.).

Nell'ambito di tale analisi, il Titolare del trattamento – con il supporto del DPO - identifica le azioni di prima risposta da intraprendere nell'immediato per contenere gli impatti della violazione dei Dati personali.

Nell'ambito dell'analisi della violazione, vengono identificate anche le seguenti informazioni:

- identificabilità degli Interessati i cui dati rappresentano l'oggetto della violazione;
- misure di sicurezza tecniche e organizzative che potrebbero aver parzialmente o in toto mitigato gli impatti relativi al Data Breach;
- ritardi nella rilevazione del Data Breach;
- numero di individui interessati.

Sulla base dei suddetti parametri, il Titolare del trattamento procede alla valutazione della gravità del Data Breach relativamente ai diritti ed alle libertà degli Interessati, a seconda della

natura dei Dati personali (ad esempio, Dati Sensibili e/o Giudiziari), delle misure di sicurezza adottate, della tipologia di interessati (ad esempio, minori o altri soggetti vulnerabili).

Risposta e notifica del Data Breach

La precedente fase di analisi fornisce al Titolare del trattamento gli strumenti necessari a identificare e valutare le conseguenze negative e gli impatti causati dalla violazione di Dati personali rilevata.

Nel caso in cui dovesse risultare improbabile che il Data Breach presenti rischi per i diritti e le libertà degli interessati, la notifica all'Autorità Garante risulta essere non obbligatoria. Tale valutazione è condivisa con il DPO.

Qualora al contrario dovesse risultare possibile che il Data Breach presenti rischi per i diritti e le libertà degli Interessati, il Dirigente Scolastico, con il supporto del DPO, procedere a predisporre la notifica all'Autorità Garante secondo il modello pubblicato nella sezione privacy del sito istituzionale (Modulo per notifica al Garante).

La notifica viene effettuata all'Autorità Garante entro 72 ore dal momento in cui il Data Breach è stato rilevato.

Nel caso in cui la valutazione del Titolare comporti la necessità della notifica, questa va trasmessa al Garante per la protezione dei dati personali, inviandola all'indirizzo: protocollo@pec.gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario. L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "notifica violazione dati personali" e opzionalmente la denominazione del Titolare del trattamento.

La suddetta notifica contiene almeno le seguenti informazioni:

- natura della violazione dei dati personali (disclosure, perdita, alterazione, accesso non autorizzato, etc.);
- tipologie di Dati personali violati;
- categorie e numero approssimativo di Interessati cui i dati compromessi si riferiscono;
- nome e dati di contatto del DPO, che sarà l'interfaccia per Titolare del trattamento nei confronti dell'Autorità di controllo;
- probabili conseguenze della violazione dei Dati personali;

- descrizione delle misure che il Titolare del trattamento ha adottato o è in procinto di adottare al fine di mitigare le conseguenze del Data Breach;
- ove la stessa non sia presentata entro 48/72 ore dalla rilevazione, i motivi dell'eventuale ritardo nella comunicazione.

Qualora non sia stato possibile fornire contestualmente tutte le informazioni obbligatorie, il Dirigente Scolastico raccoglie quanto prima le informazioni supplementari e provvede a integrare, senza ritardo, la notifica già inoltrata all'Autorità di Controllo.

Comunicazione/Notifica agli interessati

Oltre a notificare il Data Breach all'Autorità Garante, il Titolare del trattamento è tenuto a valutare l'esigenza di procedere con la denuncia all'Autorità Giudiziaria competente, nonché con la notifica del Data Breach anche ai soggetti interessati i cui dati siano stati violati.

Per stabilire se sia necessario provvedere alla notifica agli Interessati, il Titolare del trattamento, di concerto con il DPO, deve valutare i seguenti fattori:

1) il trattamento può comportare discriminazioni, furto d'identità, perdite finanziare, disturbi psicologici, pregiudizio alla reputazione, perdita di riservatezza dei Dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo;
2) gli Interessati rischiano di essere privati dei loro diritti, delle libertà o venga loro impedito l'esercizio del controllo sui Dati personali che li riguardano;
3) sono trattati Dati personali che rivelano l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;
4) in caso di valutazione di aspetti personali, in particolare 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;
5) sono trattati Dati personali di persone fisiche vulnerabili, in particolare minori;
6) il trattamento riguarda una notevole quantità di Dati personali e un vasto numero di Interessati.

La notifica agli Interessati deve, pertanto, avvenire nel caso in cui la violazione di Dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, a meno che non sia verificata almeno una delle seguenti condizioni:

- sono state applicate adeguate misure tecniche e organizzative per proteggere i dati prima della violazione, in particolare quelle in grado di renderle non intelligibili per soggetti terzi non autorizzati (ad esempio, misure di cifratura);
- a valle della rilevazione del Data Breach, sono state adottate misure per impedire il concretizzarsi dei rischi per i diritti e le libertà degli Interessati;
- la notifica del Data Breach a tutti gli Interessati singolarmente comporta uno sforzo sproporzionato rispetto al rischio. In tal caso occorrerà comunque procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati siano comunque informati con analoga efficacia.

Il Dirigente Scolastico, di concerto con il DPO, valuta di volta in volta, sulla base della tipologia e del numero di Interessati, il canale di comunicazione che appare più opportuno per trasmettere la notifica agli stessi.

Il considerando 85 del GDPR spiega che lo scopo della notifica è di limitare i danni che possono derivare per effetto di una violazione a carico degli interessati e che l'efficacia di questo dovere di limitazione dipende dalla tempestività e dall'adeguatezza con cui la violazione è affrontata.
Il gruppo " Article 29 Data Protection Working Party " (WP 29), chiarisce ulteriormente che la responsabilità del titolare deve essere commisurata secondo la sua capacità di scoprire tempestivamente un incidente ed indagarlo al fine di valutare l'obbligatorietà della notifica.

In caso di:

1) *Rischio assente:* la notifica al Garante non è obbligatoria. Tale ipotesi si verifica ad esempio quando i dati personali, oggetto della violazione, sono dati pubblici.
2) *Rischio presente:* è necessaria la notifica al Garante.
3) *Rischio elevato:* è necessaria la notifica al Garante e la comunicazione anche agli interessati. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali (ad. esempio dati vaccinali, relativi alla salute degli alunni);
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);

- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. alunni minorenni: ad. esempio in caso di dati personali relativi all'indirizzo di residenza).

Come detto, nel caso in cui dal data breach possa derivare **un rischio elevato** per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.
Il Dirigente Scolastico coadiuvato dal DPO predispone una comunicazione con un linguaggio semplice e chiaro da inviare all'interessato/agli interessati e da lui sottoscritta.
La comunicazione deve contenere:
a) nome e i dati di contatto del Titolare o di altra persona presso cui ottenere più informazioni;
b) descrizione delle probabili conseguenze della violazione dei dati personali;
c) descrizione delle 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.

Di seguito si riporta una tabella, tratta dalle *Linee Guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE 2016/679, elaborate dal Gruppo di lavoro articolo 29 per la protezione dei dati, adottate il 3 ottobre 2017, versione emendata e adottata in data 6 febbraio 2018,* contenente alcuni esempi di possibili violazioni di dati personali e di comportamenti da assumere. L'elencazione è da considerarsi meramente esemplificativa:

ESEMPIO NOTIFICA ALL'AUTORITA' GARANTE? COMUNICAZIONE	**NOTIFICA ALL'AUTORITA' GARANTE?**	**COMUNICAZIONE ALL'INTERESSATO?**	**NOTE/ RACCOMANDAZIONI**

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.
Un titolare del trattamento subisce un 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	Sì, effettuare la segnalazione all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	Sì, effettuare la segnalazione alle 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.	Se fosse stato disponibile un backup e i dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in

dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.			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'articolo 32.
Una e-mail viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo email 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 o se altri fattori	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

	presentano rischi elevati (ad esempio, il messaggio di posta elettronica contiene le password iniziali).		

Allegato 1 – Registro Data Breach

Allegato 2 – Modulo Segnalazione Data Breach

Nepi, 05/02/2021