Security Lab
SICUREZZA ON LINE

GDPR

Per essere in linea con il **Regolamento Generale sulla Protezione dei Dati (GDPR)**, un'azienda deve adottare una serie di misure per garantire la protezione dei dati personali degli individui. Ecco i principali requisiti che un'azienda deve rispettare:

1. Consenso Informato

- Ottenere il consenso esplicito e informato dagli individui prima di raccogliere, trattare o condividere i loro dati personali.
- Il consenso deve essere chiaro, non ambiguo, revocabile in qualsiasi momento e non deve essere predefinito tramite caselle già selezionate.

2. Trasparenza

- Informare gli individui su come vengono raccolti, utilizzati, conservati e trattati i loro dati personali. Questo avviene solitamente tramite una **privacy policy** chiara e accessibile.

3. Gestione dei Diritti degli Interessati

L'azienda deve consentire alle persone di esercitare i loro diritti previsti dal GDPR:

- **Diritto di accesso:** Gli individui possono richiedere una copia dei propri dati personali.
- **Diritto alla rettifica:** Gli utenti possono correggere eventuali dati errati o incompleti.
- **Diritto all'oblio:** Gli individui possono richiedere la cancellazione dei propri dati in determinate circostanze.
- **Diritto alla portabilità dei dati:** Gli individui possono trasferire i propri dati a un altro fornitore.
- **Diritto di opposizione:** Gli individui possono opporsi al trattamento dei propri dati per scopi specifici.
- **Diritto alla limitazione del trattamento:** Gli individui possono limitare l'uso dei propri dati personali.

4. Responsabile della Protezione dei Dati (DPO)

- Se un'azienda tratta dati personali su larga scala o gestisce categorie particolari di dati (sensibili), deve nominare un **Responsabile della Protezione dei Dati (DPO)**, incaricato di supervisionare la conformità alle norme del GDPR.

5. Valutazione d'Impatto sulla Protezione dei Dati (DPIA)

- Se un'azienda esegue trattamenti che possono comportare un rischio elevato per i diritti e le libertà delle persone, deve eseguire una **DPIA** per valutare e mitigare tali rischi.

6. Registro dei Trattamenti

- Tenere un registro aggiornato dei trattamenti dei dati personali, contenente informazioni su quali dati vengono trattati, per quale scopo, chi vi ha accesso e come vengono protetti.

7. Misure di Sicurezza

- Implementare adeguate **misure tecniche e organizzative** per proteggere i dati personali contro accessi non autorizzati, perdite o distruzione. Questo può includere la crittografia, controlli di accesso e backup regolari.

8. Notifica di Violazione dei Dati

- In caso di violazione dei dati personali (data breach), l'azienda deve notificare l'autorità di controllo competente (es. il Garante Privacy) entro **72 ore**, se la violazione rappresenta un rischio per i diritti e le libertà degli individui. Se il rischio è elevato, è necessario informare anche i soggetti interessati.

9. Accordi con i Fornitori e Subappaltatori

- Se l'azienda esternalizza attività che coinvolgono dati personali, deve avere accordi contrattuali con i fornitori che garantiscano la conformità al GDPR (es. Data Processing Agreement).

10. Minimizzazione dei Dati

- Trattare solo i dati personali **strettamente necessari** per raggiungere lo scopo per cui vengono raccolti, evitando il trattamento di dati in eccesso.

11. Formazione e Sensibilizzazione

- L'azienda deve formare i propri dipendenti e sensibilizzarli sui principi del GDPR, affinché comprendano l'importanza della protezione dei dati e il loro ruolo nel garantire la conformità.

12. Base Giuridica per il Trattamento

- Ogni trattamento di dati deve basarsi su una **base giuridica valida** prevista dal GDPR, come il consenso, l'esecuzione di un contratto, l'obbligo legale o un legittimo interesse.

Rispettando questi principi, un'azienda può mantenere la conformità con il GDPR e ridurre il rischio di sanzioni, che possono essere molto elevate (fino al 4% del fatturato globale annuo o 20 milioni di euro, a seconda di quale sia maggiore)