Istituto Comprensivo BRA2

Via Europa, 15 BRA
0172-413375
cnic863002@istruzione.it

GDPR Scuola
Karon srl
via G. Matteotti, 1
0163 85 26 23

Team GDPR Scuola

POLITICA SULLA PROTEZIONE DEI DATI PERSONALI

Autore:	Team GDPR Scuola
Data di creazione:	01.09.2018
Totale pagine:	9
Revisione:	

Sommario

1. Campo d'applicazione, scopo e destinatari

L'istituto scolastico si impegna a rispettare la normativa italiana ed europea in materia di privacy e di protezione dei dati personali.

Questa politica stabilisce i principi in base ai quali l'istituto tratta le informazioni di alunni, genitori o tutori, docenti, personale ATA, fornitori, associazioni ed enti.

Determina inoltre le responsabilità del titolare, dei responsabili e degli incaricati del trattamento dei dati.

I destinatari di questo documento sono tutti i dipendenti, permanenti o temporanei, e tutti i collaboratori che lavorano per conto dell'istituto scolastico.

2. Normativa e documentazione di riferimento

- Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 aprile 2016 (protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché sulla libera circolazione di tali dati), che abroga la direttiva 95/46/CE
- D.Lgs n.196 del 2003 (Codice Privacy)
- Provvedimenti dell'Autorità Garante
- Descrizione dei ruoli del responsabile della protezione dei dati
- Linee guida per l'elenco dei dati e la mappatura delle attività di trattamento
- Metodologia di valutazione d'impatto sulla protezione dei dati
- Procedura di comunicazione di una violazione dei dati

3. Definizioni

Le seguenti definizioni di termini presenti in questo paragrafo sono tratte dal Regolamento Europeo 2016/679:

"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 un 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.

"Dati personali sensibili"
Dati personali che meritano una specifica protezione e per loro natura sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro

trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Essi dovrebbero comprendere anche i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

“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.

“Profilazione”
Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati 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.

“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.

“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.

“Destinatario”
La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.
Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine, conformemente al diritto dell'Unione o degli Stati membri, non sono considerate destinatari.
Il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

“Terzo”
La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

“Consenso dell'interessato”
Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso (mediante dichiarazione o azione positiva inequivocabile) che i dati personali che lo riguardano siano oggetto di trattamento.

“Dati biometrici”
I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

“Dati relativi alla salute”
I dati personali attinenti alla salute fisica o mentale di una persona fisica (compresa la prestazione di servizi di assistenza sanitaria) che rivelano informazioni relative al suo stato di salute.

“Anonimizzazione”
Identificazione irreversibile dei dati personali, in modo tale che la persona non possa essere individuata utilizzando tempi, costi e tecnologie ragionevoli da parte del controllore o di qualsiasi altra persona.
I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile.

“Pseudonimizzazione”
Trattamento dei dati personali in modo tale che essi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
La pseudonimizzazione riduce, ma non elimina completamente, la possibilità di collegare il dato personale all’interessato.
I dati pseudonimizzati sono comunque dati personali, perciò il loro trattamento deve essere conforme ai principi contenuti nel Regolamento UE.

“Autorità di controllo”
L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento dell’UE 2016/679.
Ogni autorità di controllo monitorerà qualsiasi trattamento di dati personali qualora: a) il titolare del trattamento o il responsabile del trattamento sia stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell’autorità di controllo siano probabilmente influenzati in modo sostanziale del trattamento.

I suoi compiti e poteri elencati nel capo VI del Regolamento UE 2016/679 comprendono lo svolgimento di indagini e l'applicazione di misure amministrative e sanzioni, la promozione della consapevolezza da parte del pubblico dei rischi, delle norme, della sicurezza e dei diritti in relazione al trattamento dei dati personali, nonché l'accesso a qualsiasi sede del titolare e del responsabile del trattamento dei dati, compresi eventuali strumenti e mezzi per il trattamento.

4. Principi applicabili al trattamento dei dati personali

I principi applicabili alla protezione dei dati delineano le responsabilità del titolare del trattamento nella gestione dei dati personali.

L'articolo 5, del Regolamento UE 2016/679, enuncia i seguenti principi applicabili al trattamento dei dati:

4.1. Liceità, correttezza e trasparenza

I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Liceità: il trattamento dei dati deve essere rispettoso delle disposizioni del Regolamento e delle carte sovranazionali e nazionali dei diritti dell'uomo e del cittadino e delle altre norme di legge. Correttezza: il titolare non deve violare norme di legge o commettere abusi nel trattamento dei dati. Trasparenza: gli obblighi informativi forniti dal titolare all'interessato devono essere chiari.

4.2. Limitazione delle finalità

I dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo compatibile con tali finalità.

4.3. Minimizzazione dei dati

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario, in relazione alle finalità per cui sono trattati. L'Istituto scolastico deve applicare l'anonimizzazione o la pseudonimizzazione ai dati personali, se possibile, per ridurre il rischio per gli interessati.

4.4. Esattezza

I dati personali devono essere esatti e, se necessario, aggiornati. Devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento).

4.5. Limitazione del periodo di conservazione

I dati personali devono essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

4.6. Integrità e riservatezza

Tenendo conto delle tecnologie e di altre misure di sicurezza disponibili, dei costi di attuazione e la probabilità e gravità dei rischi per i dati personali, l'Istituto scolastico deve mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato per i dati personali, inclusa la protezione dalla distruzione accidentale o illecita, la perdita, la modifica, la rivelazione o l'accesso non autorizzati.

4.7. Responsabilizzazione (o accountability)

Il titolare del trattamento dei dati è competente per il rispetto dei principi sopra descritti e deve essere in grado di comprovarlo (il legislatore europeo all'articolo 5, comma 2, afferma: "*il titolare del trattamento è competente per il rispetto del paragrafo 1* (principi applicabili al trattamento di dati personali) *e in grado di comprovarlo*").

5. Linee guida sul corretto trattamento

Il dirigente scolastico, legale rappresentate dell'istituto scolastico, è titolare del trattamento.
Egli deve pertanto decidere in autonomia le modalità, le garanzie e i limiti del trattamento dei dati personali alla luce dei principi sopra indicati.

5.1. Comunicazioni agli interessati: l'informativa

Al momento della raccolta o prima della raccolta di dati personali, per qualsiasi tipo di attività di trattamento, il dirigente scolastico, in qualità di titolare del trattamento, è responsabile di informare adeguatamente gli interessati di quanto segue: il tipo di dati raccolti, le finalità del trattamento, i metodi di trattamento, i diritti degli interessati riguardo ai propri dati, il periodo di conservazione, i potenziali trasferimenti internazionali di dati, se i dati saranno condivisi con terzi e le misure di sicurezza dell'Istituto scolastico atte a proteggerli. Queste informazioni devono essere fornite tramite un'informativa sulla privacy.

In caso l'istituto scolastico svolga diverse attività di trattamento, dovrà predisporre informative diverse a seconda della singola attività e delle categorie di dati personali raccolti.

Laddove i dati personali siano condivisi con terzi, il dirigente scolastico deve garantire che gli interessati siano informati di ciò tramite un'informativa sulla privacy.

Non sussiste alcun obbligo di fornire l'informativa se il trattamento riguarda dati anonimi (es. aggregati) o dati di enti o persone giuridiche (i cui dati non sono soggetti alla tutela prevista dal regolamento europeo).

L'informativa quindi non è nient'altro che una comunicazione contenente tutte le informazioni relative alle finalità e alle modalità del trattamento che deve essere fornita all'interessato (ovvero alla persona cui si riferiscono i dati personali come ad esempio lo studente o il docente) al più tardi nel momento della raccolta dei dati.

5.2. La base giuridica del trattamento e il consenso

Le basi giuridiche che rendono lecito il trattamento dei dati sono indicate dall'articolo 6 paragrafo 1 del GDPR e sono:

1. Consenso
2. Adempimento obblighi contrattuali
3. Obblighi di legge a cui è sottoposto il titolare del trattamento
4. Interessi vitali della persona o interessi vitali di terzi
5. Legittimo interesse prevalente del titolare o di terzi cui i dati vengono comunicati
6. Interesse pubblico o esercizio di pubblici poteri

Genericamente la base giuridica dei trattamenti effettuati dall'istituzione scolastica consiste nell'l'esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale.

Per i trattamenti però che non hanno fini istituzionali anche la scuola dovrà acquisire il consenso dell'interessato.

Il dirigente scolastico (o chi per lui) deve fornire agli interessati le opzioni per il consenso e garantire che il consenso stesso possa essere revocato in qualsiasi momento.

Laddove la raccolta di dati personali si riferisca a un minore, il dirigente scolastico deve garantire che il consenso del titolare della responsabilità genitoriale sia fornito prima della raccolta, utilizzando il modulo di consenso del titolare della responsabilità genitoriale.

Il Dirigente Scolastico deve garantire che le richieste di correzione, modifica o distruzione dei dati personali siano gestite entro un ragionevole lasso di tempo. Deve inoltre tenere un registro di tali richieste.

I dati personali devono essere trattati solo per le finalità per cui sono stati originariamente raccolti. Nel caso in cui l'Istituto scolastico desideri trattare i dati personali raccolti per un altro scopo, deve

richiedere il consenso degli interessati in forma scritta chiara e concisa. Qualsiasi richiesta di questo tipo dovrebbe includere lo scopo originale per cui sono stati raccolti i dati e anche gli scopi nuovi o aggiuntivi. La richiesta deve includere anche il motivo del cambiamento di scopo/i.

Il responsabile della protezione dei dati è responsabile del rispetto delle regole in questo paragrafo.

Il dirigente scolastico, in qualità di titolare del trattamento, deve garantire che i metodi di raccolta siano conformi alla legge.

Il dirigente scolastico è responsabile della creazione e della manutenzione di un registro delle informative sulla privacy.

6. Organizzazione e responsabilità

La responsabilità di garantire un adeguato trattamento dei dati personali spetta a chiunque abbia accesso ai dati personali trattati dall'istituto.

Le principali aree di responsabilità per il trattamento dei dati personali sono a carico del titolare del trattamento.

Il **dirigente scolastico** è il responsabile per la gestione unitaria e il funzionamento generale dell'istituzione scolastica, in tutte le sue esplicazioni funzionali, finali o strumentali, di tipo organizzativo, didattico, amministrativo e contabile.

Il dirigente, in qualità di **titolare del trattamento dei dati**, deve decidere modalità, garanzie e limiti del trattamento dei dati personali, nonché mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento.

Il dirigente deve, progettando fin dall'inizio le modalità con cui tratterà i dati, in modo tale da fornire le tutte garanzie indispensabili, tutelare i diritti degli interessati e valutare preliminarmente tutti gli eventuali rischi.

Tra gli obblighi imposti al titolare dal principio di responsabilizzazione e dal legislatore europeo possiamo indicare i seguenti:

- Fornire informazioni agli interessati in merito ai trattamenti
- Redazione registro delle attività di trattamento
- Formazione del personale
- Designazione del responsabile della protezione dati (obbligatorio per le scuole), di responsabili del trattamento dei dati, e di incaricati
- Progettazione del trattamento

- Adozione di misure tecniche e organizzative per garantire un livello di sicurezza adeguato in base al rischio
- Valutazione di impatto sulla protezione dei dati
- Notifica delle violazioni dei dati alle autorità di controllo

Il **responsabile del trattamento** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati per conto del titolare del trattamento. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Gli **incaricati al trattamento** dei dati sono le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile. La loro designazione è effettuata per iscritto e in detto atto deve essere individuato puntualmente l'ambito del trattamento consentito.

7. Risposta agli incidenti di violazione dei dati personali

Quando l'istituto scolastico viene a conoscenza di una presunta o effettiva violazione dei dati personali, il dirigente scolastico deve eseguire un'indagine interna e adottare misure correttive appropriate in modo tempestivo, in base alla politica sulla violazione dei dati. Laddove sussistano rischi per i diritti e le libertà degli interessati, l'istituto scolastico deve informare l'autorità di controllo competente in materia di protezione dei dati senza indebiti ritardi, ove possibile entro 72 ore.