Security Lab
SICUREZZA ON LINE

MISURE DI SICUREZZA

Le misure di sicurezza che un'azienda deve adottare per essere conforme al GDPR riguardano sia gli aspetti tecnici che quelli organizzativi, per proteggere i dati personali da accessi non autorizzati, perdita, alterazione o distruzione. Le misure variano in base al tipo di dati trattati, ai rischi specifici e alle dimensioni dell'azienda, ma in generale includono le seguenti:

1. Pseudonimizzazione e Crittografia dei Dati

- **Pseudonimizzazione**: Consiste nel trattare i dati in modo tale che non possano essere attribuiti a un soggetto senza l'uso di informazioni aggiuntive, che devono essere conservate separatamente e protette.
- **Crittografia**: I dati personali devono essere criptati sia durante la trasmissione (ad esempio, tramite HTTPS) sia durante l'archiviazione (encryption at rest). Questo assicura che, anche in caso di accesso non autorizzato, i dati non siano leggibili.

2. Controllo degli Accessi

- Limitare l'accesso ai dati personali solo al personale autorizzato che ne ha necessità per eseguire le proprie mansioni.
- Implementare **sistemi di autenticazione forte** (come l'autenticazione a due fattori) per prevenire accessi non autorizzati.
- Utilizzare **ruoli e privilegi** per assicurare che gli utenti abbiano accesso solo ai dati necessari.

3. Gestione delle Password

- Le password devono essere robuste (lunghe, complesse e difficili da indovinare) e gestite in modo sicuro.
- Implementare politiche di aggiornamento regolare delle password e strumenti per la gestione delle password sicura, come i password manager.

- Vietare l'uso di password predefinite e richiedere password uniche per ogni utente e sistema.

4. Backup dei Dati

- Effettuare **backup regolari e sicuri** dei dati personali per prevenire la perdita o il danneggiamento dei dati in caso di guasti, attacchi o incidenti.
- I backup devono essere conservati in una posizione sicura e, preferibilmente, crittografati.
- Testare regolarmente il ripristino dei dati dai backup per verificarne l'integrità.

5. Protezione dai Malware e Minacce Esterne

- Installare e aggiornare regolarmente **software antivirus, antimalware e firewall** per proteggere i sistemi aziendali da attacchi esterni.
- Implementare meccanismi di rilevamento e prevenzione delle intrusioni (IDS/IPS) per monitorare attività sospette sulla rete.

6. Monitoraggio e Audit

- Monitorare l'accesso ai dati personali e le operazioni di trattamento attraverso **log di accesso** e sistemi di monitoraggio delle attività.
- Eseguire **audit regolari** per valutare la sicurezza dei sistemi e identificare potenziali vulnerabilità o aree di miglioramento.

7. Formazione del Personale

- Formare regolarmente i dipendenti sulle best practices di sicurezza e sui loro obblighi legati alla protezione dei dati.
- Implementare politiche aziendali chiare in merito al trattamento sicuro dei dati, all'uso dei dispositivi aziendali e personali (BYOD), alla gestione delle email e al phishing.

8. Gestione delle Minacce Interne

- Adottare misure per proteggere i dati da minacce interne (dipendenti o collaboratori), come:

- Politiche di accesso basate su principi di **least privilege** (accesso minimo necessario).
- Limitare l'uso di dispositivi personali per il trattamento di dati aziendali.
- Utilizzare strumenti di **Data Loss Prevention (DLP)** per monitorare, controllare e prevenire la trasmissione non autorizzata di dati.

9. Controllo degli Accessi Fisici

- Proteggere l'accesso fisico ai server, ai dispositivi di archiviazione e alle aree in cui vengono trattati i dati personali.
- Implementare sistemi di controllo accessi fisici, come badge identificativi, videocamere di sorveglianza, e serrature elettroniche.

10. Valutazione dei Fornitori

- Assicurarsi che i fornitori e i partner terzi che trattano dati personali adottino misure di sicurezza adeguate.
- Stipulare accordi (Data Processing Agreement) con i fornitori per garantire che il trattamento dei dati sia conforme al GDPR.

11. Valutazione e Gestione dei Rischi

- Condurre regolarmente una **valutazione del rischio** per identificare e mitigare potenziali vulnerabilità nei sistemi di gestione dei dati.
- Implementare una **Valutazione d'Impatto sulla Protezione dei Dati (DPIA)** quando un trattamento comporta rischi elevati per i diritti e le libertà degli individui.

12. Piani di Continuità Operativa e Recupero di Emergenza

- Avere in atto un **piano di continuità operativa** che includa misure per il recupero dei dati e il ripristino dei servizi in caso di incidenti, disastri o attacchi.
- Testare regolarmente il piano per assicurarsi che sia efficace in caso di emergenza.

13. Notifica delle Violazioni di Dati

- In caso di violazione dei dati, l'azienda deve avere una procedura per:
  - **Identificare e documentare** la violazione.
  - **Notificare l'autorità di controllo** (ad es. il Garante Privacy) entro 72 ore.
  - **Informare i soggetti interessati** se la violazione rappresenta un rischio elevato per i loro diritti e libertà.

14. Protezione dei Dati durante il Trasferimento

- Se i dati personali vengono trasferiti al di fuori dello Spazio Economico Europeo (SEE), l'azienda deve assicurarsi che siano protetti da adeguate garanzie, come:
  - Clausole contrattuali standard approvate dalla Commissione Europea.
  - Decisioni di adeguatezza che certificano che il paese terzo offra un livello di protezione adeguato.

15. Distruzione Sicura dei Dati

- Quando i dati personali non sono più necessari per lo scopo per cui sono stati raccolti, devono essere cancellati in modo sicuro. Questo include la **distruzione fisica di supporti** (ad esempio, triturazione dei documenti cartacei) o la cancellazione sicura di dati digitali mediante tecniche di sovrascrittura o distruzione dei dischi.

16. Segmentazione della Rete Separare le reti interne aziendali per limitare l'accesso non autorizzato e isolare i dati sensibili su segmenti di rete sicuri.

Adottando queste misure, un'azienda può ridurre i rischi legati al trattamento dei dati personali e garantire la conformità al GDPR, dimostrando un impegno serio nella protezione della privacy degli individui.