POLITICA PROTEZIONE DEI DATI

L'organizzazione deve raccogliere e utilizzare determinate informazioni 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).

SCOPO

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

- Sia conforme alla legge sulla protezione dei dati e seguire le buone pratiche
- Protegga i diritti di personale, clienti e partner
- Sia trasparente su come memorizza ed elabora i dati degli individui
- Si protegga dai rischi di una violazione dei dati

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, inclusa I.S.S. LUIGI EINAUDI, devono raccogliere, gestire e archiviare le informazioni 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 è sostenuto da otto importanti principi. Questi dicono che i dati personali devono:

1) Essere trattati in modo equo e legale
2) Essere ottenuto solo per scopi specifici, leciti
3) Essere adeguati, pertinenti e non eccessivi
4) Essere precisi e aggiornati
5) Non essere trattenuto più a lungo del necessario
6) Elaborato 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:

- La sede centrale
- Tutti i rami/holding
- Tutto lo staff 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 vengono distribuite in modo inappropriato.)
- ✓ **Non riuscire a offrire una scelta**. (tutte le persone dovrebbero essere libere di scegliere in che modo l'azienda utilizza i dati che le riguardano.)
- ✓ **Danno reputazionale**. (l'azienda potrebbe soffrire se gli hacker hanno ottenuto con successo l'accesso a dati personali trattati.)

Responsabilità

Chiunque lavori per o con I.S.S. LUIGI EINAUDI ha una certa responsabilità nel garantire che i dati vengano raccolti, archiviati e gestiti in modo appropriato.
Ogni squadra che gestisce i dati personali deve garantire che sia gestita e elaborata in linea con questa politica e i principi di protezione dei dati.

Tuttavia, queste persone hanno aree 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) è responsabile di:

  - Mantenere il titolare di trattamento aggiornato sulle responsabilità, i rischi e le questioni relativi alla protezione dei dati.
  - Revisione di tutte le procedure di protezione dei dati e delle relative politiche, in linea con un programma concordato.
  - Organizzare formazione e 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 di accesso**').
- Verifica e approvazione di eventuali contratti o accordi con terze parti che possano gestire i dati personali trattati dall'azienda

- Il **Responsabile IT** (**RSI**) è responsabile di:

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

- Il **Responsabile Commerciale/Amministrazione (DSGA)** è responsabile di:

  - Approvazione di qualsiasi dichiarazione sulla protezione dei dati allegata a comunicazioni quali e-mail e lettere.
  - Affrontare qualsiasi domanda di protezione dei dati da parte di giornalisti o agenzie di stampa come i giornali.
  - Laddove necessario, collaborare con altro personale per garantire che le iniziative di marketing 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 alle informazioni confidenziali, i dipendenti possono richiederlo ai propri manager di linea.

⇒ 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 seguenti.

⇒ 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'azienda o esternamente.

⇒ I dati personali devono **essere rivisti e regolarmente aggiornati** se si ritiene che non siano aggiornati. Se non sono più necessari, devono essere eliminato e eliminato.

⇒ I dipendenti **devono chiedere aiuto** al proprio manager di linea o al responsabile della protezione dei dati 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 sono **archiviati su carta** devono essere conservati in un luogo sicuro dove le persone non autorizzate non possono vederli.

Queste linee guida si applicano anche ai dati 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 sono **archiviati elettronicamente**, devono essere protetti da accessi non autorizzati, cancellazioni accidentali e tentativi di Hacking illecito:

- ✓ 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 bloccati in modo 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 devono **essere salvati frequentemente**. Questi backup dovrebbero essere testati regolarmente, in linea con le procedure di backup standard dell'azienda.
- ✓ I dati non dovrebbero **mai essere salvati direttamente su laptop o altri dispositivi mobili** come tablet o smartphone.
- ✓ Tutti i server e i computer contenenti dati 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 dovrebbe mai essere inviato via e-mail, in quanto questa forma di comunicazione non è sicura.
- I dati **devono essere 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'azienda.*)
- ✓ 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'Accesso

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.
- Chiedi **come accedervi**.
- Essere informato **su come tenerlo aggiornato**.
- Essere informato su come l'organizzazione **sta rispettando i propri obblighi di protezione dei dati**.

Se un individuo contatta l'organizzazione che richiede questa informazione, questa viene chiamata Richiesta di accesso.

Le richieste di accesso da parte di soggetti devono essere inviate per e-mail, indirizzate al **Titolare del trattamento** all'indirizzo [*indirizzo e-mail*]. Il responsabile del trattamento dei dati può fornire un modulo di richiesta standard (Vedi **Modulo Richiesta di accesso**), anche se gli individui non devono utilizzarlo.

Per approfondire vedi la procedura di riferimento **P 8.2.12 Richiesta d'accesso**

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 dai consulenti legali della organizzazione laddove necessario.

Dare informazioni

I.S.S. LUIGI EINAUDI mira a garantire che le persone siano consapevoli del fatto che i loro dati sono trattati e che capiscono:

- ⇒ **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 organizzazione.

[*Questa è disponibile su richiesta. Una versione di questa dichiarazione è disponibile anche sul sito Web.*]

CREMONA, 06/03/2018

LA DIREZIONE/ IL TITOLARE DI TRATTAMENTO