POLITICA PROTEZIONE DEI DATI PERSONALI

L'organizzazione raccoglie e utilizza determinati dati sulle persone.

Questi possono includere clienti, fornitori, contatti commerciali, dipendenti e altre persone con cui l'organizzazione 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 del BS 10012:2017.

SCOPO

Questa politica di protezione dei dati garantisce che l'organizzazione:

- Sia conforme alla legge sulla protezione dei dati personale e segue le buone pratiche
- Protegga i diritti di 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, incluso tutto il personale affiliato a terze parti e a tutte le attrezzature di proprietà o in leasing dell'organizzazione.

MODALITÀ OPERATIVE

Il Regolamento Ue 679/2016 (GDPR)

Il Regolamento Ue 679/2016 (GDPR) descrive come le organizzazioni, incluso l'IC di Brembate di Sopra, 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 guida su come trattare il dato 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

Responsabilità

Chiunque lavori per o con l'IC di Brembate di Sopra 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:

- La **Direzione/ Titolare di trattamento** è in ultima analisi responsabile di garantire che l'organizzazione soddisfi i propri obblighi legali.

- Il **Responsabile della protezione dei dati** (DPO), se presente, è responsabile di:

  - Mantenere il titolare di trattamento aggiornato sulle responsabilità, i rischi e le questioni relativi alla protezione dei dati.
  - Revisionare tutte le procedure di protezione dei dati e le relative politiche, in linea con un programma concordato.
  - Organizzare la formazione e la consulenza sulla protezione dei dati per le persone coperte da questa politica.
  - Gestire le domande sulla protezione dei dati da parte del personale e di chiunque altro coperto da questa politica.
  - Gestire le richieste da parte di individui per vedere i dati che l'organizzazione tiene su di loro (Vedi '**Modulo richiesta d'esercizio dei diritti dell'interessato**').
  - Verificare e approvare eventuali contratti o accordi con terze parti che possano gestire i dati personali trattati dall'organizzazione

- 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 la società sta considerando di utilizzare per archiviare o elaborare dati. (Ad esempio, servizi di cloud computing.)

- Il **Responsabile Commerciale/Amministrazione** è responsabile di:

  - Approvare qualsiasi dichiarazione sulla protezione dei dati allegata a comunicazioni quali e-mail e lettere.
  - Laddove necessario, collaborare con altro personale per garantire che le iniziative di marketing eventualmente presenti rispettino i principi di protezione dei dati.

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 un CD o un DVD), 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**, lontano dallo spazio ufficio generale.
- ✓ I dati personali devono **essere salvati frequentemente**. Questi backup dovrebbero essere testati regolarmente, in linea con le procedure di backup standard dell'organizzazione.
- ✓ 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 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 modo informale**. In particolare, non dovrebbero mai essere inviati via e-mail, in quanto questa forma di comunicazione non è sicura.
- È preferibile che i dati personali siano **crittografati prima di essere trasferiti elettronicamente**. Il Responsabile IT può spiegare come inviare dati a contatti esterni autorizzati.
- I dati personali **non dovrebbero mai essere trasferiti al di fuori dello Spazio economico europeo**, senza seguire la corretta procedura.
- I dipendenti **non devono salvare copie di dati personali sui propri computer**. Sempre accedere e aggiornare la copia centrale di tutti i dati.

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'organizzazione 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 della società, laddove necessario.

Dare informazioni

IC di Brembate di Sopra mira a garantire che le persone siano consapevoli del fatto che i loro dati sono trattati e che capiscano:

- ⇒ **Come vengono utilizzati i dati**
- ⇒ **Come esercitare i loro diritti**

A tal fine l'organizzazione ha una informativa sulla privacy che stabilisce come i dati relativi alle persone sono utilizzati dalla società.

BREMBATE DI SOPRA (BG), 21.08.18

LA DIREZIONE/ IL TITOLARE DI TRATTAMENTO

IL DIRIGENTE SCOLASTICO
DOTT.ssa CRISTINA LOCATELLI
Cristina Locatelli