La Direzione della NOLOOP S.r.l. ritiene importante perseguire, da parte di tutta l'organizzazione aziendale, gli obiettivi del proprio sistema di gestione per la sicurezza delle informazioni, la continuità operativa e la protezione dei dati personali, progettato e implementato conformemente alla norma ISO/IEC 27001 ed al Regolamento UE 2016/679 GDPR.

La gestione della sicurezza delle informazioni, della continuità operativa e della protezione dei dati personali è un processo complesso, che coinvolge le risorse umane delle unità organizzative all'interno del perimetro di certificazione, descritto nel manuale del sistema di gestione per la sicurezza delle informazioni.

L'Organizzazione attua la politica per la sicurezza delle informazioni, la continuità operativa e la protezione dei dati personali, facendo propri i principi di:

- Equità
- Lealtà
- Correttezza
- Conformità
- Responsabilizzazione (Accountability)
- Tutela dei diritti e delle libertà delle persone fisiche

Per tali ragioni, NOLOOP S.r.l. è costantemente impegnata a mantenere e migliorare il proprio sistema di gestione, che persegue i seguenti obiettivi di alto livello:

- Garantire elevati standard di sicurezza relativi alla sicurezza delle informazioni trattate, alla continuità operativa e alla protezione dei dati personali intercettando eventuali rischi e opportunità inerenti al contesto di riferimento;
- Proteggere gli interessi degli stakeholder rilevanti per il sistema di gestione per la sicurezza delle informazioni, la continuità operativa e la protezione dei dati personali;
- Limitare il rischio del business, prevenendo e minimizzando l'impatto degli incidenti di sicurezza sulle informazioni (aziendali e personali);
- Tutelare la protezione dei dati personali durante l'intero ciclo di vita dei trattamenti;
- Assicurare la resilienza dell'Organizzazione nell'erogazione dei propri servizi core a fronte di eventi avversi che possano colpirne gli asset portanti attraverso il proprio processo di continuità operativa, meccanismi di backup e disaster recovery;

- Garantire la conformità alla normativa vigente, cogente e volontaria, ai vincoli contrattuali e ai requisiti definiti dalle terze parti.

Al fine di perseguire gli obiettivi sopra indicati, si rende necessario pianificare e realizzare, nell'ambito del sistema di gestione, le seguenti attività:

- Mettere a disposizione le risorse necessarie, inclusi i profili con le competenze adeguate, per stabilire, attuare, mantenere e migliorare in modo continuo il sistema di gestione per la sicurezza delle informazioni;
- Definire e segregare i ruoli e i compiti necessari per coordinare e supportare il sistema di gestione, in particolare individuando e nominando formalmente un Data Protection Officer (DPO) che garantisca la conformità dei sistemi alla normativa cogente e volontaria applicata;
- Classificare tutte le informazioni, inclusi dati personali trattati dall'Organizzazione, in base al loro livello di criticità applicando i principi di security / data protection by design & by default in modo da garantirne la riservatezza, disponibilità ed integrità; arantire la tutela dei diritti e delle libertà delle persone fisiche, con riferimento ai trattamenti di dati personali, in conformità alle prescrizioni normative vigenti e ai requisiti delle norme ISO di riferimento;
- Manutenere e testare il proprio sistema di gestione della continuità operativa al fine di migliorare la propria resilienza e permettere all'Organizzazione di affrontare efficacemente ogni evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulle attività aziendali;
- Selezionare e verificare periodicamente i fornitori in grado di presentare adeguate garanzie in merito al proprio livello di conformità, con particolare riferimento alla capacità di proteggere informazioni e dati personali trattati per conto dell'organizzazione;
- Verificare periodicamente l'efficacia ed efficienza del sistema di gestione, in modo da favorire l'attivazione di un processo di miglioramento continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali, delle esigenze degli interessi degli stakeholder e degli interessati ai sensi del GDPR;
- Mantenere aggiornata e diffondere a tutti gli stakeholder interni ed esterni la propria "Politica per la sicurezza delle informazioni, la continuità operativa e la protezione dei dati personali", in conformità allo standard ISO/IEC 27001 ed al Regolamento UE 2016/679 GDPR;

- Migliorare in modo continuo il proprio sistema di gestione adattandolo alle variazioni di contesto significative per gli obiettivi del sistema, sulla base dell'evoluzione delle minacce e in generale dei rischi che ne derivano, dell'efficacia/efficienza dei processi implementati e delle evidenze emergenti dalle verifiche periodiche interne ed esterne;
- Assicurare la conformità ai vincoli contrattuali relativi al trattamento dei dati personali, sia nei casi in cui l'organizzazione operi in qualità di Data Controller (Titolare del trattamento), sia nei casi in cui svolga il ruolo di Data Processor (Responsabile del trattamento) su incarico dei propri Clienti, seguendo le istruzioni da questi impartite;
- Diffondere i principi e i valori dichiarati nella politica aziendale dall'organizzazione e a rendere attiva ed efficace la comunicazione da e verso le diverse parti interessate affinché tale politica sia compresa e partecipata.

La Direzione è impegnata ad attuare, sostenere e verificare periodicamente la presente politica e a divulgarla a tutti i soggetti che lavorano per l'azienda o per conto di essa o che con essa collaborano a qualsiasi titolo.
Il presente documento è pubblico e disponibile per la consultazione da parte di tutte le parti interessate.

La Direzione

Firmato digitalmente da:
Donzelli Paolo
Data: 11/04/2024 12:31:58