Introduzione:

PROMOFARMA SVILUPPO SRL, con l'obiettivo di fornire ai propri clienti un servizio sempre più professionale garantendo la sicurezza delle informazioni e 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 delCloud Computing. Promofarma Sviluppo si impegna a garantire la protezione adeguata delle informazioni personali identificabili (PII) dei suoi clienti. Come parte di questo impegno, ci sforziamo di raggiungere la conformità con le leggi e i regolamenti applicabili in materia di protezione delle PII. Questo documento di politica descrive le misure che adottiamo per garantire il rispetto della legislazione sulla privacy, inclusi il Regolamento generale sulla protezione dei dati (GDPR), la legge nazionale sulla protezione dei dati (DPA) 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 UNI EN ISO 27001 al fine di proteggere le informazioni critiche e mitigare i rischi associati alla loro gestione.

Obiettivi:

a. Identificare e valutare i rischi per la sicurezza delle informazioni.
b. Definire misure di sicurezza adeguate per mitigare i rischi identificati.
c. Garantire la conformità alle leggi e alle normative applicabili in materia di sicurezza delle informazioni.
d. Promuovere la consapevolezza e la formazione del personale in merito alla sicurezza delle informazioni.
e. Monitorare e valutare costantemente l'efficacia del SGSI.

Conformità con la legislazione sulla protezione delle PII:

Promofarma Sviluppo si impegna a rispettare tutte le leggi e i regolamenti applicabili in materia di protezione delle PII. Ci impegniamo a condurre una ricerca accurata e continua per identificare le leggi e i regolamenti specifici che si applicano alle nostre operazioni in vari giurisdizioni. 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) e la DPA nei paesi in cui tali leggi sono in vigore. Adottiamo misure tecniche e organizzative adeguate per garantire la protezione delle PII, inclusa l'implementazione di misure di sicurezza adeguate, la nomina di un responsabile della protezione dei dati (Data Pro-

tection Officer) e la conduzione di valutazioni periodiche dell'impatto sulla protezione dei dati (Data Protection Impact Assessments) quando necessario.

1. Ambito di applicazione:
   La politica per la norma UNI EN ISO 27001, 27017, 27018 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.

2. Responsabilità:
   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.

3. Gestione dei rischi:
   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.

4. Sicurezza delle risorse umane:
   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 per la selezione, l'addestramento, l'assegnazione delle responsabilità e la gestione delle risorse umane in modo da garantire la sicurezza delle informazioni.

5. Controllo degli accessi:
   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.

6. Gestione delle attività di sistema:
   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 formazioni, l'etichettatura e il trasferimento delle informazioni, il backup dei dati e la gestione delle vulnerabilità.

7. Conformità legale:
   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.

8. Accesso e gestione delle informazioni
   Le informazioni archiviate nell'ambiente di cloud computing possono essere soggette ad accesso e gestione da parte del fornitore di servizi cloud. Il cliente del servizio cloud deve adottare misure di sicurezza adeguate per proteggere le informazioni sensibili e definire i livelli di accesso e le autorizzazioni per il fornitore di servizi cloud.

9. Risorse nell'ambiente di cloud computing
   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.

10. Servizi cloud virtualizzati e multi-tenant
    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.

11. Utenti del servizio cloud
    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.

12. Amministratori del 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.

13 Ubicazioni geografiche e memorizzazione dei dati

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.

14.Termini contrattuali con i clienti

Promofarma Sviluppo 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 cliente 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.
- Responsabilità: Promofarma Sviluppo ha individuato RSGSI-AD (l'Amministratore Delegato) come responsabile della protezione dei dati personali nel contesto del trattamento cloud.
- Subappaltatori: Nel caso in cui ci sia necessità di ricorrere al sub appalto Promofarma Sviluppo srl 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 Promofarma Sviluppo srl verranno ospitati in Datacenter italiani e non possono essere trasferiti in altre giurisdizioni.
- Architettura della rete cloud: Il fornitore di servizi Cloud è certificato Iso IEC 27001, 27018, 27017
- Acquisto di servizi da fornitori: Promofarma Sviluppo srl acquisisce servizi cloud da fornitori come IAAS (Infrastructure-as-a-Service) da fornitore certificato Iso IEC 27001, 27018, 27017
- Costruzione di un proprio livello di infrastruttura: Promofarma Sviluppo srl 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

15. Valutazione e miglioramento:

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.

L'organizzazione si impegna a valutare periodicamente l'efficacia del SGSI attraverso audit interni e revisioni di gestione. Sono definiti meccanismi per raccogliere e analizzare le prestazioni del SGSI al fine di identificare opportunità di miglioramento e prendere le necessarie azioni correttive.