Security Lab
SICUREZZA ON LINE

Misure di Sicurezza per la Conformità al GDPR

Le aziende devono adottare misure tecniche e organizzative per proteggere i dati personali da accessi non autorizzati, perdite, alterazioni o distruzioni. Le misure variano in base al tipo di dati trattati, ai rischi e alle dimensioni dell'azienda, ma generalmente includono:

1. Pseudonimizzazione e Crittografia dei Dati

- **Pseudonimizzazione**: Trattare i dati in modo che non siano attribuibili a un soggetto senza informazioni aggiuntive (conservate separatamente).
- **Crittografia**: Criptare i dati in transito (es. HTTPS) e in archivio (encryption at rest).

2. Controllo degli Accessi

- Limitare l'accesso solo al personale autorizzato.
- Usare autenticazione forte (es. 2FA) e gestione dei privilegi (principio del minimo accesso).

3. Gestione delle Password

- Password complesse e aggiornate periodicamente.
- Vietare password predefinite e usare password manager.

4. Backup dei Dati

- Backup regolari, crittografati e conservati in luoghi sicuri.
- Testare periodicamente il ripristino.

5. Protezione da Malware e Minacce Esterne

- Antivirus, firewall e sistemi IDS/IPS aggiornati.
- Rilevamento di intrusioni e attività sospette.

6. Monitoraggio e Audit

- Log degli accessi e audit periodici per identificare vulnerabilità.

7. Formazione del Personale

- Corsi su sicurezza informatica, phishing e best practices GDPR.

8. Gestione delle Minacce Interne

- Limitare l'accesso ai dati sensibili (least privilege).
- Usare strumenti di **Data Loss Prevention (DLP)** per prevenire fughe di dati.

9. Controllo degli Accessi Fisici

- Proteggere server e aree con dati sensibili tramite badge, videocamere e serrature sicure.

10. Valutazione dei Fornitori

- Verificare che i partner rispettino il GDPR e stipulare **Data Processing Agreement (DPA)**.

11. Valutazione e Gestione dei Rischi

- **DPIA (Valutazione d'Impatto sulla Privacy)** per trattamenti ad alto rischio.

12. Piani di Continuità Operativa e Disaster Recovery

- Procedure per ripristinare dati e servizi dopo incidenti.

13. Notifica delle Violazioni di Dati

- Segnalare violazioni al Garante Privacy entro **72 ore** e agli interessati se il rischio è elevato.

14. Trasferimento di Dati Fuori dall'UE

- Usare **clausole contrattuali standard** o verificare l'**adeguatezza** del paese terzo.

15. Distruzione Sicura dei Dati

- Cancellazione sicura (crittografica o sovrascrittura) o distruzione fisica (es. triturazione documenti).

16. Segmentazione della Rete

- Isolare reti interne per limitare accessi non autorizzati.

Conclusione

L'adozione di queste misure riduce i rischi e garantisce la conformità al GDPR, dimostrando impegno nella protezione della privacy.