

Linee Guida per il GDPR

Per essere conformi al **Regolamento Generale sulla Protezione dei Dati (GDPR)**, le aziende devono adottare misure precise per proteggere i dati personali delle persone fisiche. Ecco i principali requisiti da rispettare:

1. Consenso Informato

- Ottenere il **consenso esplicito e consapevole** prima di raccogliere, trattare o condividere dati personali.
 - Il consenso deve essere:
 - **Chiaro e non ambiguo**
 - **Revocabile** in qualsiasi momento
 - **Non preimpostato** (no caselle già selezionate)
-

2. Trasparenza

- Informare gli utenti su:
 - Come vengono raccolti e usati i loro dati
 - Dove e per quanto tempo vengono conservati
 - Utilizzare una **privacy policy** chiara, accessibile e aggiornata.
-

3. Diritti degli Interessati

Le persone devono poter esercitare i seguenti diritti:

- **Accesso**: conoscere quali dati personali sono trattati.
 - **Rettifica**: correggere dati errati o incompleti.
 - **Cancellazione (diritto all'oblio)**: richiedere l'eliminazione dei dati in specifici casi.
 - **Portabilità**: trasferire i dati a un altro fornitore.
 - **Opposizione**: rifiutare il trattamento per motivi legittimi.
 - **Limitazione**: bloccare temporaneamente l'uso dei dati.
-

4. Responsabile della Protezione dei Dati (DPO)

- Obbligatorio se l'azienda:
 - Tratta dati su **larga scala**
 - Gestisce dati **sensibili** (salute, orientamento sessuale, ecc.)
 - Il DPO verifica la conformità al GDPR e fa da punto di contatto con le autorità.
-

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

- Necessaria se il trattamento comporta **rischi elevati** per i diritti e le libertà degli interessati.
 - Serve a **valutare** i rischi e **definire misure** per ridurli.
-

6. Registro dei Trattamenti

- Documentare:
 - Quali dati vengono trattati
 - Per quali scopi
 - Chi vi ha accesso
 - Come sono protetti
 - Il registro deve essere **aggiornato** e disponibile in caso di controlli.
-

7. Misure di Sicurezza

- Adottare soluzioni tecniche e organizzative per proteggere i dati da:
 - Accessi non autorizzati
 - Perdita o distruzione accidentale
 - Esempi: **crittografia, backup regolari, controlli di accesso.**
-

8. Notifica di Violazione dei Dati (Data Breach)

- In caso di violazione:
 - Notificare l'**autorità competente** (es. Garante Privacy) entro **72 ore**
 - Informare anche gli interessati **se il rischio è elevato**
-

9. Accordi con Fornitori e Subappaltatori

- Quando si esternalizzano attività che coinvolgono dati personali:
 - Firmare un **contratto specifico** (es. **Data Processing Agreement**) che garantisca la conformità al GDPR.
-

10. Minimizzazione dei Dati

- Raccogliere e trattare **solo i dati strettamente necessari.**
 - Evitare la raccolta di dati inutili o in eccesso.
-

11. Formazione e Sensibilizzazione

- Informare e formare il personale sul GDPR e sull'importanza della protezione dei dati.
 - Creare **una cultura della privacy** in azienda.
-

12. Base Giuridica del Trattamento

- Ogni trattamento deve basarsi su una delle **basi legali previste** dal GDPR:
 - **Consenso**
 - **Contratto**
 - **Obbligo legale**
 - **Legittimo interesse**
-

☐ **Conclusione**

Rispettando queste linee guida, un'azienda:

- Garantisce i diritti delle persone
- Riduce i rischi di violazioni e sanzioni
- Dimostra trasparenza e affidabilità

💡 **Attenzione:** le sanzioni per la mancata conformità al GDPR possono arrivare fino al **4% del fatturato annuo globale** o **20 milioni di euro**, a seconda di quale importo sia maggiore.