

## Misure tecniche ed organizzative adottate per l'erogazione dei Servizi di Assistenza

La Pegaso Informatica Snc riconosce l'importanza della protezione dei dati personali dei clienti e si impegna a rispettare le disposizioni del Regolamento UE 2016/679 (GDPR) per garantire la privacy e la sicurezza dei dati personali nel corso dell'attività di assistenza sistemistica e sui software applicativi, adottando le seguenti misure tecniche ed organizzative:

| AREA                                                                                     | MISURA                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1. Pianificazione della sicurezza dei dati</b>                                        | <ul style="list-style-type: none"> <li>Definizione di una politica di sicurezza dei dati che identifica i rischi associati al trattamento dei dati personali e relative procedure per gestirli</li> <li>Revisione e aggiornamento periodico della politica di sicurezza dei dati per assicurare la conformità alle migliori pratiche e agli standard di sicurezza</li> </ul>                            |
| <b>2. Ruoli e responsabilità</b>                                                         | <ul style="list-style-type: none"> <li>Designazione di una figura interna all'organizzazione aziendale che monitora e garantisce la conformità alle misure di sicurezza dei dati</li> <li>Assegnazione di specifiche responsabilità all'interno dell'azienda per la gestione e la protezione dei dati personali</li> </ul>                                                                              |
| <b>3. Formazione del personale</b>                                                       | <ul style="list-style-type: none"> <li>Formazione periodica del personale coinvolto nell'erogazione del servizio di assistenza sul software applicativo, sensibilizzandolo riguardo alla sicurezza dei dati personali e alle buone pratiche di trattamento</li> <li>Mantenimento di un registro della formazione fornita e delle attività di sensibilizzazione svolte</li> </ul>                        |
| <b>4. Gestione degli accessi</b>                                                         | <ul style="list-style-type: none"> <li>Limitazione dell'accesso ai dati personali solo al personale autorizzato, assegnando privilegi di accesso basati sul principio di necessità</li> <li>Utilizzo di meccanismi di autenticazione forte, come password complesse e autenticazione a due fattori, per garantire la protezione degli account e dei sistemi</li> </ul>                                  |
| <b>5. Crittografia dei dati</b>                                                          | <ul style="list-style-type: none"> <li>Se del caso crittografia dei dati personali in transito e a riposo per prevenire l'accesso non autorizzato</li> <li>Adozione di algoritmi di crittografia robusti e gestione adeguata delle chiavi di crittografia per garantire l'integrità e la riservatezza dei dati</li> </ul>                                                                               |
| <b>6. Gestione degli incidenti</b>                                                       | <ul style="list-style-type: none"> <li>Adozione di un processo di gestione degli incidenti che prevede la notifica tempestiva delle violazioni dei dati personali alle autorità competenti e, se necessario, agli interessati coinvolti</li> <li>Mantenimento di un registro delle violazioni dei dati e delle eventuali misure correttive adottate</li> </ul>                                          |
| <b>7. Backup e ripristino dei dati</b>                                                   | <ul style="list-style-type: none"> <li>Adozione di procedure di backup regolari e sicure per garantire l'integrità e la disponibilità dei dati personali</li> <li>Test periodico di ripristino dei dati per verificare l'efficacia delle procedure di backup</li> </ul>                                                                                                                                 |
| <b>8. Analisi dei rischi e Valutazione dell'impatto sulla protezione dei dati (DPIA)</b> | <ul style="list-style-type: none"> <li>Conduzione dell'analisi dei rischi per identificare i rischi per la privacy associati al Trattamento dei dati personali nell'erogazione del servizio di assistenza sul software applicativo e se del caso Valutazione dell'Impatto sulla Protezione dei Dati (DPIA)</li> <li>Conseguente adozione delle misure di mitigazione dei rischi identificati</li> </ul> |
| <b>9. Contratti con terze parti</b>                                                      | <ul style="list-style-type: none"> <li>Stipula di contratti che definiscono chiaramente le responsabilità delle parti, in relazione alla protezione dei dati personali con le terze parti eventualmente coinvolte nell'erogazione del servizio di assistenza sul software applicativo</li> <li>Verifica di garanzie sufficienti da parte delle terze parti riguardo alla conformità al GDPR</li> </ul>  |
| <b>10. Monitoraggio e audit</b>                                                          | <ul style="list-style-type: none"> <li>Monitoraggio regolare dell'efficacia delle misure di sicurezza dei dati adottate</li> <li>Effettuazione di audit interni o esterni per valutare la conformità e l'efficacia delle nostre politiche e procedure di sicurezza dei dati</li> </ul>                                                                                                                  |

**11. Amministratori di Sistema**

Attribuzione individuale dell'incarico di Amministratore di sistema al proprio personale che possiede un livello adeguato di esperienza, competenza e affidabilità per garantire il pieno rispetto delle norme relative al trattamento dei dati, compreso il profilo relativo alla sicurezza con indicazione specifica degli ambiti operativi consentiti in base al loro profilo di autorizzazione