POLITICA DÌ PROTEZIONE DEI DATI PERSONALI

L'"ISTITUTO SCOLASTICO" raccoglie e utilizza determinati dati sulle persone.
Questi possono includere clienti, fornitori, contatti commerciali, dipendenti e alunni e loro famigliari e altre persone con cui l'"ISTITUTO SCOLASTICO" ha una relazione o potrebbe aver bisogno di contattare. Questa politica descrive come questi dati personali devono essere raccolti, gestiti e archiviati per soddisfare gli standard di protezione dei dati delineati dal Regolamento EU 679/2016 (GDPR) e seguenti interventi legislativi.

SCOPO

Questa politica di protezione dei dati garantisce che l'"ISTITUTO SCOLASTICO":

- Sia conforme alla legge sulla protezione dei dati personale e segue le buone pratiche
- Protegga i diritti di alunni, personale, clienti e partner
- Sia trasparente su come raccoglie e tratta i dati degli individui
- Si protegga dai rischi di una violazione dei dati personali

CAMPO DI APPLICAZIONE

Questa politica si applica ai dipendenti, collaboratori, consulenti, lavoratori temporanei, alunni e loro famigliari incluso tutto il personale affiliato a terze parti.

II Regolamento Ue 679/2016 (GDPR) descrive come le organizzazioni, incluso l'"ISTITUTO SCOLASTICO", devono raccogliere, gestire e archiviare i dati personali. Queste regole si applicano indipendentemente dal fatto che i dati siano archiviati elettronicamente, su carta o su altri materiali.

Per rispettare la legge, le informazioni personali devono essere raccolte e utilizzate correttamente, conservate in modo sicuro e non divulgate Illegalmente.

Il GDPR (Regolamento Ue 679/2016) è sostenuto da otto importanti principi, linee guide su come trattare i dati personali. In particolare i dati personali devono:

1) Essere trattati in modo equo e legale
2) Essere ottenuti solo per finalità specifiche, lecite
3) Essere adeguati, pertinenti e non eccessivi
4) Essere precisi e aggiornati
5) Non essere trattenuti più a lungo del necessario
6) Essere elaborati conformemente ai diritti degli interessati
7) Essere protetti nei modi appropriati
8) Non essere trasferiti al di fuori dello Spazio economico europeo (SEE), a meno che tale paese o territorio garantisca anche un livello adeguato di protezione, ci sia una base contrattuale o sia state delineate delle BRC (Binding Corporate Rules)

Applicazione, rischi e responsabilità

Questa politica si applica all'organizzazione nel suo intero:

- ➢ Sede centrale
- ➢ Tutti i Plessi
- ➢ Tutto il personale e i volontari
- ➢Tutti gli appaltatori, i fornitori e le altre persone che lavorano per conto dell'organizzazione

Si applica a tutti i dati che l'organizzazione detiene in relazione a persone identificabili. Ciò può includere:

✓Nomi di individui
✓Indirizzi postali
✓Indirizzi E-mail
✓Numeri di telefono
✓Qualsiasi altra informazione relativa alle persone

Rischi

Questa politica aiuta a proteggere l'"ISTITUTO SCOLASTICO" da alcuni rischi di sicurezza dei dati personali molto reali, tra cui:

- Violazioni di riservatezza (informazioni personali sono state ottenute, modificate, cancellate o distribuite in modo inappropriato).
- Non riuscire a offrire una scelta (tutte le persone dovrebbero essere libere di scegliere in che modo l'"ISTITUTO SCOLASTICO" utilizza i dati che le riguardano).
- Danno reputazionale (l'"ISTITUTO SCOLASTICO" potrebbe soffrire un danno d'immagine in caso di materializzazione di un data breach (violazione dei dati personali).

Responsabilità

Chiunque lavori per o con l'"ISTITUTO SCOLASTICO" ha una certa responsabilità nel garantire che i dati personali vengano raccolti, archiviati e gestiti in modo appropriato.
Ogni persona che gestisce i dati personali deve garantire che siano gestiti e elaborati in linea con questa politica e i principi di protezione dei dati. In particolare, le seguenti persone hanno ruoli chiave di responsabilità:
Il Dirigente scolastico/Titolare di trattamento è in ultima analisi responsabile di garantire che l'"ISTITUTO SCOLASTICO" soddisfi i propri obblighi legali.

Il Responsabile della protezione dei dati (DPO), è il soggetto designato dal titolare o dal responsabile del trattamento per assolvere le funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR (art. 37 GDPR)

• **Il Responsabile IT** è responsabile di:

- Garantire che tutti i sistemi, i servizi e le apparecchiature utilizzate per la memorizzazione dei dati soddisfino standard di sicurezza accettabili.
- Eseguire controlli e scansioni regolari per garantire che l'hardware e il software di sicurezza funzionino correttamente.
- Valutare eventuali servizi di terzi che l'Istituto sta considerando di utilizzare per archiviare o elaborare dati. (Ad esempio, servizi di cloud computing.)

Gli incaricati ("autorizzati" o "designati") del trattamento dei dati /Direttore dei Servizi Generali DSGA, Amministrativi, Docenti e collaboratori dell'istituto scolastico sono responsabili di:

=> Laddove necessario, collaborare con il titolare del trattamento, con il DPO o altro personale, per garantire che le attività o iniziative di vario tipo eventualmente presenti rispettino i principi di protezione dei dati.

Linee guida generali per il personale

=> Le uniche persone in grado di accedere ai dati coperti da questa politica dovrebbero essere coloro che ne hanno bisogno per il loro lavoro.

=> I dati **non devono essere condivisi in modo informale**, quando è richiesto l'accesso ad informazioni confidenziali, i dipendenti si rivolgono al Titolare del Trattamento o chi ne fa le veci.

=> L'"ISTITUTO SCOLASTICO" **fornirà informazione a tutti i dipendenti** per aiutarli a comprendere le loro responsabilità nella gestione dei dati.

=> I dipendenti devono mantenere tutti i dati personali al sicuro, adottando precauzioni e seguendo le linee guida presentate in questa politica.

In particolare, è necessario:

a. **Utilizzare password complesse**, che non devono mai essere condivise.

b. **I dati personali non devono essere divulgati** a persone non autorizzate, all'interno dell'"ISTITUTO SCOLASTICO" o esternamente.

c. I dati personali devono **essere rivisti e regolarmente aggiornati**. Se non sono più necessari, devono essere eliminati.

d. I dipendenti, prima di agire, **devono chiedere aiuto** al Titolare del Trattamento o a chi ne fa le veci se non sono sicuri riguardo a qualsiasi aspetto della protezione dei dati.

Conservazione dei dati

Queste regole descrivono come e dove i dati devono essere archiviati in modo sicuro. Le domande sulla memorizzazione sicura dei dati possono essere indirizzate al Titolare.

Quando i dati personali siano **archiviati su carta** devono essere conservati in un luogo sicuro dove le persone non autorizzate non possono accedervi.

Queste linee guida si applicano anche ai dati personali che vengono solitamente archiviati elettronicamente ma per qualche motivo sono stati stampati:

Se non richiesto diversamente, la carta o i file devono essere conservati in un cassetto o in uno schedario/armadio chiuso a chiave.

I dipendenti devono assicurarsi che la carta e le stampe non vengano lasciate dove persone non autorizzate potrebbero vederle, come in una stampante.

Le stampe dei dati devono essere triturate e smaltite in modo sicuro quando non sono più necessarie.

Quando i dati personali siano archiviati **elettronicamente, devono essere protetti da accessi non autorizzati**, cancellazioni accidentali e modifiche involontarie:

I dati devono essere **protetti da password complesse** che vengono cambiate regolarmente e mai condivise tra dipendenti.

Se i dati sono archiviati **su un supporto rimovibile** (come CD, DVD, chiavetta USB, HD rimovibile, ecc..), questi dovrebbero essere tenuti chiusi a chiave in un luogo sicuro quando non vengono utilizzati.

I dati devono essere **memorizzati solo su unità e server designati** e devono essere caricati solo **su servizi di cloud computing approvati.**

I server contenenti dati personali devono essere collocati in un luogo sicuro.

I dati personali **devono essere salvati frequentemente**. Questi backup dovrebbero essere testati regolarmente, in linea con le procedure di backup standard dell'"ISTITUTO SCOLASTICO".

I dati personali non dovrebbero **mai essere salvati direttamente (in locale) su laptop o altri dispositivi mobili come tablet o smartphone.**

Tutti i server e i computer contenenti dati personali devono essere protetti **da un software di sicurezza antivirus approvato e da un firewall.**

Utilizzo dei dati

Quando si lavora con dati personali, i dipendenti devono assicurarsi **che gli schermi dei loro computer siano sempre bloccati quando lasciati incustoditi.**

I dati personali non devono essere condivisi in mancanza di finalità istituzionali e senza l'utilizzo di canali ufficiali dell'Istituto scolastico.

I dati personali **non dovrebbero mai essere trasferiti al di fuori dello spazio economico europeo**, senza la presenza di finalità istituzionali e seguire la corretta procedura.

I dipendenti non devono salvare copie di dati personali sui propri computer, bisogna sempre accedere e aggiornare la copia centrale di tutti i dati.

Accuratezza dei dati

La legge richiede che l'"ISTITUTO SCOLASTICO" adotti misure adeguate per garantire che i dati siano mantenuti accurati e aggiornati.

Più importante è il fatto che i dati personali siano accurati, maggiore è lo sforzo che l'"ISTITUTO SCOLASTICO" dovrebbe compiere per garantirne l'accuratezza.

E' responsabilità di tutti i dipendenti che lavorano con dati personali adottare misure ragionevoli per garantire che siano mantenuti il più precisi e aggiornati possibile.

II personale non deve richiedere e/o raccogliere dati aggiuntivi non necessari.

II personale dovrebbe **cogliere ogni opportunità per garantire che i dati vengano aggiornati**.

L'"ISTITUTO SCOLASTICO" renderà semplice per gli interessati **l'aggiornamento delle informazioni** che detiene su di loro.

I dati devono **essere aggiornati quando vengono scoperte inesattezze.**

Richiesta d'esercizio dei diritti dell'interessato

Tutti gli individui che sono oggetto di dati personali detenuti dall'"ISTITUTO SCOLASTICO" hanno diritto a:

A. Chiedere quali informazioni l'"ISTITUTO SCOLASTICO" detiene su di loro e perché
B. Chiedere la rettifica dei propri dati
C. Chiedere la portabilità delle informazioni personali
D. Chiedere la cancellazione
E. Chiedere la limitazione od opporsi al trattamento

Le richieste d'esercizio di tali diritti da parte di soggetti devono essere inviate per e - mail, indirizzate **al Titolare del trattamento** all'indirizzo _____

Divulgazione dei dati per altri motivi

In determinate circostanze, il GDPR consente di divulgare i dati personali alle forze dell'ordine senza il consenso dell'interessato. In queste circostanze, l'"ISTITUTO SCOLASTICO" rivelerà i dati richiesti.

Tuttavia, il Titolare del trattamento assicurerà che la richiesta sia legittima, richiedendo assistenza al Responsabile della protezione dei dati (DPO) e ai consulenti legali, laddove necessario.

Dare informazioni

L'"ISTITUTO SCOLASTICO" mira a garantire che le persone siano consapevoli del fatto che i loro dati sono trattati e che capiscano:

A. **Come vengono utilizzati i dati**
B. **Come esercitare i loro diritti**

A tal fine l'"ISTITUTO SCOLASTICO" ha redatto informativa sulla privacy che stabilisce come i dati relativi alle persone sono utilizzati dalla scuola

OBBLIGO DI NOTIFICA DELLE VIOLAZIONI DEI DATI (CD. "DATA BREACH")

Con la presente circolare si evidenzia che l'art. 33 del ***Regolamento UE 2016/679*** **relativo alla** ***protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati)***, che è entrato definitivamente in vigore il 25 maggio 2018, ribadisce ed enfatizza un concetto, per la protezione dei dati personali - *Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche*, riguardante l'obbligo da parte di tutte le Pubbliche Amministrazioni di comunicare al Garante per la protezione dei dati personali qualsiasi evento di "*violazione di dati personali*".
Lo stesso Regolamento UE 2016/679, all'art. 4 punto 12), fornisce la seguente definizione di violazione dei dati personali: "*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*".
Contrariamente a quanto si potrebbe pensare, pertanto, la definizione di "*violazione di dati personali*" contempla non solo le fattispecie in cui vi sia stato un accesso abusivo ai dati personali, casistica invero fortunatamente abbastanza rara, ma anche il caso della distruzione o della perdita dei dati personali, che

invece sono eventi che si possono verificare con una certa frequenza, ad esempio a causa del guasto di un supporto di memorizzazione, di un virus informatico, di un non corretto svolgimento delle procedure di *backup*, etc. Oppure può riguardare la casistica di dati personali o sensibili comunicati o portati a conoscenza di soggetti, interni o esterni all'Istituto, non autorizzati o non titolati.
È importante inoltre ricordare che la violazione dei dati personali non riguarda solamente i dati in formato elettronico, ma può riguardare anche i dati in formato cartaceo; questa seconda casistica, anzi, è la più critica da gestire, in quanto se vi fosse la perdita o il furto di fascicoli cartacei contenenti dati personali, tale evenienza potrebbe essere molto difficile da rilevare.

Nel dettaglio, l'art. 33 del Regolamento UE 2016/679 prevede:

"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 (se presente) 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."

Inoltre, l'art. 34 del Regolamento UE 2016/679 prevede:

"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."

Si chiede, pertanto, di porre la massima attenzione nel monitorare e rilevare tempestivamente tutti gli eventi di tipo "*violazione dei dati personali*", compresi gli eventi per i quali non vi sia la certezza ma anche solo un sospetto, e comunicarli immediatamente al Dirigente Scolastico, il quale provvederà ad informare tempestivamente il Responsabile della protezione dei dati dell'Istituto designato ai sensi dell'art. 37 del GDPR, che provvederà ad effettuare tutte le valutazioni del caso di concerto con il Dirigente Scolastico ed a predisporre, se ve ne siano i presupposti, la notificazione da effettuare entro 72 ore all'Autorità di Controllo nazionale (Garante per la protezione dei dati personali).

La Dirigente Scolastica