

QUESTIONARIO RESPONSABILI DEL TRATTAMENTO

Il sottoscritto _____, nato a _____ il _____, in qualità di legale rappresentante della Società _____, con sede legale in _____ (C.F./P.IVA _____), consapevole delle responsabilità civili e penali in caso di dichiarazioni mendaci, dichiara ai sensi degli artt. 46 e 47 del D.P.R. 28 dicembre 2000, n. 445, che la Società dispone delle misure minime di carattere organizzativo e di sicurezza di cui agli artt. 25 e 32 del Regolamento (UE) 2016/679 (GDPR), come di seguito indicate.

Laddove la misura non sia presente o non sia applicabile il fornitore è tenuto a indicare nelle note la motivazione e/o l'indicazione circa il fatto che tale misura sarà applicabile.

MISURE TECNICHE ED ORGANIZZATIVE		SI	NO	NON APPLICABILE	NOTE
1.1.	Adozione di una Politica aziendale in materia di protezione dei dati personali che garantisca e documenti la conformità a tutti i requisiti legali e normativi applicabili all'attività svolta				
1.2.	Nomina del Responsabile della protezione dei dati (DPO) / di una funzione interna deputata alla gestione degli adempimenti privacy. Nome: Numero di telefono: Indirizzo e-mail:				
1.3.	Definizione di un organigramma privacy aziendale				
1.4.	Autorizzazione al trattamento e formazione del personale che accede ai dati oggetto del trattamento.				
1.5.	Redazione del Registro dei trattamenti ex art. 30.2 GDPR.				
1.6.	Adozione di una procedura/una prassi operativa per la gestione delle richieste degli Interessati				
1.7.	Adozione di una procedura/una prassi operativa per la gestione di eventuali data breach				
1.8.	Adozione di un regolamento/una procedura/una policy sulla gestione e sull'utilizzo dei dispositivi IT				
1.9.	Implementazione di un catalogo di asset contenente la descrizione complessiva della propria architettura tecnologica				

1.10.	Adozione di misure di sicurezza ritenute adeguate in relazione alla tipologia di dati personali trattati (livello di rischio definito sulla base della tipologia di dati, categorie di interessati, numerosità degli interessati)				
Trattamento attraverso mezzi cartacei		SI	NO	NON APPLICABILE	NOTE
2.1.	Il personale incaricato al trattamento dal Responsabile è obbligato a non lasciare mai incustoditi e accessibili i documenti contenenti i dati personali trattati per conto del Titolare durante e dopo l'orario di lavoro				
2.2.	Sono individuati profili di autorizzazione differenziati per ciascun incaricato e/o per classi omogenee di incaricati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento di competenza di ciascuno				
2.3.	Sono chiaramente identificati e comunicati agli incaricati gli archivi in cui riporre i documenti contenenti i dati personali (armadi, stanze, casseforti, ecc.).				
2.4.	La conservazione dei documenti contenenti dati personali di categorie particolari e dati giudiziari trattati sotto la titolarità dell'ASL avviene in luoghi separati e distinti da quelli di archiviazione dei documenti contenenti dati personali comuni.				
2.5.	La conservazione dei documenti contenenti dati personali di categorie particolari e dati giudiziari trattati sotto la titolarità dell'ASL avviene in luoghi separati e distinti da quelli di archiviazione dei documenti contenenti dati personali comuni.				
Trattamento attraverso mezzi informatici		SI	NO	NON APPLICABILE	NOTE
3.1.	Sono presenti password personali/username/misure di protezione all'accesso dei sistemi con cui sono trattati i dati personali di cui l'ASL è Titolare.				
3.2.	Adozione di una procedura di autorizzazione che regoli in maniera differenziata l'accesso degli Incaricati ai dati personali di cui l'ASL è Titolare.				

3.3.	Adozione di meccanismi idonei ad evitare l'uso di password deboli da parte degli utenti.				
3.4.	Adozione di un meccanismo idoneo ad escludere l'assegnazione di un'utenza ad un incaricato diverso da quello originario.				
3.5.	Adozione di una procedura atta a garantire la sospensione delle utenze non utilizzate per oltre sei mesi.				
3.6.	Adozione di una procedura atta a garantire la pronta cancellazione delle utenze relative ad incaricati che hanno cambiato o lasciato la propria mansione.				
3.7.	Per l'amministrazione dei sistemi attivazione di un account ADMIN indipendente che differisce dall'account utente individuale ed effettivo dell'amministratore di sistema.				
3.8.	Previsione di un limite di tentativi di accesso con un nome utente / password in caso di errore.				
3.9.	Previsione di un blocco automatico dello schermo protetto da password.				
3.10.	Verifica periodica della validità delle autorizzazioni di accesso.				
3.11.	Posizionamento della sala in cui è ubicato il server/data center in luoghi adeguatamente protetti.				
3.12.	Adozione di misure di protezione dei sistemi IT dalla perdita dei dati/dall'accesso ai dati non autorizzato (es. virus, firewall, ecc.).				
3.13.	Adozione di misure di sicurezza adeguate sulla posta elettronica (es. autenticazione a doppio fattore o password forti, antimalware, antiphishing, protocolli cifrati etc.)				
Conservazione		SI	NO	NON APPLICABILE	NOTE
4.1.	Adozione di una politica formale e automatica per l'esecuzione almeno giornaliera di backup.				
4.2.	Duplicazione dei dati di backup in sedi separate e distanti almeno 10 km in linea d'aria.				
4.3.	Controlli regolari della funzionalità del ripristino da backup è controllata regolarmente.				

4.4.	Adeguate procedure di smaltimento dei supporti dati non più necessari (chiavette USB, dischi fissi) su cui sono memorizzati i dati personali di cui l'ASL è Titolare.				
Pseudonimizzazione e Cifratura		SI	NO	NON APPLICABILE	NOTE
5.1.	I dati personali sono trattati in modo pseudonimizzato/criptato. Indicazione delle tecniche utilizzate:				
Utilizzo di sistemi di intelligenza artificiale		SI	NO	NON APPLICABILE	NOTE
6.1.	In caso di utilizzo di sistemi di intelligenza artificiale specificare nelle note le logiche di funzionamento dei sistemi di I.A. utilizzati/sviluppati/forniti, le potenzialità, sull'autonomia e sui limiti degli stessi				
6.2.	Specificare nelle note in che modo il sistema di intelligenza artificiale consenta un'effettiva supervisione umana sul funzionamento				

Data e luogo

Firma del Responsabile
