ALLEGATO 2 – Misure di Sicurezza

Il RESPONSABILE garantisce di avere adottato le seguenti misure di sicurezza a protezione dei trattamenti effettuati per conto del TITOLARE.

ID	MISURE DI SICUREZZA
1	**Procedura di autenticazione e credenziali di autenticazione**
1.1	L'accesso ai sistemi utilizzati per il trattamento di dati personali è consentito al solo personale autorizzato al trattamento dotato di credenziali di autenticazione univoche che consentano la loro autenticazione.
1.2	Le credenziali di autenticazione consistono in un codice per l'identificazione della Persona Autorizzata associato a una parola chiave riservata conosciuta solamente dal medesimo, oppure in un dispositivo di autenticazione in possesso e uso esclusivo del personale autorizzato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica del soggetto autorizzato, eventualmente associata a un codice identificativo o a una parola chiave.
1.3	Ad ogni Persona Autorizzata sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
2	**Regole di creazione, gestione e disattivazione dei codici identificativi**
2.1	Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altre Persone Autorizzate, neppure in tempi diversi.
2.2	Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica, e le credenziali sono disattivate anche in caso di perdita della qualità che consente alla Persona Autorizzata l'accesso ai dati personali.
3	**Regole di creazione e sostituzione delle password di autenticazione**
3.1	La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito e siano adottate delle regole per garantirne la complessità.
3.2	Con le istruzioni impartite alle Persone Autorizzate è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo della Persona Autorizzata.
4	**Sistemi di autorizzazione – profili di autorizzazione**
4.1	I poteri di accesso ai dati personali attribuiti alle Persone Autorizzate sono attribuiti in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
4.2	Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
5	**Altre misure di sicurezza**
5.1	I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici aggiornati tempestivamente.
5.2	Gli aggiornamenti periodici dei programmi per elaboratore (ad esempio Sistemi operativi) volti a prevenire la vulnerabilità di tali strumenti e a correggerne difetti sono effettuati periodicamente e comunque almeno semestralmente.
5.3	I dati personali sono sottoposti a back-up giornalieri idonei a garantire la conservazione sicura dei dati e il loro ripristino in un tempo massimo di 7 giorni.
5.4	Sono installati sistemi di protezione adeguati contro le minacce logiche/software pericolosi (es. antivirus, anti-malware, anti-spam, ecc.)
5.5	La rete aziendale è protetta da sistemi anti-intrusione o comunque idonea a combattere gli attacchi informatici (es. firewall, filtraggio, Intrusion Prevention System, Intrusion Detection System, etc.). L'infrastruttura utilizzata, quale Amazon Web Services, per l'erogazione dei servizi software Ydea, gode di livelli di sicurezza e certificazioni ottenute da Amazon Web Services, consultabili al seguente link: https://aws.amazon.com/it/compliance/gdpr-center/

5.6	È vietato il trattamento su supporti removibili di dati personali effettuato per conto del TITOLARE fatta salva l'adozione di adeguate misure di sicurezza (quali la cifratura) che non consentano a terzi non autorizzati l'accesso a tali dati in caso di furto o smarrimento del supporto rimovibile.
6	**Trattamento senza l'ausilio di strumenti elettronici**
6.1	Sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali
6.2	Quando gli atti e i documenti contenenti categorie particolari di dati o dati giudiziari sono affidati a Persone Autorizzate al trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dalle Persone Autorizzate fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
6.3	L'accesso agli archivi contenenti categorie particolari di dati o dati giudiziari è controllato. Le persone ammesse, a qualunque titolo, sono identificate e registrate. Quando gli archivi non siano dotati di strumenti elettronici per il controllo degli accessi o di autorizzati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Per conto del RESPONSABILE
Nome e Cognome: Paolo Colleluori
Qualifica/potere di firma: Rappresentante Legale
Luogo e data: Rimini, 28/02/2025

Firma: _____