Ministero dell' Istruzione, dell'Università e della Ricerca
ISTITUTO COMPRENSIVO EST 1 – BRESCIA
Via A. Del Verrocchio, 328, 25124 BRESCIA – BSIC878006 - C. F. 98093050171 Tel. 0302306867 Fax 0302306462
bsic878006@istruzione.it; bsic878006@pec.istruzione.it www.istitutocomprensivoest1.gov.it

Data Breach

Valutazione delle violazioni di dati o sistemi

Revisione	*Data*
2019_1109	*17/11/2019*

Proposta da **Responsabile Protezione Dati**

Adottata da **Dirigente Scolastico**

Destinatari **U.O. segreteria**

U.O. docenti

U.O. personale ausiliario

Riferimenti normativi

Documento WP250rev.01 Linee guida sulla notifica delle violazioni

GDPR articolo 33 e articolo 34

Articolo 33 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.

4. 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.
5. 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.

Articolo 34 Comunicazione di una violazione dei dati personali all'interessato (C86-C88)

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.

Premessa

Lo scopo di questa procedura è quello di definire gli elementi che caratterizzano una violazione di dati personali al fine di:

- riconoscere una violazione;
- valutare le conseguenze;

- valutare gli adempimenti derivanti;
    - comunicazione al garante
    - comunicazione agli interessati
- valutare le misure di sicurezza da correggere o adottare.

La valutazione, da parte del Titolare, deve essere effettuata tempestivamente, possibilmente entro 72 ore dalla sua conoscenza (articolo 33 paragrafo 1). Se la violazione avviene sui sistemi affidati ad un responsabile, questi ne informa il Titolare "senza ingiustificato ritardo". Da quel momento, e non dal verificarsi della violazione, decorreranno le 72 ore per la valutazione e la eventuale segnalazione.

È quindi necessario riconoscere innanzitutto che si è verificata una violazione.

> *Articolo 4 punto 12 (definizioni)*
>
> *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*

il concetto di "perdita" necessita di un approfondimento. Secondo il Garante:

> *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*

Tipi di violazione

Le violazioni possono esser classificate in base a tre principi:
"violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzato o accidentale;
"violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
"violazione della disponibilità", in caso di perdita, accesso[15] o distruzione accidentali o non autorizzati di dati personali.

La valutazione della violazione della disponibilità può avere elementi di indeterminatezza. Una perdita o una distruzione permanenti dei dati saranno sempre considerate violazioni della disponibilità.
Tuttavia, come possiamo considerare la indisponibilità temporanea? Alcuni esempi:

- virus che ci priva della disponibilità dei dati che, in breve tempo, recuperiamo dalle copie;
- guasto subito da un apparato o da una memoria dei quali possiamo risalire ad una copia precedente;
- indisponibilità della connessione web che non ci consente di accedere ai dati presenti su portali web.

Afferma il Garante che:

> *nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".*

> *Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche.*

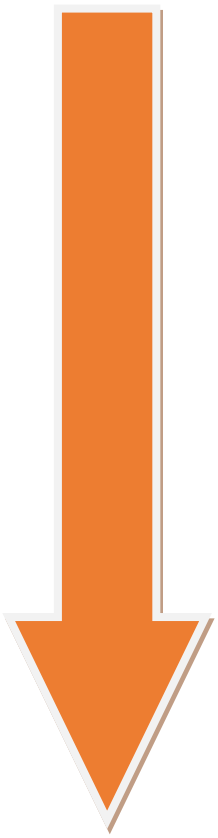
Dunque, anche un evento che ci ha privato temporaneamente della disponibilità dei dati DEVE comportare una valutazione dell'impatto che può avere avuto sui diritti e sulle libertà delle persone, così come una perdita di disponibilità definitiva, un accesso non autorizzato o la diffusione non controllata.
Risulta quindi fondamentale che il titolare, e in alcuni casi prima di lui il responsabile, ne venga a conoscenza tempestivamente.
Non tutte le violazioni attiveranno la necessità di notificare al Garante o agli interessati, ma senz'altro tutte dovranno essere annotate (articolo 33 paragrafo 5) nei loro elementi salienti così come dovranno essere annotate le valutazioni in base alle quali verranno prese le decisioni successive.

Fasi

Possiamo suddividere la procedura di valutazione delle violazioni nelle seguenti fasi:

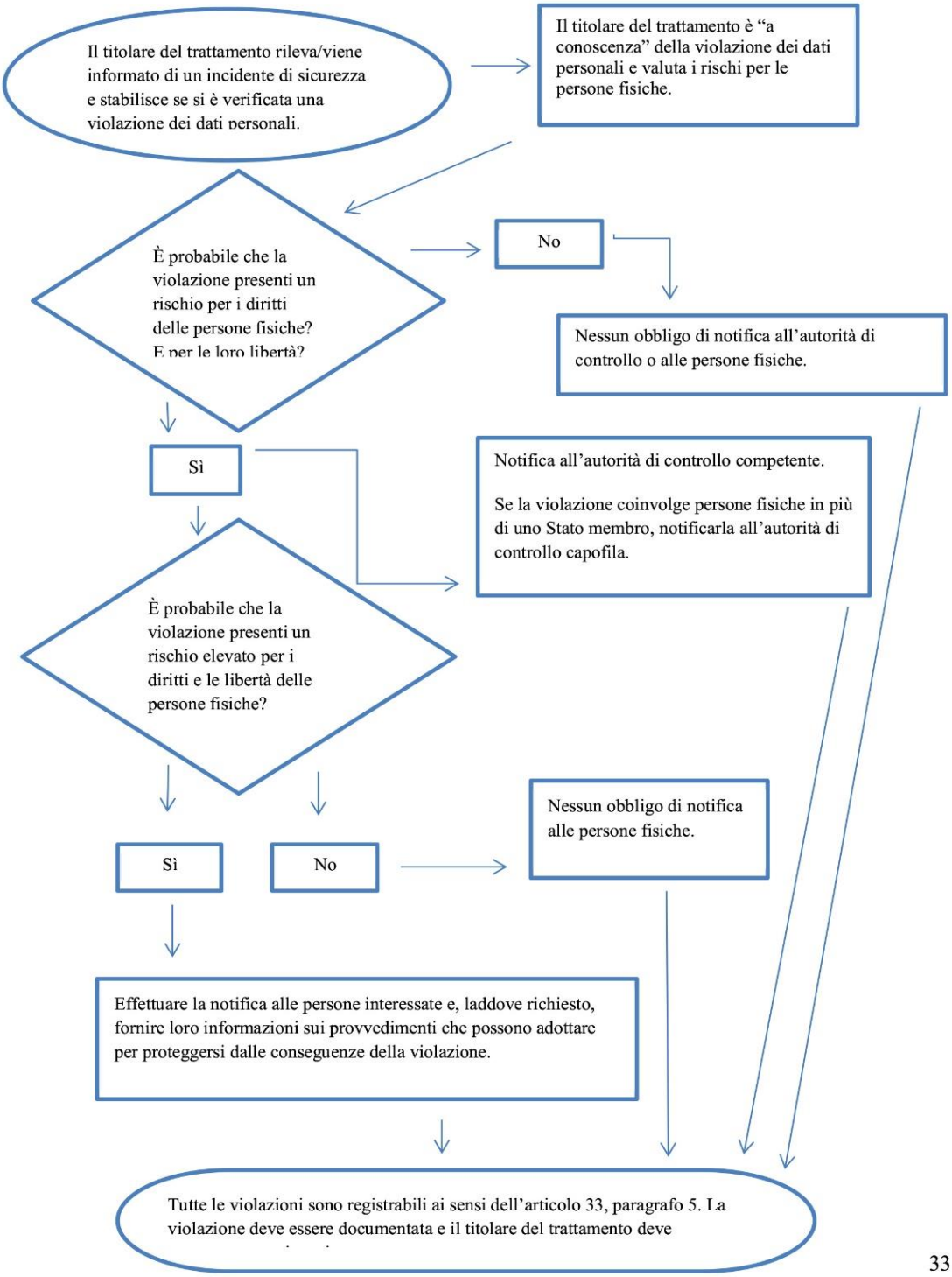
a) riconoscimento del sussistere della violazione
b) comunicazione degli elementi da valutare
c) annotazione sul registro art 33 par 5
d) valutazione degli elementi
e) eventuale notifica al Garante
f) eventuale notifica agli interessati
g) completamento dell'annotazione sul registro art 33 par 5
h) eventuale indicazione di nuove misure di sicurezza e loro verifica

inseriamo il diagramma delle fasi contenuto nel documento WP250



VII. **Allegato**

A. Diagramma di flusso che illustra gli obblighi di notifica



In dettaglio:

a) Riconoscimento della violazione

Una violazione è un incidente di sicurezza, ma non tutti gli incidenti di sicurezza comportano violazione di dati personali.
Questa affermazione di principio, sempre citata dal documento WP250, ci fa capire che dobbiamo tenere conto e valutare **ogni incidente di sicurezza**.

Tabella incidenti di sicurezza

Perdita di uno o più documenti o fascicoli intestati ad un interessato
accesso o utilizzo da parte di terzi non autorizzati a documenti o fascicoli intestati ad un interessato
invio o consegna a terzi non legittimati di documenti o fascicoli intestati ad un interessato
guasto ad una memoria di massa che ne pregiudichi l'utilizzo
smarrimento di una memoria di massa
guasto ad un dispositivo di elaborazione che lo renda inutilizzabile
smarrimento di un dispositivo di elaborazione
cancellazione di documenti, cartelle o unità logiche contenenti dati personali
compromissione di documenti, cartelle o unità logiche contenenti dati personali
collegamento non autorizzato da parte di terzi, con permessi di lettura o modifica, a sistemi contenenti dati
Utilizzo di credenziali di autenticazione per accesso a sistemi, programmi, portali, da parte di soggetti non legittimati
invio mediante posta elettronica di documenti o dati a terzi non legittimati
invio massivo di email a liste di soggetti senza utilizzare la funzione di CCN o BCC
guasto alla infrastruttura di connessione web che impedisce la raggiungibilità di servizi di elaborazione esterni

questi incidenti sono riscontrabili dagli incaricati che operano per conto del titolare o del responsabile dei trattamenti.

Se uno di questi incidenti occorre, ad esempio, ad un responsabile di trattamenti esterni, il Titolare dovrà ricevere la notizia solo al fine di valutare le conseguenze per gli interessati e l'eventuale necessità di informarli. La valutazione relativa alla necessità di notifica al garante dovrà essere fatta dal Responsabile stesso, in qualità, a sua volta, di Titolare.

È anche possibile che non si abbia riscontro di un indicente o di una violazione fino a quando non ne diventi evidente la conseguenza. In alcuni casi potrebbe arrivare da fonti esterne la notizia che interi archivi o parti di essi sono stati resi pubblici o sono disponibili su piattaforme di condivisione o di commercio, legali o meno.

b) Comunicazione degli elementi da valutare

L'incaricato, o qualsiasi altro soggetto che venga a conoscenza, per una delle casistiche elencate al punto precedente, di una violazione fra quelle elencate, o di altra natura e tipologia ma per la quale abbia il dubbio che sussista la necessità di valutazione da parte del Titolare, è tenuto a comunicare quanto accaduto ad una delle seguenti funzioni:

responsabili d'area	D.S.G.A.
amministratori di sistema	Secondo organigramma
responsabile protezione dati	Pro tempore

Il destinatario della comunicazione annoterà tutti gli elementi significativi dell'evento e li trasmetterà al RPD, a meno che la segnalazione non sia stata fatta direttamente a lui, a mezzo email all'indirizzo rpd@vincenzi.com

c) annotazione sul registro art 33 par 5

il RPD istituisce un registro degli incidenti di sicurezza nel quale annoterà:

data e rora di conoscenza	
data e ora dell'indicente (se possibile)	
Fonte della segnalazione	
elementi coinvolti	
Sistemi	
Programmi	
Memorie	
archivi e documenti	
categorie di dati personali	
Interessati o categorie di interessati	
descrizione dell'incidente	
Presenza di rischio per PPFF	
presenza rischio elevato per diritti e libertà di PPFF	
Azioni intraprese	
Data	Annotazione

Il RPD dovrà valutare la necessità di raccogliere altre informazioni sia dalla fonte della segnalazione che da altre funzioni aziendali o esterne coinvolte o che possano fornire elementi utili alla valutazione da compiere.

Il RPD trasmetterà per iscritto quanto prima gli elementi e l'esito della propria valutazione al Titolare il quale, sentiti, se ritenuti necessari, anche altri pareri, deciderà riguardo alla classificazione dell'incidente e della eventuale relativa violazione.

d) Valutazione degli elementi

Il RPD, nel compilare il registro previsto al punto precedente, dovrà esprimere una valutazione al fine di determinare la necessità di procedere con gli adempimenti previsti ai due punti successivi.
Gli elementi sono:

Che tipo di violazione?

A. violazione della riservatezza
B. violazione dell'integrità
C. violazione della disponibilità
D. indisponibilità temporanea significativa
E. violazione di sicurezza
• *distruzione,*
• *perdita,*
• *modifica,*

• *divulgazione non autorizzata* • *accesso ai dati personali non autorizzato*	
quali categorie di dati sono stati oggetto della violazione?	
Quanti interessati, approssimativamente, ha riguardato la violazione?	
Ci sono evidenze di diffusione dei dati o delle informazioni?	
Ci sono evidenze di utilizzo dei dati o delle informazioni?	
Abbiamo recuperato la disponibilità dei dati?	
se SI, dopo quanto tempo?	

Esito:

A) La violazione presenta un rischio per i diritti e le libertà delle persone fisiche SI NO

B) La violazione presenta un rischio elevato per i diritti e le libertà delle persone fisiche SI NO

In caso di esito positivo A procedere al punto e)

In caso di esito positivo B procedere al punto f)

e) eventuale notifica al Garante

caso 1) compilazione e invio da parte del Titolare

il RPD provvede a verificare sul sito web dell'Autorità Garante la presenza di un modulo di invio della segnalazione di "data breach" aggiornato e delle relative istruzioni.

Una volta individuato il modulo corretto, il RPD ne predispone la compilazione includendo, se necessari, documenti allegati a corredo delle motivazioni.

Il documento dovrà essere condiviso con il Titolare e da questi inviato secondo le modalità previste.

Il RPD indicherà i propri recapiti come contatti per l'Autorità e seguirà personalmente eventuali richieste o comunicazioni che debbano pervenire per definire la pratica.

Caso 2) invio da parte del responsabile di trattamento esterno

Qualora l'analisi dell'evento riveli che la violazione è dovuta alla responsabilità del soggetto al quale il Titolare ha affidato il trattamento o parte di esso, la comunicazione sarà d questi dovuta.

Il RPD verificherà che la comunicazione avvenga nei tempi previsti e provvederà a farsi rilasciare idonea documentazione dell'evento e dei tempi di invio.

Resta a carico del RPD la valutazione della necessità di procedere comunque alla segnalazione agli interessati.

f) eventuale notifica agli interessati

il RPD valuterà la necessità di informare gli interessati del fatto che si sia verificato l'evento di violazione e condividerà le sue valutazioni con il Titolare.

Il Titolare, congiuntamente al RPD, valuterà quanto emerso alla luce del contenuto del WP250, del quale riportiamo alcuni passaggi:

L'articolo 34, paragrafo 1, del GDPR afferma che:
"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".

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.

Ai fini della comunicazione alle persone fisiche, il titolare del trattamento deve fornire almeno le seguenti informazioni:
• una descrizione della natura della violazione;
• il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
• una descrizione delle probabili conseguenze della violazione;
• una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

In linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c).
Nel comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard. Ciò contribuisce a rendere la comunicazione della violazione chiara e trasparente.
completamento dell'annotazione sul registro art 33 par 5

vedi punto c)

le sezioni:

Presenza di rischio per PPFF	
presenza rischio elevato per diritti e libertà di PPFF	
Azioni intraprese	
Data	Annotazione

Vanno compilate dal RPD dopo che è stata fatta la valutazione.

g) eventuale indicazione di nuove misure di sicurezza e loro verifica

alla luce dell'analisi di quanto si è verificato, in modo particolare nel caso che la violazione sia avvenuta su sistemi o procedure la cui responsabilità sia in carico al Titolare, e non ad un responsabile esterno, il RPD analizzerà, con l'aiuto dell'amministratore di sistema, le implicazioni tecniche che hanno portato al verificarsi dell'evento, al fine di produrre un piano di miglioramento che può andare in una delle seguenti direzioni:

- miglioramento del livello di sicurezza tecnico dei sistemi;
- adeguamento delle procedure di trattamento;
- formazione del personale;
- richiesta di adeguamento di procedure e strumenti al responsabile dei trattamenti;
- implementazione o miglioramento del monitoraggio dell'efficacia delle misure di sicurezza.

Le misure individuate come correttive ed efficaci per prevenire il verificarsi di nuovi eventi, andranno condivise con il Titolare che disporrà della loro attuazione.

IL DIRIGENTE SCOLASTICO
Gaetano Greco

Firmato da:
GRECO GAETANO
Codice fiscale: GRCGTN64B29C351W
17/11/2019 11:24:21