Regione Siciliana
**AZIENDA SANITARIA PROVINCIALE DI SIRACUSA**
**Corso Gelone, 17 – 96100 Siracusa (SR)**
Cod. Fisc./P.IVA: 01661590891

**Allegato II – "Misure di Sicurezza"**

# Checklist Privacy

| Domande | Risposta (di base SI/NO) |
|---|---|
| **Controlli generali** | |
| Il responsabile ha attivato in prima persona, una politica di protezione dei dati, debitamente documentata e regolarmente aggiornata? | |
| Quale è la struttura di supporto che verifica e mantiene aggiornata questa politica? | |
| Le procedure di protezione dei dati sono documentate formalmente ove richiesto (ad es. in materia di amministratori di sistema), e periodicamente riesaminate, e comprovate con documenti oggettivi (ad esempio con verbali di riunioni, liste, logs informatici), che attestino la costante diligenza e vigilanza nello svolgimento dell'attività di protezione dei dati personali? | |
| **Diritto di accesso (art. 15 e segg.)** | |
| Tutti gli incaricati aziendali sono al corrente delle modalità di esercizio del diritto di accesso e della procedura di comunicazione delle richieste di esercizio dei diritti al Titolare? | |
| Esiste un registro generale delle richieste di accesso? | |
| Chi è la persona/funzione responsabile per fornire spiegazioni scritte al Titolare? | |
| Le procedure in atto, che consentono al Titolare di conoscere le richieste degli interessati al diritto di accesso, sono tali da facilitare e rapidizzare al massimo tale comunicazione? | |
| Esiste un termine massimo di comunicazione delle richieste al Titolare? | |
| Se il responsabile offre una piattaforma/servizio tecnologico ha condiviso con il Titolare una procedura per il riscontro delle richieste di limitazione, cancellazione, portabilità dei dati personali? | |
| Il Responsabile ha condiviso una procedura per documentare per iscritto al Titolare l'evasione di una richiesta scritta di limitazione, cancellazione, portabilità? | |

| Domande | Risposta (di base SI/NO) |
|---|---|
| **Informativa (art. 13)** – ove applicabile | |
| Le persone incaricate di offrire l'informativa e della raccolta del consenso, anche per conto del Titolare, sono state formate in modo specifico? | |
| Vengono effettuati controlli periodici sul comportamento delle persone addette alla offerta di informativa e raccolta di consenso? | |
| In fase di informativa, il personale addetto è in grado di informare con chiarezza l'interessato dei suoi diritti, oralmente o per iscritto? | |
| Vengono registrate le fonti da cui sono ricavati i dati personali? | |
| **Incaricati (art. 29)** | |
| Tutti gli incaricati sono stati formalmente designati come tali, personalmente o per classi omogenee? | |
| Tutti gli incaricati, personalmente o per classi omogenee, hanno ricevuto specifiche istruzioni scritte sulla modalità di trattamento e protezione dei dati personali? | |
| È aggiornato l'elenco degli incaricati del trattamento ed essi hanno tutti ricevuto adeguata formazione e istruzione? | |
| Tale formazione è adeguatamente documentata? | |
| Viene periodicamente verificato che il privilegio di accesso, concesso agli incaricati del trattamento, sia congruo ed aggiornato, e che le istruzioni impartite siano anch'esse aggiornate? | |
| Il Responsabile si avvale di partner nell'erogazione dei servizi oggetto di Accordo con il Titolare? | |
| Esistono rapporti ulteriori con responsabili esterni (cd. sub-responsabili) limitatamente alle attività connesse al trattamento di dati personali effettuato per conto del Titolare, rispetto a quelli già indicati? | |
| **Misure di sicurezza** | |
| Esistono dei contenitori sicuri, in numero e distribuzione appropriati, a disposizione degli incaricati per la custodia anche temporanea dei dati personali, sotto qualunque forma (cartacea, magnetica, ecc.)? | |
| Esiste una politica di gestione e controllo delle chiavi di sicurezza dei contenitori sicuri, del sito del trattamento ed in genere di tutti i luoghi e contenitori ove possono trovarsi dati personali? | |
| Vengono effettuati controlli circa il fatto che i documenti contenenti dati sensibili non vengano lasciati incustoditi, quando sono affidati agli incaricati e si trovano all'esterno degli archivi protetti? | |
| Come vengono usati, archiviati e cancellati i supporti magnetici? | |
| Gli incaricati hanno ricevuto specifiche istruzioni, in merito alle modalità di cancellazione o distruzione di supporti, prima del riutilizzo? | |

| Domande | Risposta (di base SI/NO) |
|---|---|
| Gli incaricati hanno a disposizione e possono agevolmente utilizzare distruggitori di documenti? | |
| Prima di riutilizzare un qualsiasi supporto magnetico, contenente dati sensibili, si provvede sempre alla sua cancellazione? | |
| Prima di riutilizzare un qualsiasi supporto cartaceo, contenente dati sensibili, si provvede sempre alla sua cancellazione o meglio, alla sua distruzione? | |
| Come vengono usati, archiviati e cancellati i supporti cartacei? | |
| L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato? | |
| Le persone ammesse all'accesso di archivi contenenti dati sensibili o giudiziari, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate? | |
| Quando gli archivi contenenti dati sensibili o giudiziari non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate? | |

| **Formazione** | |
|---|---|
| I neo assunti vengono debitamente istruiti prima di iniziare a svolgere attività di trattamento di dati personali? | |
| Come viene valutato il livello di integrità ed affidabilità dei dipendenti, prima di affidare loro attività che comportino l'accesso a dati personali? | |
| Gli incaricati ricevono regolarmente aggiornamenti operativi in tema di sicurezza? | |
| Sono state distribuite delle linee guida di sicurezza a tutti gli incaricati? | |
| Esiste una documentazione di supporto e convalida della attività di formazione? | |