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'I.P.I.A. Cesare Pesenti, 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

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 email
- ✓ Numeri di telefono
- ✓ ... più qualsiasi altra informazione relativa alle persone

Rischi

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

- ✓ **Violazioni di riservatezza** (le 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'organizzazione utilizza i dati che le riguardano).
- ✓ **Danno reputazionale** (l'organizzazione 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'I.P.I.A. Cesare Pesenti 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.

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'organizzazione **fornirà formazione 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:

- **Utilizzare password complesse, che non devono mai essere condivise.**
- I dati personali **non devono essere divulgati** a persone non autorizzate, all'interno dell'organizzazione o esternamente.
- I dati personali devono **essere rivisti e regolarmente aggiornati.** Se non sono più necessari, devono essere eliminati.
- 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 **Responsabile IT** o 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, la carta o i file devono essere conservati in **un cassetto o in uno schedario 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 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.

Accuratezza dei dati

La legge richiede che l'organizzazione adotti misure ragionevoli 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'organizzazione dovrebbe compiere per garantirne l'accuratezza.

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

- ✓ I dati verranno **conservati solo in posti assolutamente necessari**. Il personale non deve creare set di dati aggiuntivi non necessari.
- ✓ Il personale dovrebbe **cogliere ogni opportunità per garantire che i dati vengano aggiornati.** (*Ad esempio, confermando i dettagli di un cliente quando chiamano*).
- ✓ L'organizzazione renderà **semplice per gli interessati l'aggiornamento delle informazioni** che detiene su di loro. (*Ad esempio, tramite il sito web dell'organizzazione*).
- ✓ I dati devono essere **aggiornati quando vengono scoperte inesattezze.** (*Ad esempio, se un cliente non può più essere raggiunto sul numero di telefono memorizzato, dovrebbe essere rimosso dal database*).

Richiesta d'Esercizio dei diritti dell'interessato

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

- Chiedere **quali informazioni** l'organizzazione **detiene** su di loro e perché
- Chiedere la rettifica dei propri dati
- Chiedere la portabilità delle informazioni personali
- Chiederne la cancellazione
- 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 *info@istitutopesenti.it*. L'organizzazione fornisce un modulo di richiesta standard (Vedi **Modulo Richiesta d'esercizio dei diritti dell'interessato**), anche se gli individui non devono utilizzarlo.

Per approfondire vedi la procedura di riferimento **P 8.2.1 Richiesta d'esercizio dei diritti dell'interessato**

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

I.P.I.A. Cesare Pesenti 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.

BERGAMO, 15/03/2019

LA DIREZIONE/ IL TITOLARE DI TRATTAMENTO

Firmato digitalmente da

Marco Pacati

C = IT
Data e ora della firma:
05/04/2019 11:38:17