San Martino di Lupari, li 19 ottobre 2021

**Oggetto: Questionario di valutazione del Responsabile ex art. 28 e 32 GDPR 2016/679.**

In qualità di nostro Responsabile del trattamento, Vi invitiamo a procedere alla compilazione e alla successiva trasmissione del seguente questionario per la valutazione nonché l’autovalutazione della compliance alla vigente normativa in materia di protezione dei dati personali, ai sensi dell’art. 28 GDPR 2016/679 e dell’art. 32 GDPR 2016/679.

In alternativa e/o in aggiunta alla compilazione del presente questionario, è sempre possibile inviare alla Scrivente diversa documentazione attestante la propria compliance privacy (es. Procedura Valutazione Fornitori ISO 9001/27001, o ulteriore materiale messo a disposizione anche mediante il sito web).

Il questionario è compilato in data \_\_/\_\_/\_\_ dal Sig./Sig.ra \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

per conto dell’Azienda/dello Studio/Ente \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Si ricorda che per la corretta compilazione dovrà essere inserita una spunta in ciascuna delle voci, a seconda dello stato di implementazione della misura, evidenziando che è altresì richiesto, a titolo di trasparenza, riportare nelle note una breve descrizione delle valutazioni preventive adottate, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l’applicazione del regolamento.

**1. Viene redatto e periodicamente revisionato ed aggiornato il Registro dei Trattamenti del Titolare e siete in grado di comprovarlo.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**2. Viene redatto e periodicamente revisionato ed aggiornato il Registro dei Trattamenti del Responsabile e siete in grado di comprovarlo.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**3. Il Responsabile ha nominato un responsabile della protezione dei dati (DPO/RPD).**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti/Se presente DPO/RPD fornire dati identificativi e di contatto: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**4. Sono fornite agli interessati informative sul trattamento dei dati personali e raccolti, ove necessario, i consensi.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**5. Ove si sia provveduto a raccogliere i consensi, se ne tiene traccia mediante una specifica procedura e siete in grado di comprovarlo.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**6. Esistono specifiche procedure per comunicare al Titolare del Trattamento la richiesta di esercizio dei diritti da parte dell’Interessato.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**7. È stata redatta una valutazione rischi sui trattamenti dei dati, periodicamente revisionata ed aggiornata e siete in grado di comprovarlo. In base a tale valutazione, vengono poste in essere eventuali azioni di miglioramento e/o volte a ridurre i rischi rilevati.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**8. Esiste una procedura da seguire in caso di "data breach" (violazioni sui dati personali), che comprenda la segnalazione di tali violazioni al Titolare del Trattamento.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**9. Esiste una procedura per smaltire regolarmente e in sicurezza i dati personali non più necessari in base ai tempi di conservazione fissati.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**10. Sono stati regolati i rapporti con i propri Responsabili (es. Commercialista, Consulente del Lavoro, Enti di certificazione, Consulente Informatico, Software House del gestionale aziendale, ecc.) mediante Data Processing Agreement, clausola contrattuale o diverso atto giuridico e siete in grado di comprovarlo.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**11. I propri Responsabili vengono periodicamente valutati sotto il profilo della compliance alla normativa vigente sulla protezione dei dati personali nonché della sicurezza delle informazioni e siete in grado di comprovarlo.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**12. I dipendenti e collaboratori che trattano dati personali sono stati istruiti in relazione ai trattamenti stessi, con l'indicazione dei trattamenti loro consentiti e dei dati a cui hanno accesso e siete in grado di comprovarlo.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**13. I dipendenti e collaboratori hanno ricevuto adeguata formazione sulla protezione dei dati personali e la sicurezza delle informazioni e siete in grado di comprovarlo.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**14. Si dispone di controlli per limitare l'accesso ai locali e alle attrezzature al fine di prevenire accessi fisici non autorizzati nonché la perdita, il danneggiamento, il furto o la compromissione dei dati personali.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**15. Si dispone di modalità di archiviazione sicura per proteggere i record cartacei e informatici al fine di prevenire la perdita, il danneggiamento, il furto o la compromissione dei dati personali e siete in grado di comprovarlo.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**16. È stato adottato e correttamente configurato un sistema di autenticazione (accesso ai PC mediante utente e password) e di autorizzazione (accesso alle condivisioni di rete selezionato per utente o gruppo) che consente la profilazione dei singoli addetti al trattamento all’accesso al Sistema Informativo.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**17. Viene garantita la sicurezza del lavoro mobile e l'utilizzo dei dispositivi di elaborazione mobile.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**18. I singoli componenti, hardware e software, sono protetti da adeguato software antivirus e da un sistema di sicurezza informatica perimetrale (Firewall) opportunamente configurato ed aggiornato.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**19. È stato adottato un sistema per la gestione delle copie di riserva dei dati (backup) che consente il ripristino dei dati in tempi rapidi e siete in grado di comprovarlo.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**20. I dati trattati sono soggetti a trasferimento al di fuori dello Spazio Economico Europeo. SI NO**

**In particolare verso il seguente Paese Terzo** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Per tali trasferimenti dei dati extra SEE, è implementato uno degli strumenti di cui agli artt. 44 ss. per assicurare che il livello di protezione delle persone fisiche non sia pregiudicato.**

|  |  |  |
| --- | --- | --- |
|  | Non ancora implementato o pianificato | Note/Commenti/Indicare quale strumento è implementato: |
|  | Parzialmente implementato o pianificato |
|  | Implementato |
|  | Non applicabile |

**21.Si indicano i Responsabili che intervengono nei trattamenti svolti per conto del Titolare del Trattamento.**

|  |  |  |
| --- | --- | --- |
|  | Non applicabile (nessun Responsabile interviene nei trattamenti svolti per conto del Titolare del Trattamento) | Es. Nome Cognome - Commercialista / ACME SRL, Consulente Privacy |
|  | |

**22. Si indicano le persone fisiche che svolgono interventi tipici da Amministratori di Sistema nei sistemi del Titolare del Trattamento.**

|  |  |  |
| --- | --- | --- |
|  | Non applicabile (non sono forniti servizi IT di alcun tipo) | Es. Nome Cognome - Backup Manager |
|  | |

Con la sottoscrizione del presente questionario, il Responsabile del Trattamento:

* Si assume la piena responsabilità della veridicità e dell’accuratezza delle proprie dichiarazioni;
* Prende atto che, con riferimento ai singoli punti ai quali è stata fornita risposta negativa o parzialmente negativa (“Non ancora implementato o pianificato”, “Parzialmente implementato o pianificato”), si configura una totale o parziale violazione della normativa vigente in materia di protezione dei dati personali e **s’impegna pertanto a procedere quanto prima alla messa in conformità, previo accordo con il Titolare del Trattamento e successiva nuova valutazione**, o in alternativa a fornire informazioni integrative o adeguate motivazioni alla Scrivente;
* Prende atto che, anche sulla base dei riscontri al presente questionario e/o di evidenze diverse e ulteriori, il Titolare del Trattamento procede alle necessarie valutazioni ai sensi dell’art. 28 par. 1 e par 3 let. h) del GDPR 2016/679 e **si riserva di adottare gli opportuni provvedimenti qualora le non conformità rilevate costituiscano violazione della normativa vigente in materia di protezione dati, incluso il recesso contrattuale per giusta causa**.

|  |  |
| --- | --- |
| Per il Titolare del Trattamento | Per il Responsabile del Trattamento |
| *MICHELAZZO GIORGIO* |  |