MAGNETIC MEDIA NETWORK S.P.A. è consapevole che per fornire un livello di servizio sempre più professionale è necessario garantire ai suoi stakeholder un adeguato livello di sicurezza delle informazioni che le affidano proteggendone la riservatezza, l'integrità e la disponibilità.

La presente politica definisce le linee guida e le direttive per garantire la sicurezza delle informazioni nel contesto della gestione del perimetro dell'Information Technology. Magnetic Media Network S.p.A. si impegna pertanto a garantire una protezione adeguata delle informazioni personali identificabili (PII) dei suoi clienti. Come parte di questo impegno, Magnetic Media Network S.p.A. si impegna per raggiungere la conformità con le leggi e i regolamenti applicabili in materia di protezione delle PII. Questo documento di politica descrive le misure che vengono adottate per garantire il rispetto della legislazione sulla privacy, inclusi il Regolamento generale sulla protezione dei dati (GDPR), la legge nazionale sulla protezione dei dati e altre leggi pertinenti, a seconda del luogo in cui le informazioni vengono conservate ed elaborate.
L'organizzazione si impegna a implementare e mantenere un SGSI conforme alla norma ISO/IEC 27001:2022 con l'estensione alle linee guida UNI CEI EN ISO/IEC 27017:2021 e UNI CEI EN ISO/IEC 27018:2020 al fine di proteggere le informazioni critiche e mitigare i rischi associati alla loro gestione.

La politica della sicurezza delle informazioni di Magnetic Media Network S.p.A. si ispira ai seguenti principi:

- Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione;
- Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari;
- Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando policy volte al rispetto di adeguati livelli di sicurezza;
- Garantire che l'organizzazione e le terze parti che collaborano al trattamento delle informazioni, abbiano piena consapevolezza delle problematiche relative alla sicurezza;
- Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business;
- Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti;
- Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti;
- Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni;
- Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.
- Considerare nella progettazione e nell'implementazione del proprio sistema di gestione gli eventuali impatti derivanti dai cambiamenti climatici.

Magnetic Media Network S.p.A. si impegna a rispettare tutte le leggi e i regolamenti applicabili in materia di protezione delle PII. Le nostre politiche e procedure sono progettate per garantire che le PII siano gestite in conformità con tali leggi e regolamenti. In particolare, ci impegniamo a rispettare il GDPR nell'Unione Europea (UE). Adottiamo misure tecniche e organizzative adeguate nel garantire la protezione delle PII, inclusa l'implementazione di misure di sicurezza adeguate e la conduzione di valutazioni periodiche dell'impatto sulla protezione dei dati (Data Protection Impact Assessments) quando necessario.

La politica per la norma ISO/IEC 27001:2022, UNI CEI EN ISO/IEC 27017:2021 e UNI CEI EN ISO/IEC 27018:2020 si applica a tutti i dipendenti, fornitori, consulenti e terze parti che accedono alle informazioni dell'organizzazione. Inoltre, si estende a tutti i sistemi, processi, strutture e attività che coinvolgono la gestione delle informazioni.

La responsabilità per l'implementazione e il mantenimento del SGSI è attribuita alla direzione dell'organizzazione. Sono designati ruoli e responsabilità specifici per garantire l'efficace attuazione delle misure di sicurezza delle informazioni e il raggiungimento degli obiettivi definiti.

L'organizzazione adotta un approccio sistematico per identificare, valutare e gestire i rischi per la sicurezza delle informazioni. Vengono definiti processi per valutare periodicamente i rischi, implementare contromisure adeguate e monitorare l'efficacia delle azioni intraprese.

L'organizzazione si impegna a promuovere la consapevolezza e la comprensione delle politiche e delle procedure per la sicurezza delle informazioni tra il personale. Vengono adottate misure adeguate nella selezione, l'addestramento, l'assegnazione delle responsabilità e la gestione delle risorse umane in modo da garantire la sicurezza delle informazioni.

Sono definiti controlli di accesso appropriati per garantire che l'accesso alle informazioni sia limitato ai soggetti autorizzati. Vengono adottate politiche e procedure per gestire i privilegi di accesso, le credenziali degli utenti, l'autenticazione e l'autorizzazione.

L'organizzazione stabilisce e implementa procedure per la gestione delle attività di sistema, comprese la gestione degli incidenti di sicurezza, il monitoraggio dei registri di sistema, l'inventario delle informazioni, l'uso accettabile delle informazioni, la restituzione delle attività, la classificazione delle informazioni, l'etichettatura e il trasferimento delle informazioni, il backup dei dati e la gestione delle vulnerabilità.

L'organizzazione si impegna a conformarsi a tutte le leggi e le normative applicabili in materia di sicurezza delle informazioni. Vengono definiti processi per identificare, monitorare e garantire la conformità alle disposizioni legislative e regolamentari pertinenti.

Le informazioni archiviate possono essere soggette ad accesso e gestione da parte del fornitore di servizi cloud. Il cliente che usufruisce del servizio in cloud deve adottare misure di sicurezza adeguate a proteggere le informazioni sensibili e definire i livelli di accesso e le autorizzazioni per il fornitore di servizi cloud.

Le risorse, come i programmi applicativi, possono essere mantenute nell'ambiente di cloud computing. Il cliente del servizio cloud deve garantire la sicurezza di queste risorse, ad esempio, implementando controlli di accesso appropriati e adottando misure per prevenire la compromissione dei programmi applicativi.

I processi possono essere eseguiti su un servizio cloud virtualizzato e multi-tenant. Il cliente del servizio cloud deve considerare i rischi associati alla condivisione di risorse con altri utenti del servizio cloud e adottare misure per isolare e proteggere le proprie risorse e i propri dati.

Il cliente del servizio cloud deve tenere conto degli utenti del servizio cloud e del contesto in cui utilizzano il servizio cloud. Deve essere stabilito un processo di autenticazione e autorizzazione per garantire che solo gli utenti autorizzati possano accedere al servizio cloud.

Gli amministratori del servizio cloud del cliente del servizio cloud che hanno accesso privilegiato devono essere soggetti a controlli adeguati. Deve essere definito un processo per la gestione degli amministratori e per garantire che i privilegi siano assegnati in base alle necessità di lavoro.

Il cliente del servizio cloud deve prendere in considerazione le ubicazioni geografiche dell'organizzazione del fornitore di servizi cloud e i Paesi in cui il fornitore di servizi cloud può memorizzare i dati del cliente del servizio

cloud. Devono essere adottate misure adeguate per garantire la conformità alle leggi e ai regolamenti applicabili in materia di protezione dei dati e privacy.

Magnetic Media Network S.p.A. riconosce l'importanza di stabilire termini e condizioni contrattuali chiari e trasparenti con i suoi clienti per garantire la protezione delle PII. I nostri contratti delineano le responsabilità e gli obblighi di entrambe le parti in relazione alla gestione delle PII. I termini contrattuali includono, fra le altre:

- Finalità del trattamento: Specifichiamo le finalità per cui raccogliamo e trattiamo le PII dei clienti, assicurandoci che siano in linea con le leggi e i regolamenti applicabili.
- Base giuridica del trattamento: Indichiamo la base giuridica su cui ci basiamo per il trattamento delle PII dei clienti, come il consenso esplicito del cli- ente o l'esecuzione di un contratto.
- Trasferimento delle PII: Se le PII dei clienti vengono trasferite al di fuori dell'UE o di altre giurisdizioni in cui la protezione dei dati potrebbe essere diversa, ci impegniamo a garantire che tali trasferimenti avvengano in conformità con le leggi e i regolamenti applicabili.
- Misure di sicurezza: Descriviamo le misure di sicurezza tecniche e organizzative che adottiamo per proteggere le PII dei clienti da accessi non autorizzati, perdite o divulgazioni indebite.
- Periodo di conservazione: Specifichiamo il periodo per cui conserviamo le PII dei clienti e le modalità di distruzione o anonimizzazione delle informazioni una volta scaduto il periodo di conservazione.
- Subappaltatori: Nel caso in cui ci sia necessità di ricorrere al sub appalto Magnetic Media Network S.p.A. specificherà se l'incaricato del trattamento può avvalersi di subappaltatori per fornire i servizi cloud e quali misure di sicurezza devono essere adottate nei confronti di tali subappaltatori.
- Ubicazione dei servizi: Le informazioni dei clienti di Magnetic Media Network S.p.A. verranno ospitati in Datacenter con adeguate misure tecniche ed organizzative.
- Costruzione di un proprio livello di infrastruttura: Magnetic Media Network S.p.A. si impegna a proteggere la privacy e la sicurezza dei dati dei propri clienti. In conformità con il GDPR consente ai propri clienti di costruire il proprio livello di sicurezza all'interno dell'infrastruttura cloud dell'incaricato del trattamento:
    - Crittografia
    - Accesso e controllo
    - Sicurezza fisica
    - Sicurezza del software

Magnetic Media Network S.p.A. si impegna ad adire le opportune azioni disciplinari o legali nei confronti dei soggetti che abbiano tenuto un comportamento illegittimo in contrasto con i principi della presente Politica, mettendo a disposizione degli stakeholder canali di comunicazione atti ad incoraggiare a segnalare in buona fede fenomeni sospetti, senza timore di subire ritorsioni.

La presente politica di sicurezza delle informazioni deve essere periodicamente revisionata e aggiornata per assicurare la sua efficacia continua e la conformità alle norme e alle best practice di sicurezza delle informazioni.

Magnetic Media Network S.p.A. si impegna a valutare periodicamente l'efficacia del SGSI attraverso gli audit interni e i riesami della direzione. Sono definiti meccanismi per raccogliere e analizzare le prestazioni del SGSI al fine di identificare opportunità di miglioramento e prendere le necessarie azioni correttive.

CEO

Data: 03/05/2024

_____

(PIER DAMIANO AIROLDI)