Procedura di DATA BREACH

dell'Istituto

prot. _____ del _____

Sommario

Il presente documento ha l'obiettivo di descrivere il processo adottato dall'Istituzione Scolastica per la gestione dei *data breach* ovvero quegli eventi di violazione dell'integrità, riservatezza e disponibilità degli archivi cartacei o elettronici che contengono dati personali ai sensi del nuovo regolamento europeo in materia di protezione dei dati personali (*REGOLAMENTO (UE) 2016/679*, noto anche come *GDPR – General Data Protection Regulation*).

1 DEFINIZIONE

Il concetto di *"data breach"* è definito nell'art. 4 del GDPR dove è prescritto che per "violazione dei dati personali" si intende *"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"* (Fonte: GDPR, art. 4)

Partendo da tale definizione, nei successivi articoli 33 e 34 del GDPR è disciplinata la procedura di "Notifica di una violazione dei dati personali all'autorità di controllo" nonché di "Comunicazione di una violazione dei dati personali all'interessato".

L'art. 33 in materia di "Notifica di una violazione dei dati personali all'autorità di controllo" prescrive che: *"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".

Il successivo art. 34, in materia di "Comunicazione di una violazione dei dati personali all'interessato" prescrive che: *"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).

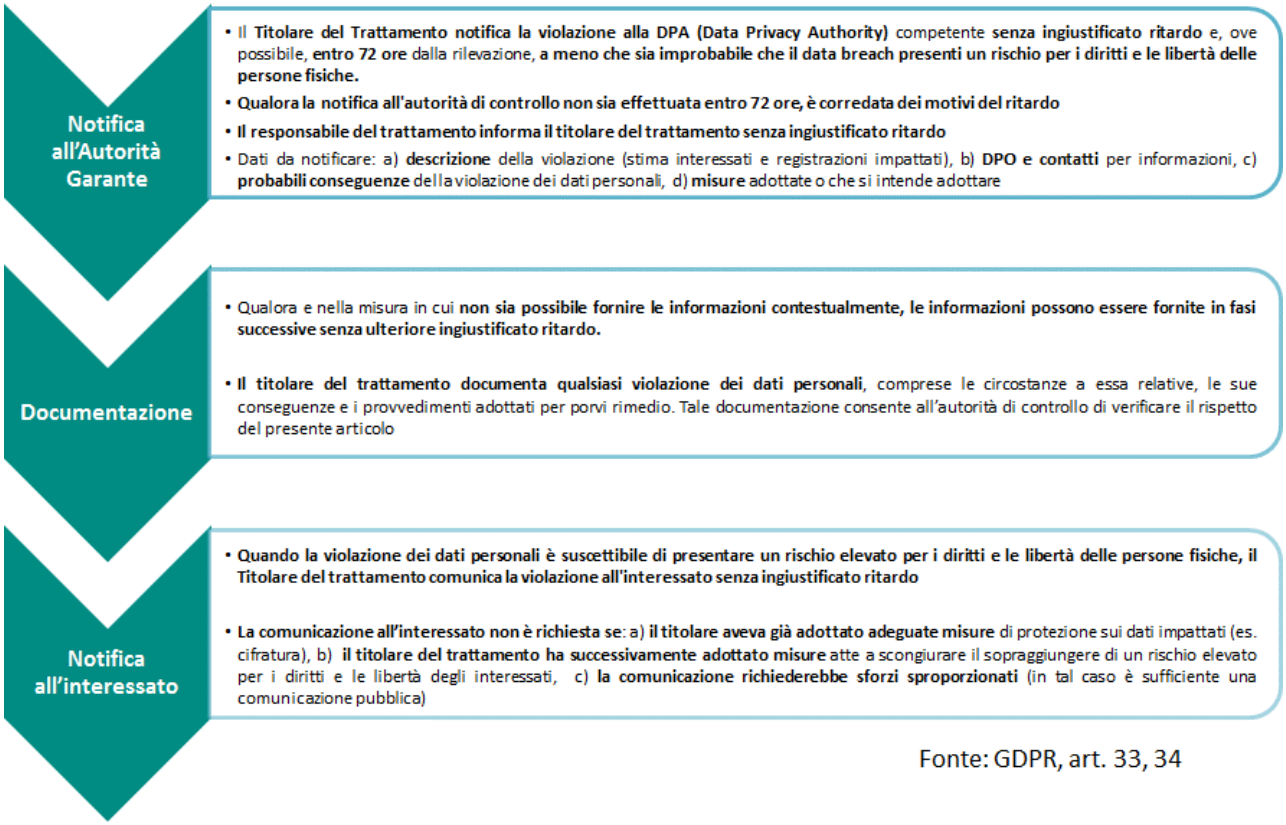
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

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".

2 RAPPRESENTAZIONE GRAFICA DEGLI OBBLIGHI NORMATIVI

Alla luce delle suddette disposizioni normative gli obblighi in caso di violazione dei dati possono riassumersi nel seguente schema:



Fonte: GDPR, art. 33, 34

3 CRITERI PER LA GESTIONE DELA DATA BREACH

Il Titolare del trattamento, ha redatto e tiene aggiornato il **registro di tutti i processi interni che comportano il trattamento di dati personali.**

In particolare attraverso il registro è possibile determinare informazioni di interesse, quali ad esempio:

- la tipologia di dati trattati dal particolare processo aziendale (dati personali, dati sensibili e giudiziari);
- le macro finalità del trattamento;
- la presenza di eventuali outsourcer che supportano il funzionamento del processo;
- le misure di sicurezza tecniche e/o organizzative adottate e quelle per le quali è prevista l'adozione.

Sulla base dei requisiti della normativa e dell'esigenza di concentrare gli sforzi sugli ambiti a maggior rischio per i diritti e le libertà degli interessati, si ritiene essenziale garantire una maggior protezione ed attenzione ai processi che gestiscono le seguenti categorie di dati definite dal GDPR quali "categoria particolari di dati" e rientranti nel tradizionale concetto di dati:

- **sensibili** (quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale);
- **giudiziari (**quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato);
- **profilazione** (dati personali che consentano qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica).

4 PROCESSO DI GESTIONE DEI DATA BREACH

Le segnalazioni di *data breach* possono provenire da molteplici fonti, quali:

- personale interno
- fornitori
- alunni e famiglie
- enti di controllo e/o autorità e/o associazioni
- altre fonti

La gestione dell'evento deve pervenire al Titolare del trattamento, contattabile ai seguenti recapiti:

- Mail: ……

- Telefono: …….

Si precisa che tale iter di segnalazione dell'evento vale sia per gli episodi conclamati che sospettati e per i quali sono in corso indagini e valutazioni.
Il Titolare del Trattamento dispone del Registro di Trattamento ove sono riportati tutti i trattamenti di dati personali svolti dall'Istituzione Scolastica e la relativa tipologia di dati trattati da ciascun processo ivi censito.
In tale fase del processo il Titolare del Trattamento ha il compito di raccogliere le informazioni necessarie per un'adeguata valutazione dell'evento.
In particolare sono necessarie le seguenti informazioni:

- una descrizione dell'evento occorso che ha originato la segnalazione;
- ove possibile i sistemi/processi/servizi impattati;
- ove possibile, almeno il numero approssimativo di registrazioni dei dati personali in questione;
- ove possibile la categoria di record impattati (es. tutti le tipologie di record, o solo la parte anagrafica, ecc.).

Se lo ritiene necessario, il Titolare del Trattamento può contattare il segnalante per reperire direttamente via telefono ulteriori informazioni a supporto dell'analisi.
Ricevuta la segnalazione si dovrà immediatamente dare comuicazione al DPO.
Entro 8 h lavorative dal ricevimento della segnalazione in ogni caso il Titolare deve completare la prima analisi dell'evento e decidere se innescare il processo di gestione del Data Breach per l'evento occorso.
Preliminarmente convoca prima telefonicamente e successivamente anche a mezzo mail (se possibile) le seguenti figure per valutare congiuntamente l'evento:

- il titolare del trattamento
- gli incaricati del trattamento eventualmente coinvolti nell'evento
- il personale o consulenti esterni competenti per la gestione dei sistemi informatici
- il DPO.

La riunione può avere luogo eventualmente anche mediante call-conference.
Il Titolare del trattamento, sentito le suddette figure decide se dichiarare la condizione di Data Breach.
Da questo momento partono le 72 h per effettuare la notifica al Garante Privacy.
In questa fase, tutto il personale e i consulenti esterni coinvolti nell'evento il cui contributo può risultare necessario per la gestione dell'evento, sono tenuti a collaborare con il Titolare soprattutto per quanto concerne l'ausilio al processo di comunicazione con l'Autorità Garante e l'eventuale comunicazione con gli interessati impattati dall'evento.
A questo punto il Titolare redige sulla base delle informazioni raccolte una relazione sull'evento accaduto che riporta i seguenti contenuti:

- una descrizione della 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;
- il nome e i dati di contatto del Titolare e di ogni altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali, sulla base delle analisi svolte nelle fasi precedenti di gestione dell'evento;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Ai fini della notifica all'Autorità, il Titolare verifica sul sito del Garante per la Protezione dei dati personali (www.garanteprivacy.it) se è prevista una modulistica specifica per la segnalazione dell'evento ed un canale specifico (mail, telefono, app ecc.) per la comunicazione dell'evento.
Il Titolare, una volta redatta la relazione sull'accaduto notifica l'evento all'Autorità Garante.
Qualora e nella misura in cui non sia possibile fornire le informazioni previste dalla relazione all'Autorità Garante contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo, riportando ciò nella stessa relazione al Garante e le relative motivazioni.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare avvia le operazioni per comunicare la violazione agli interessati coinvolti senza ingiustificato ritardo, con un linguaggio semplice e chiaro (in forma scritta laddove possibile) che riporti almeno le seguenti informazioni:

- il nome e i dati di contatto del Titolare o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Prima dell'inoltro della comunicazione agli interessati coinvolti, la stessa deve essere verificata e validata dal DPO. Naturalmente la comunicazione è obbligatoria solo nei casi previsti dall'art. 34 del GDPR.

Si tenga presente che, in accordo a quanto previsto dall'art. 34 del GDPR:

- Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
  - sono state messe 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;

- 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;
- 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 l'Istituzione Scolastica 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 per non effettuare la comunicazione è soddisfatta.

Firma del titolare del trattamento