NOMINA NELL'AMBITO DEL TRATTAMENTO E DELLA PROTEZIONE DEI DATI PERSONALI DI AMMINISTRATORE DI SISTEMA, AI SENSI DELL'ARTICOLO 28 DEL REGOLAMENTO UE 679/2016 E DEL PROVVEDIMENTO DEL GARANTE ITALIANO PER LA PROTEZIONE DEI DATI "MISURE E ACCORGIMENTI PRESCRITTI AI TITOLARI DEI TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI RELATIVAMENTE ALLE ATTRIBUZIONI DEL AMMINISTRATORE DI SISTEMA - 27 NOVEMBRE 2008 (G.U. N. 300 DEL 24 DICEMBRE 2008)"

Il sottoscritto Eliseo Micci, in qualità di Legale Rappresentante di ERGA TAPES srl, Titolare del trattamento, conformemente a quanto sopra riportato, nomina, con il presente accordo contrattuale, il Sig. Angelo Rossi della INFOCOM GROUP S.R.L. P.IVA - C.F. 02453470342 C.so Garibaldi, 127 - 29017 Fiorenzuola d'Arda - PC **AMMINISTRATORE DI SISTEMA di ERGA TAPES srl**.

COMPITI E RESPONSABILITÀ DELL'AMMINISTRATORE DI SISTEMA

All'Amministratore di Sistema vengono attribuiti i seguenti compiti:

- Assicurare la progettazione e la messa in funzione delle soluzioni tecniche per garantire e gestire le misure minime di sicurezza richieste dal Regolamento UE 679/2016
- Collaborare nella predisposizione ed aggiornamento delle "best practice" relative alla gestione della sicurezza informatica e alla gestione degli accessi ai dati
- Collaborare nelle predisposizione ed aggiornamento del documento "Politiche di Protezione Dati e Codice di Condotta", se richiesto dal Titolare
- Definire le modalità di accesso al sistema ed alle differenti risorse di rete (locale o remota), nonché ai locali ove siano custodite le macchine e gli elaboratori centrali
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di hackers) e di furto dati (Data Breach)
- Assicurare la protezione dal rischio di virus mediante idonei programmi, garantendone l'efficacia e verificando la definizione dei virus stessi nel tempo
- Garantire sempre il costante aggiornamento degli applicativi utilizzati per la gestione dei dati e dell'operatività interna
- Assicurare la gestione degli aggiornamenti sistematici del software installato (gestione delle patch)
- Garantire, qualora alcune soluzioni tecniche per le misure minime di sicurezza fossero demandate a soggetti esterni alla Società, la verifica della loro conformità alle policy interne e la ricezione da parte del fornitore esterno della descrizione scritta dell'intervento effettuato
- Garantire che, per ciascuna persona autorizzata al trattamento da parte del Titolare, sia predisposto il Codice identificativo personale (USER-ID) e che esso sia consegnato unitamente alla prima Password per l'accesso alle banche dati abilitate ad ognuno
- Gestire e monitorare l'utilizzo degli USER-ID in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consenta l'accesso all'elaboratore o qualora gli stessi non vengano utilizzati per un periodo superiore a 6 mesi
- Garantire la modifica delle Password secondo quanto stabilito dalla Policy interna e definita nel documento "Politiche di Protezione Dati e Codice di Condotta" o documentazione equivalente e provvedere a disattivare le password inutilizzate per più di 60 giorni
- Provvedere a sostituire o revocare, in caso di necessità o secondo quanto stabilito dalla policy del Titolare o documentazione equivalente, le Password che per motivi diversi possano rendere adito a ragionevole dubbio sul loro utilizzo
- Revocare tempestivamente tutte le password assegnate a soggetti che, su comunicazione del Titolare o del Responsabile del Trattamento, non sono più autorizzati ad accedere ai dati
- Accertarsi che gli incaricati utilizzino le Password con diligenza
- Controllare periodicamente l'esecuzione delle copie di backup dell'archivio dati ed accertarsi che tali copie siano di qualità e vengano conservate in luogo adatto e sicuro
- Coadiuvare il Titolare del Trattamento nell'attuazione di tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e garantire il ripristino degli stessi entro 72 ore, con la possibilità di delegare ad altra persona tale attività solo ed esclusivamente in caso di assenza forzata
- Garantire al Titolare la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici attraverso l'adozione di sistemi idonei. Tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi

L'Amministratore di Sistema dichiara di:

- Essere a conoscenza di quanto stabilito dal Regolamento UE 679/2016 e dal Provvedimento del Garante Italiano per la protezione dei dati "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni del amministratore di sistema - 27 novembre 2008(G.U. n. 300 del 24 dicembre 2008)"
- Garantire l'idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza
- Possedere l'esperienza, le qualità tecniche, professionali e di condotta, ovvero le competenze minime necessarie allo svolgimento del suddetto incarico
- Di essere stato formato/informato adeguatamente sull'utilizzo dei sistemi informatici di ERGA TAPES srl
- Di mettersi a completa disposizione del Titolare per le attività di verifica, con cadenza almeno annuale, previste dalla Legge col fine di controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati

Sesto San Giovanni, lì _____ Per accettazione (timbro e firma)

Per il Titolare del trattamento _____