**CIRCOLARE**

**I. C. VOLVERA**
Tel. 011.985.30.93 –011.985.07.37
**E-mail:** TOIC83800T@istruzione.it
**sito:** www.icvolvera.edu.it

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Nr. 207** | | | | Data *Si Veda Segnatura* | | | |
| **DESTINATARI** | | **DOCENTI** | **X** | **GENITORI** | **X** | **DA PUBBLICARE** | **P** |
| | | **ATA** | **X** | **PERS. ESTERNO** | **X** | **DSGA** | **X** |
| **OGGETTO** | **INDICAZIONI PROCEDURA DATA BREACH** | | | | | | |

Gentilissimi,

si indicano di seguito alcune indicazioni di procedura per la gestione di *data breach* ai sensi del GDPR.

## PREMESSA

Una violazione dei dati personali (c.d. *data breach*) 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.

## NORMATIVA E DOCUMENTI DI RIFERIMENTO

- *Regolamento UE 679/2016, considerando n. 85, 86, 87, 88 artt. 33, 34*
- *Guidelines on Personal data breach notification under Regulation 2016/679 – article 29 data protection working party (Adopted on 3 October 2017 – as last Revised and Adopted on 6 February 2018)*

## SCOPO DEL DOCUMENTO E AMBITO DI APPLICAZIONE

Il presente documento si prefigge lo scopo di indicare le opportune modalità di gestione del *data breach*, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016.
In questo documento si sintetizzano le regole per garantire il rispetto dei principi esposti e la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione del *data breach*, sotto i diversi aspetti relativi a:

- modalità e profili di segnalazione al Titolare per il tramite del referente privacy
- modalità e profili di segnalazione all'Autorità Garante
- valutazione dell'evento accaduto
- eventuale comunicazione agli interessati

## DEFINIZIONI

***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).

***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).

***Profilazione***: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo degli stessi per valutare gli aspetti 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 (art.4, punto 4)

***Archivio:*** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6).

***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). In questo contesto, sono titolari del trattamento le istituzioni scolastiche.

***Referente privacy***: la persona fisica (direttamente o indirettamente) afferente ad una scuola che operativamente si occupa delle *policy* di privacy, dei regolamenti sulla privacy e sul trattamento dati ed effettua e valuta controlli sugli stessi.

***Data Protection Officer***: la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).

***Delegato del trattamento:*** la persona fisica che, secondo l'organizzazione scolastica, ricopre un ruolo gestionale e di responsabilità all'interno della scuola che determina specifiche modalità organizzative rispetto ad uno o più trattamenti.

***Autorizzato al trattamento***: la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 4, punto 10).

***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).

***Violazione dei dati personali (c.d. 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, punto 12)

## GESTIONE DEL *DATA BREACH* INTERNO ALLA STRUTTURA

### Premesse

La circolare è finalizzata a dare notizia a tutti gli operatori in merito alla procedura per la gestione dei data breach.
Nella scuola è individuato il referente privacy che assume, ai fini della presente procedura, il ruolo di responsabile del processo.

### Modalità e profili di notifica all'Autorità Garante Privacy

Ogni operatore scolastico autorizzato a trattare dati, qualora venga a conoscenza di un potenziale caso di *data breach,* avvisa tempestivamente il delegato al trattamento.
Quest'ultimo, valutato l'evento, se confermate le valutazioni di potenziale *data breach*, lo segnala tempestivamente al referente privacy utilizzando il modulo allegato.
La segnalazione perviene al referente privacy tramite le consuete modalità di gestione dei flussi documentali già in uso.
Il referente privacy effettua una valutazione dell'evento avvalendosi, nel caso, del gruppo privacy e di eventuali altre professionalità necessarie per la corretta analisi della situazione.
Quest'ultimo può avvalersi del DPO per eventuali funzioni consulenziali.
Ai fini di una corretta classificazione dell'episodio, il referente privacy utilizzerà lo schema di scenario di *data breach*, allegato alla presente procedura.
Pertanto, sulla scorta delle determinazioni raggiunte, il referente privacy predispone l'eventuale comunicazione all'Autorità Garante, a firma del titolare, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.
È comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi)
La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del referente privacy.

## GESTIONE DEL *DATA BREACH* ESTERNO ALLA STRUTTURA

### Premesse

Ogniqualvolta la scuola/titolare del trattamento si trovi ad affidare il trattamento di dati ad un soggetto terzo/responsabile del trattamento, stipula con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal titolare in materia di protezione dati: la presente procedura di segnalazione di *data breach* è inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di *data breach*.
Ad ogni responsabile del trattamento deve essere comunicato il contatto del referente privacy al quale effettuare la predetta segnalazione (TOIC83800T@pec.istruzione.it).

## Modalità e profili di notifica all'Autorità Garante Privacy

Ogni responsabile del trattamento, qualora venga a conoscenza di un potenziale *data breach* che riguardi dati di cui l'Istituto Comprensivo sia titolare, ne dà avviso senza ingiustificato ritardo al referente privacy tramite il modulo allegato.
Per "ingiustificato ritardo" si considera la notizia pervenuta al titolare al più tardi entro 12 ore dalla presa di conoscenza iniziale da parte del responsabile.
Il referente privacy effettua una valutazione dell'evento avvalendosi, nel caso, del gruppo privacy e di eventuali altre professionalità necessarie per la corretta analisi della situazione.
Quest'ultimo può avvalersi del DPO per eventuali funzioni consulenziali.
Ai fini di una corretta classificazione dell'episodio il referente privacy utilizzerà lo schema di scenario di *data breach*.
Pertanto, sulla scorta delle determinazioni raggiunte, il referente privacy agisce come già descritto nella gestione dei data breach interno alla struttura, predispone l'eventuale comunicazione all'Autorità Garante, a firma del titolare, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.
È comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi)
La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del referente privacy.

## MODALITÀ DI COMUNICAZIONE AGLI INTERESSATI

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 referente privacy predispone l'eventuale comunicazione all'interessato/agli interessati, a firma del titolare, da inviarsi nei tempi e nei modi che lo stesso, anche attraverso la funzione consulenziale del DPO, individuerà come più opportuna come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

Cordiali saluti.

Il Dirigente Scolastico
Lorenza LA TONA
*Firmato digitalmente*