|  |  |
| --- | --- |
| Requisiti | Possesso requisito (Sì|No) - Note |
| La Società ha definito una policy privacy e di sicurezza IT *compliant* alla normativa di settore? |  |
| La Società ha nominato un *Data Protection Officer* (Responsabile della Protezione dei Dati)? Se sì, indicare i riferimenti. |  |
| La Società ha definito una struttura specializzata in ambito privacy, identificando funzioni preposte per la gestione di eventuali anomalie o violazioni correlate al trattamento dei dati personali? |  |
| La Società ha formalizzato un registro dei trattamenti ed è in grado di dimostrarlo? |  |
| La Società ha effettuato una valutazione d’impatto (DPIA) al fine di tutelare le libertà e i diritti degli interessati ed è in grado di dimostrarlo? |  |
| La Società ha formalizzato una procedura di *Incident Management* ed è in grado di dimostrarlo? |  |
| La Società ha formalizzato una procedura di *Data Breach* ed è in grado di dimostrarlo? |  |
| La Società ha definito un *Disaster Recovery Plan* ed è in grado di dimostrarlo? |  |
| La Società ha definito un *Business Continuity Plan* ed è in grado di dimostrarlo? |  |
| La Società ha formalizzato una procedura di *Change management* ed è in grado di dimostrarlo? |  |
| La Società ha messo in atto una procedura per la gestione delle utenze secondo il principio del “*need to know”* e prevede un sistema di separazione dei compiti e responsabilità in base al servizio richiesto? |  |
| La Società ha messo in atto procedure di sicurezza sui dati personali a rischio alto come la cifratura o la pseudonimizzazione? Se sì, quali? |  |
| La Società prevede iniziative di formazione e sensibilizzazione destinate al personale interno ed esterno (ad esempio consulenti e dipendenti di partner commerciali) sul corretto utilizzo delle applicazioni e degli strumenti informatici sotto il profilo della privacy/della sicurezza informatica e della riservatezza delle informazioni ed è in grado di documentarlo? |  |
| La Società ha censito i propri *asset*, *device* mobili aziendali e supporti (ad es. server, pc, tablet, smartphone, chiavette USB) in ottica privacy? |  |
| Tali *device* sono criptati? Quali in particolare? |  |
| La Società ha messo in atto delle misure per proteggere i locali all'interno dei quali sono contenuti dati personali? (es. sale CED, archivi cartacei, ecc.)? |  |
| La Società garantisce gli aggiornamenti di sicurezza dei dispositivi concessi ai propri dipendenti nonché delegati/subfornitori? |  |
| La Società dispone di sistemi di difesa perimetrale? Se sì, quali? |  |
| La Società effettua delle attività di Log Management relativamente alle attività svolte dai propri utenti? |  |
| La Società ha adottato dei sistemi di *backup* che contribuiscono ad innalzare il livello di protezione da perdita di dati personali? |  |
| Ne caso in cui il servizio da fornire richiede la connessione per lo scambio di dati personali e critici, la Società dispone di una rete protetta (es. VPN)? |  |
| La Società ha provveduto a nominare gli amministratori di sistema in conformità con le disposizioni specifiche in materia adottate dal Garante Privacy italiano? |  |
| La Società dispone di un *tool di ticketing* per la gestione delle abilitazioni, delle *change* e degli *incident* a sistema in ottica privacy? |  |
| È possibile produrre una reportistica relativa all’utilizzo di tale tool? |  |
| È prevista una policy di autenticazione e di gestione dell’uso personale delle utenze e password (ad es. gestione della lunghezza, complessità, durata, conservazione sicura delle password, il censimento delle password tecniche, ecc.) e può provarlo? |  |
| È prevista una procedura per la periodica validazione e il censimento delle utenze e delle abilitazioni e può provarlo? |
| La Società ha nominato dei subfornitori che offrono servizi di supporto in ambito IT e ha previsto delle procedure per la gestione dell'accesso alla rete da parte di questi? |  |
| La Società ha effettuato un *penetration* test negli ultimi 12 mesi ed è in grado di dimostrarlo? |  |
| In caso di fornitura di applicazione e sviluppo delle stesse sono previsti test di sicurezza e può provarlo? |  |
| La Società ha subito degli attacchi che hanno comportato la violazione dei dati personali negli ultimi 12 mesi? |  |
| La Società effettua periodicamente delle verifiche per valutare la riservatezza, l'integrità, la disponibilità e resilienza dei dati personali? |  |
| La Società effettua periodicamente delle verifiche per valutare l'adeguatezza delle misure organizzative e tecniche preposte per la protezione dei dati? |  |
| La Società ha ottenuto una delle seguenti certificazioni?  - ISAE 3402 (SOC1 e/o SOC2 type 2)  - SSA16 (SOC1 e/o SOC2 type 2)  - ISO 27001  - ISO 22301 |  |
| La Società ha ottenuto altre certificazioni in ambito *privacy*/*security*? Se sì, quali? |  |