ISTITUTO COMPRENSIVO - "ARDITO - DON BOSCO"-LAMEZIA TERME
Prot. 0005460 del 25/04/2023
IV (Uscita)

ISTITUTO COMPRENSIVO ARDITODON BOSCO
88046 LAMEZIA TERME
Viale Michelangelo, 1 - Tel. 0968/22030 - Fax 0968/23700 - Cod. Mecc. CZIC864001 -
C.F. 82006620791 e mail: czic864001@istruzione.it czic864001@pec.istruzione.it sito web www.arditodonbosco.gov.it

Gestione degli eventi di violazione dati (Data Breach)

Il Regolamento UE 2016/679 disciplina la violazione dei dati personali (artt. 33 e 34) e, preventivamente, la previsione di misure tecniche e organizzative (art. 32) idonee a garantire un livello di sicurezza adeguato al rischio, nel rispetto del principio di accountability (responsabilizzazione) in capo al Titolare del trattamento (Istituto scolastico). Il presente documento affronta le conseguenze del verificarsi del rischio, e quindi la gestione di una eventuale violazione di dati (redatto in parte sulla base delle Linee guida del Gruppo di Lavoro art. 29 per la protezione dei dati " Comitato Europeo per la Protezione dei Dati").

Cos'è il Data Breach (Violazione di dati personali)

Il Data Breach è una 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. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
Alcuni possibili esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- 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 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.
L'evento dannoso può essere fisico/logistico (furto, calamità naturale, incendio, distruzione, …) o informatico (accesso non autorizzato al sistema, virus, malfunzionamento software, …).

Considerazioni di base in materia di sicurezza

Per impostare il livello di sicurezza informatica delle PA, Agid ha emanato delle misure minime di sicurezza ICT (Tecnologie riguardanti i sistemi integrati di telecomunicazione), che in base alla realtà organizzativa dell'ente possono essere implementate in modo graduale seguendo tre livelli di attuazione: minimo, standard o avanzato. Tali misure sono un importante supporto metodologico, oltre che un mezzo attraverso il quale le Amministrazioni, soprattutto quelle più piccole e che hanno meno possibilità di avvalersi di professionalità specifiche, possono verificare autonomamente la propria situazione e avviare un percorso di monitoraggio e miglioramento.
L'Istituto scolastico, in considerazione della propria organizzazione e delle risorse disponibili, ha attuato le

misure ritenute idonee a garantire dei livelli di sicurezza standard, che vengono periodicamente verificate e adeguate quando necessario.
Il Regolamento GDPR, inoltre, impone tanto al titolare quanto al responsabile del trattamento di disporre di misure tecniche e organizzative adeguate a garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati. Tali soggetti dovrebbero tenere conto: dello stato dell'arte e dei costi di attuazione; della natura, dell'oggetto, del contesto e delle finalità del trattamento; del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
Inoltre, il Regolamento impone di mettere in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali, il che a sua volta consente di stabilire se scatta l'obbligo di notifica.

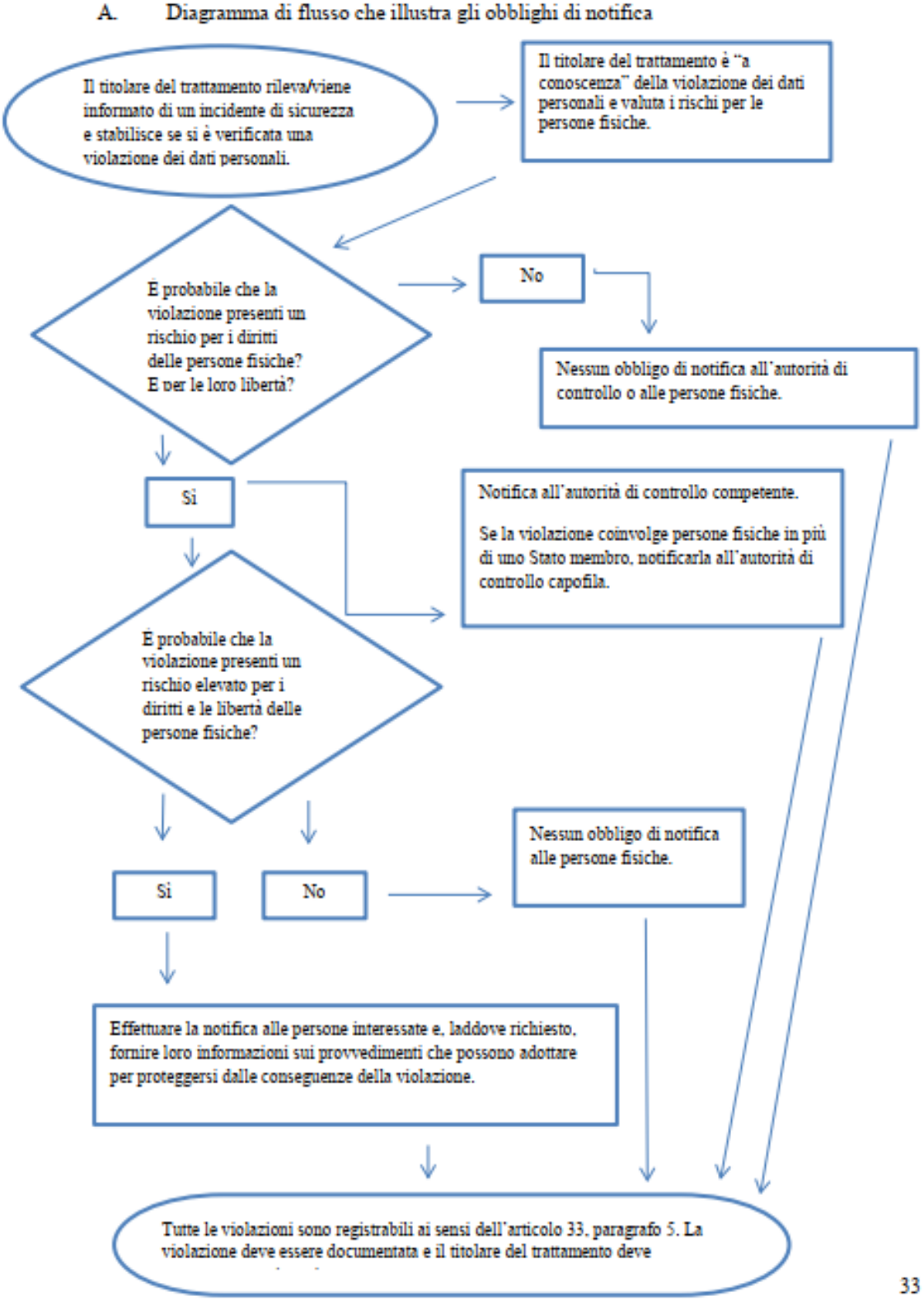
Tipi di violazioni di dati personali e possibili conseguenze
Le violazioni possono essere classificate in base ai seguenti tre principi della sicurezza delle informazioni:

- "*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 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.
Una violazione può avere potenzialmente numerosi effetti negativi significativi sulle persone fisiche, che possono causare danni fisici, materiali o immateriali, ad esempio la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo alle persone fisiche interessate. Di conseguenza, 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.

Quando effettuare la notifica

Art. 33 GDPR: *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*.
Questo solleva la questione relativa al momento in cui il titolare del trattamento può considerarsi "a conoscenza" di una violazione. Il Gruppo di lavoro ritiene che il titolare del trattamento debba considerarsi "a conoscenza" nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali. 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 posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario. Il titolare del trattamento dovrebbe inoltre disporre di accordi con i responsabili del trattamento ai quali fa ricorso, i quali hanno a loro volta l'obbligo di notificare al titolare del trattamento eventuali violazioni.



Le figure coinvolte e cosa devono fare

Abbiamo visto come la tempestività sia importante per poter valutare se un evento si possa configurare come violazione, e nel caso se si determinano effettivi pregiudizi per gli interessati. A volte questa analisi può richiedere tempo per:

- rilevare l'anomalia
- accertarsi della sua natura
- individuare le cause

- valutare gli effetti
- coinvolgere il Responsabile del trattamento (se interessato)
- ottenere riscontri da parte del Responsabile
- valutare se ci sono stati effetti sui dati (perdita, modifica, furto, ecc…)
- valutare il rischio per gli interessati

Ma chi sono i soggetti coinvolti nell'organizzazione del Titolare?

Personale: il personale della scuola, docente e ata, opera a vario titolo nell'organizzazione e tratta i dati di propria pertinenza, in base al ruolo svolto e alle funzioni assegnate. Il dipendente che, nello svolgimento dei propri compiti, rileva un'anomalia che si può potenzialmente configurare come violazione dati, deve immediatamente informare il Dirigente scolastico, l'animatore digitale, il referente informatico, il responsabile di plesso o qualunque altra figura di riferimento in relazione al tipo di evento, per poter tempestivamente intervenire e valutare quando accaduto. Le violazioni riscontrate potrebbero essere non solo informatiche, ma anche fisiche (es. perdita di un fascicolo, distruzione di una pendrive) e i comportamenti da seguire sono i medesimi in entrambi i casi, perché la perdita di un documento cartaceo contenente dati personali non è meno importante dell'invio a terzi di documenti a mezzo email. E' grave colpa del dipendente omettere tali informazioni, che potrebbero compromettere la sicurezza di molti e determinare serie responsabilità in capo al Titolare del trattamento.

Alunni/Famiglie: anche gli alunni o i loro familiari/tutori che dovessero rilevare delle anomalie o dei malfunzionamenti delle piattaforme didattiche utilizzate, entrare in possesso di documenti altrui, venire a conoscenza di credenziali di accesso non proprie, ricevere per errore dalla scuola email o comunicazioni con documenti o contenuti non destinati a loro, devono darne immediata comunicazione al Dirigente scolastico o, in caso di irreperibilità, contattare il coordinatore di classe o inviare una email all'indirizzo di posta elettronica della scuola segnalando la potenziale violazione ma senza inserire informazioni sui dati di cui si è venuti a conoscenza.

E' grave colpa omettere tali eventi, che potrebbero compromettere la sicurezza di molti e determinare serie responsabilità in capo al Titolare del trattamento.

Figure informatiche: sono quei soggetti interni alla scuola che si occupano delle attività informatiche e digitali della scuola. L'animatore digitale, l'amministratore della piattaforma cloud, la funzione strumentale per il sito web, l'assistente tecnico, cioè tutte quelle figure che con ruoli e compiti diversi (che possono anche coincidere in capo ad una stessa persona) di occupano della parte digitale/informatica della scuola. Possono anche esistere figure esterne incaricate, ad esempio un amministratore di sistema, che gestisce la manutenzione hardware dei dispositivi utilizzati a scuola. Tutte queste figure possono essere coinvolte, singolarmente o congiuntamente, nella gestione di una violazione dati per quanto di propria pertinenza. L'incaricato che, nello svolgimento delle proprie funzioni, rileva un'anomalia che si può potenzialmente configurare come violazione dati, deve immediatamente informare il Dirigente scolastico ed è grave colpa omettere tali eventi, che potrebbero compromettere la sicurezza di molti e determinare serie responsabilità in capo al Titolare del trattamento.

Responsabile del Trattamento: è il soggetto che tratta in modo stabile e continuativo i dati per conto del titolare, per effetto di un contratto o atto giuridico che vincoli il responsabile al titolare. Deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato. E' tale, ad esempio, il fornitore del Registro elettronico o il fornitore della piattaforma didattica cloud. Il Responsabile ha precisi compiti e obblighi per i dati trattati e deve collaborare con il Titolare in caso di violazioni. Sebbene il titolare del trattamento conservi la responsabilità generale per la protezione dei dati personali, il responsabile del trattamento svolge un ruolo importante nel consentire al titolare del trattamento di adempiere ai propri obblighi, segnatamente in materia di notifica delle violazioni. Se il titolare del trattamento 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, il responsabile del trattamento deve notificarla al titolare "senza ingiustificato ritardo". Va notato che il responsabile non deve valutare la probabilità di rischio derivante dalla violazione prima di notificarla al titolare del trattamento; spetta infatti a quest'ultimo effettuare la valutazione nel momento in cui viene a conoscenza della violazione. Il responsabile del trattamento deve soltanto stabilire se si è verificata una violazione e quindi notificarla al titolare del trattamento. Poiché quest'ultimo si serve del responsabile del trattamento per conseguire le proprie finalità, in linea di principio dovrebbe considerarsi "a conoscenza" della violazione non appena il responsabile del trattamento gliela notifica. L'obbligo del responsabile del trattamento di effettuare la notifica al titolare consente a quest'ultimo di far fronte alla violazione e di stabilire se deve notificarla all'autorità di controllo.

Responsabile della Protezione dei Dati (RPD)**:** è un soggetto esterno che ha la funzione di affiancare titolare, addetti e responsabili del trattamento affinché gestiscano i dati in modo da minimizzare i rischi per gli interessati, seguendo i princìpi e le indicazioni del Regolamento europeo.
Nel caso in cui il titolare del trattamento riscontri una violazione dati, consulta il proprio RPD, che può fornire supporto sulle procedure da attuare e affiancare il titolare nella comunicazione all'autorità di controllo.

Cosa fa il Titolare del trattamento dopo la segnalazione

Il dirigente scolastico coinvolge immediatamente le figure interne di cui si avvale per affrontare le questioni informatiche e tecniche e consulta il proprio RPD, procedendo ad analizzare gli eventi segnalati per valutare se può configurarsi una effettiva violazione dati. Si prendono in considerazione i fatti, si ricostruiscono le fasi, si considerano le circostanze, cercando di individuare i possibili rischi derivanti e attuando le misure che possano risolverli o contenerli. Qualora l'esito delle valutazioni dovesse far emergere una effettiva violazione e un pregiudizio grave per gli interessati, il Dirigente dovrà valutare la necessità di effettuare la comunicazione all'autorità garante ed eventualmente agli interessati a cui i dati appartengono. Il tempo previsto per la comunicazione è di 72 ore ma, se le circostanze non consentono il rispetto dei tempi previsti, la notifica al Garante dovrà essere corredata dai motivi del ritardo. La riscontrata violazione dovrà essere anche annotata nel Registro delle violazioni.

Quando non è richiesta la notifica

L'articolo 33, paragrafo 1, del GDPR chiarisce che se è "improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche" tale violazione non è soggetta a notifica all'autorità di controllo. E' quindi necessario valutare la tipologia di informazioni violate, la natura, la tipologia di violazione per decidere se ci sono i presupposti della notifica.
Se, ad esempio, si compromette una pendrive su cui erano archiviati documenti organizzativi come l'orario delle lezioni e l'elenco dei docenti divisi per classi, non si configura nessun rischio per i diritti degli interessati (cioè dei docenti), perché tale perdita non determina alcun pregiudizio per gli stessi, ma solo l'onere amministrativo di dover ricomporre quegli elenchi.

Comunicazione all'interessato

In alcuni casi, oltre a effettuare la notifica all'autorità di controllo, il titolare del trattamento è tenuto a comunicare la violazione alle persone fisiche interessate, laddove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche. La soglia per la comunicazione delle violazioni alle persone fisiche è quindi più elevata rispetto a quella della notifica alle autorità di controllo, pertanto non tutte le violazioni dovranno essere comunicate agli interessati, il che li protegge da inutili disturbi arrecati dalla notifica. Il regolamento afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "senza ingiustificato ritardo", il che significa il prima possibile. L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi. Va tenuto presente che, sebbene la comunicazione possa inizialmente non essere richiesta se non vi è alcun rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato. Se il titolare del trattamento decide di non comunicare una violazione all'interessato, l'autorità di controllo può richiedere che lo faccia, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato.

Notifica al Garante privacy

Quando ricorrono le circostanze per effettuare la notifica all'autorità garante, essa deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/.
La procedura attivata dal Garante prevede:

- *uno strumento di autovalutazione*, che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza;
- *un fac-simile* del modello di notifica, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante;
- la compilazione del format telematico utilizzando la firma digitale

A seguito della notifica, il Garante può prescrivere misure correttive (v. art. 58, paragrafo 2, del

Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Possono essere previste sanzioni pecuniarie.

IL DIRIGENTE SCOLASTICO
Dott.ssa Margherita PRIMAVERA