Ecco una **checklist completa** per verificare se l'azienda è conforme alle misure di sicurezza previste dal **GDPR** (Regolamento Generale sulla Protezione dei Dati) in relazione a:

- **Struttura informatica**
- **Gestione della privacy e dei dati personali**

□ Checklist GDPR – Sicurezza Informatica e Privacy

🗂️ 1. Valutazione e Mappatura dei Dati

- ☐ È stato redatto un **registro dei trattamenti** aggiornato (art. 30 GDPR)?
- ☐ Sono stati identificati tutti i dati personali trattati e i relativi scopi?
- ☐ Sono stati classificati i dati in base alla loro **sensibilità** (es. dati sanitari, biometrici, ecc.)?
- ☐ È stata effettuata una **Valutazione d'Impatto sulla Protezione dei Dati (DPIA)** dove necessaria?

🔐 2. Sicurezza della Struttura Informatica

- ☐ Sono presenti **firewall**, **antivirus** e **sistemi IDS/IPS** attivi e aggiornati?
- ☐ Tutti i dispositivi aziendali sono protetti con **autenticazione sicura** (password complesse, MFA)?
- ☐ I dati personali sono **crittografati** sia in transito che a riposo?
- ☐ I backup vengono effettuati regolarmente e **testati** per il ripristino?
- ☐ È presente una **policy di gestione degli accessi** basata su ruoli e necessità?
- ☐ I software utilizzati sono **aggiornati** e **supportati** (patch management attivo)?
- ☐ L'accesso remoto (VPN, desktop remoto) è **sicuro** e **monitorato**?
- ☐ I dispositivi mobili aziendali sono soggetti a **MDM (Mobile Device Management)**?

💻 3. Gestione degli Utenti e Formazione

- ☐ Tutti i dipendenti sono stati **formati** sul GDPR e la sicurezza dei dati?
- ☐ Esiste un **processo formale di onboarding/offboarding** per gestire gli accessi?
- ☐ Sono presenti **log di accesso** e attività sugli account?
- ☐ I dipendenti sono tenuti a firmare **accordi di riservatezza**?
- ☐ È prevista una politica per evitare **shadow IT** (software non autorizzato)?

🔄 4. Gestione dei Dati Personali

- ☐ Gli interessati sono informati tramite **informative privacy trasparenti** (art. 13-14)?
- ☐ Sono in atto procedure per **rispondere alle richieste degli interessati** (accesso, rettifica, cancellazione, portabilità)?
- ☐ Esiste una procedura interna per la **notifica di violazioni dei dati (data breach)** entro 72 ore?
- ☐ I dati vengono **cancellati o anonimizzati** al termine del trattamento?
- ☐ È stato definito un **periodo di conservazione** per ciascun tipo di dato?

🔄 5. Gestione di Terze Parti e Fornitori

- ☐ Tutti i fornitori che trattano dati personali per conto dell'azienda sono stati **valutati**?
- ☐ Sono stati firmati **contratti di nomina a Responsabile del trattamento** (art. 28)?
- ☐ Sono in atto misure per verificare periodicamente la **compliance dei fornitori**?

📊 6. Audit, Monitoraggio e Miglioramento Continuo

- ☐ Sono stati effettuati **audit interni** o esterni sulla sicurezza e privacy?
- ☐ Sono documentati i risultati e i **piani di azione correttiva**?
- ☐ L'azienda ha nominato un **DPO (Data Protection Officer)**, se obbligatorio?
- ☐ Esiste un **piano di continuità operativa** e un **disaster recovery plan**?

---

info@securitylab.services

🔑 7. Eventuali Documenti da Tenere a Disposizione

- ☐ Registro dei trattamenti
- ☐ Informative privacy
- ☐ Contratti con responsabili esterni
- ☐ DPIA (se presenti)
- ☐ Policy aziendali (privacy, sicurezza, BYOD, accessi, ecc.)
- ☐ Log di sicurezza e accessi
- ☐ Evidenze delle attività formative
