**ATTO DI DESIGNAZIONE A RESPONSABILE DEL TRATTAMENTO**

TRA

L’Ente\_\_\_\_\_\_\_\_\_\_, con sede legale in \_\_\_\_\_\_\_\_\_, codice fiscale e partita I.V.A. \_\_\_\_\_\_\_\_\_\_\_\_\_, in persona \_\_\_\_\_\_\_\_\_\_\_\_\_, nato a \_\_\_ il \_\_\_\_\_, codice fiscale \_\_\_\_\_\_, munito dei necessari poteri per il compimento del presente atto, in qualità di Titolare del trattamento

E

“INSIEL – Informatica per il Sistema degli Enti Locali S.p.A.” con unico socio, Direzione e coordinamento Regione Autonoma Friuli Venezia Giulia, con sede legale in Trieste, Via San Francesco d’Assisi numero 43, iscritta al Registro delle Società di Trieste, numero di iscrizione, codice fiscale e partita I.V.A. 00118410323, e al R.E.A. di Trieste al n. 71598, in persona dell’Amministratore Unico, dott. Diego Antonini, nato a Trieste il 14/04/1962, codice fiscale NTNDGI 62D14L424U, giusta Delibera dell’Assemblea dei Soci di data 31/05/2022, munito dei necessari poteri per il compimento del presente atto, in qualità di Responsabile del trattamento

**Premesso che:**

1. l’Ente \_\_\_\_\_\_\_\_\_\_\_ e Insiel sono qualificati nel prosieguo anche, rispettivamente, quali Titolare e Responsabile;
2. Insiel è affidataria *in house* delle attività di sviluppo e gestione del Sistema Informativo Integrato Regionale (S.I.I.R.) e delle infrastrutture di telecomunicazione della Regione Autonoma Friuli Venezia Giulia ai sensi della legge regionale 14 luglio 2011, n. 9 (Disciplina del sistema informativo integrato regionale del Friuli Venezia Giulia) e svolge tali servizi in base ad un disciplinare di servizio, relativo ai servizi di sviluppo e gestione del SIIR e delle infrastrutture di telecomunicazione (di seguito “Disciplinare”), approvato con delibera di giunta regionale e di durata novennale ai sensi dell’art. 9 della succitata l.r. ed è controllata dalla medesima Regione Autonoma Friuli Venezia Giulia per il 100% del Capitale Sociale;
3. il S.I.I.R., ai sensi dell’art. 4, commi 1 e 5, della l.r. 9/2011, è costituito dai sistemi informativi, telematici e tecnologici di soggetti diversi e comprende il complesso delle basi di dati, dei servizi, delle procedure e dei servizi applicativi, nonché delle reti trasmissive dei suddetti soggetti ed è articolato in ragione dei settori di competenza dei singoli soggetti, per le funzioni amministrative, gestionali e tecniche dei dati e dei servizi;
4. i servizi messi a disposizione dalla Regione Autonoma Friuli Venezia Giulia per il tramite di Insiel sono disciplinati da un Protocollo d’Intesa fra Regione ed Ente per la prestazione di servizi forniti nell’ambito del Sistema Informativo Integrato Regionale (S.I.I.R.).
5. lo svolgimento dei suddetti servizi comporta il trattamento, da parte di Insiel per conto dell’Ente, dei dati personali di interessati di cui l’Ente stesso è Titolare (di seguito, “Dati Personali”);
6. Insiel dichiara di possedere esperienza, competenze tecniche e risorse che le consentono di mettere in atto misure tecniche e organizzative adeguate, atte a garantire la conformità alla normativa in materia di tutela dei dati personali e la tutela degli interessati;
7. Insiel ha conseguito la certificazione ISO/IEC 27001 e le relative estensioni ISO/IEC 27017 e ISO/IEC 27018, qualificandosi Cloud Service Provider per la Pubblica Amministrazione;
8. con il presente atto l’Ente, in qualità di Titolare del trattamento, intende nominare Insiel Responsabile del trattamento ai sensi di quanto disposto dall’art. 28 del Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - Regolamento Generale sulla Protezione dei Dati Personali (di seguito, “RGDP” o “Regolamento”);
9. il presente contratto di affidamento include il contenuto minimo richiesto dall’art. 28 del RGDP.

Tutto ciò premesso e costituendo le premesse parte integrante e sostanziale del presente atto contrattuale), fra le Parti si conviene e si stipula quanto segue:

1. **OGGETTO**

A Insiel, per mezzo del suo legale rappresentante pro tempore, che sottoscrive il presente atto, è affidato l’incarico di Responsabile del trattamento dei Dati Personali connesso all’erogazione dei servizi oggetto del Protocollo d’intesa stipulato tra la Regione Autonoma Friuli Venezia Giulia ed il Titolare.

I servizi comprendono:

* + la connessione dell’Ente alla Rete Unitaria della Pubblica Amministrazione Regionale (RUPAR);
  + l’utilizzo da parte dell’Ente dei prodotti e dei servizi informatici previsti dal S.I.I.R. ed elencati nel documento “Repertorio”, allegato sub “A” al Protocollo di Intesa;
  + l’utilizzo da parte dell’Ente dei prodotti e dei servizi di pubblicazione ed interscambio, dei dati di natura cartografica, territoriale ed ambientale previsti nel documento “Servizi IRDAT fvg”, allegato sub “B” al Protocollo di Intesa.

Le categorie di interessati sono: utenti dei servizi, dipendenti e collaboratori dell’Ente, cittadini.

Le categorie di dati personali trattati sono dati comuni (dati anagrafici, indirizzi IP, indirizzi e-mail) e dati particolari ai sensi dell’art. 9 del RGDP (Dati Personali).

1. **OBBLIGHI DEL RESPONSABILE**

Il Responsabile è tenuto a trattare i Dati Personali solo ed esclusivamente ai fini dell’esecuzione dei servizi di cui all’articolo 1, nel rispetto di quanto disposto dalla normativa applicabile in materia di protezione dei dati personali, nonché dalle istruzioni del Titolare riportate nei successivi articoli e di ogni altra indicazione scritta che potrà essergli dallo stesso fornita.

1. **MISURE DI SICUREZZA**

Il Responsabile assiste il Titolare nell’adozione delle misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell’arte, dei costi di attuazione, della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Le principali misure di sicurezza adottate sono:

1. Misure di identificazione e autorizzazione dell'utente (autenticazione a più fattori);
2. Misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento

Ai fini di assicurare i requisiti di riservatezza, integrità e disponibilità delle informazioni è previsto il mantenimento di un vero e proprio Sistema di Gestione per la Sicurezza delle Informazioni, fondato sui dettami dello standard internazionale ISO 27001.

Il sistema di gestione per la sicurezza delle informazioni preserva la riservatezza, l'integrità e la disponibilità delle informazioni mediante l'applicazione di un processo di gestione del rischio e dà fiducia alle parti interessate sull'adeguatezza della gestione dei rischi, comprendendo un insieme di azioni strutturate aventi impatto sulla dimensione fisica, logica ed organizzativa.

1. Misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico

Ai fini di assicurare la continuità operativa è previsto il mantenimento di un vero e proprio Sistema di Gestione della Continuità operativa (o BCMS – Business Continuity Management System), fondato sui dettami dello standard internazionale ISO22301.

Lo standard definisce i requisiti per attuare, mantenere e migliorare un sistema di gestione per proteggere l'organizzazione, ridurre la probabilità che si verifichino interruzioni, prepararsi, rispondere e riprendersi dalle interruzioni quando si verificano, cioè un efficace sistema di gestione per la continuità operativa.

1. Procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Secondo quanto previsto dallo standard internazionale ISO27001, è previsto che siano condotti, ad intervalli pianificati, audit interni per fornire informazioni tali da permettere di riconoscere se il sistema di gestione per la sicurezza delle informazioni è conforme allo standard di riferimento adottato.

È previsto altresì il riesame, a intervalli pianificati, del sistema di gestione per la sicurezza delle informazioni dell'organizzazione, per assicurarne la continua idoneità, adeguatezza ed efficacia.

1. Misure di protezione dei dati durante la trasmissione

È previsto che le reti siano gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni. Nelle reti vengono previste delle configurazioni atte a segregare gruppi di servizi, di utenti e di sistemi informativi, secondo i requisiti previsti.

Le informazioni trasmesse attraverso la posta elettronica vengono protette in modo appropriato attraverso l’adozione di specifici sistemi di protezione da minacce informatiche.

1. Misure di protezione dei dati durante la conservazione

Sono previste copie di backup delle informazioni, del software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata, secondo i requisiti specifici previsti.

1. Misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati

Sono previsti dei parametri di sicurezza per proteggere le aree che contengono informazioni critiche e le strutture di elaborazione delle informazioni.

Le aree di sicurezza vengono protette da appropriati controlli per l'ingresso atti ad assicurare che solo il personale autorizzato abbia il permesso di accedervi.

Viene progettata e applicata la sicurezza fisica agli uffici, ai locali ed agli impianti.

Le apparecchiature vengono disposte e protette al fine di ridurre i rischi derivanti dalle minacce e dai pericoli ambientali, oltre alle occasioni di accesso non autorizzato.

1. Misure per garantire la registrazione degli eventi

Gli eventi di accesso ai sistemi da parte degli Amministratori di Sistema vengono gestiti secondo quanto previsto dal Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”.

Le applicazioni implementano i requisiti di registrazione degli eventi. Gli apparati ed i sistemi registrano gli eventi conformemente con le necessità operative.

1. Misure di certificazione/garanzia di processi e prodotti

Tale misura si applica con il perseguimento del mantenimento di specifiche certificazioni che siano pertinenti con il contesto di elaborazione delle informazioni, dei processi di gestione e delle attività del Responsabile. A titolo esemplificativo, si possono citare le certificazioni ISO9001, ISO20000, ISO27001, ISO22301.

1. Misure per garantire la minimizzazione dei dati

Nella realizzazione delle attività concordate, si darà indicazione di prediligere il trattamento della minima quantità di dati e informazioni necessarie allo svolgimento delle specifiche attività previste.

1. Pseudonimizzazione e cifratura dei Dati Personali.
2. **VIOLAZIONI DI DATI PERSONALI (C.D. “DATA BREACH”)**

Il Responsabile si impegna a informare il Titolare, senza ingiustificato ritardo (inviando una comunicazione a mezzo PEC all’indirizzo \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ) di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai Dati Personali trasmessi, conservati o comunque trattati, fornendo almeno le informazioni minime citate nelle Linee Guida del Gruppo di Lavoro ex articolo 29 “Guidelines on Personal data breach notification under Regulation 2016/679”, adottate e riviste il 6 febbraio 2018, così come descritte nella parte II, lettera B, paragrafo 1.

In caso si rilevi la necessità di notifica della violazione all’autorità di controllo o agli interessati, il Responsabile si impegna a collaborare con il Titolare ai fini della notifica della violazione entro i tempi massimi stabiliti dal RGDP ed a prestare ogni necessaria collaborazione al Titolare ad ogni altro adempimento degli obblighi sullo stesso gravanti, di notifica delle suddette violazioni all’Autorità ai sensi dell’art. 33 del RGDP o di comunicazione della stessa agli interessati ai sensi dell’art. 34 del RGDP.

1. **VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI**

Il Responsabile s’impegna fin da ora a fornire al Titolare ogni elemento utile all’effettuazione, da parte di quest’ultimo, della valutazione di impatto sulla protezione dei dati, qualora lo stesso sia tenuto ad effettuarla ai sensi dell’art. 35 del RGDP, nonché ogni collaborazione nell’effettuazione della eventuale consultazione preventiva al Garante ai sensi dell’art. 36 del RGDP stesso.

Il Responsabile, ove necessario ai sensi della normativa vigente o su richiesta del Titolare, relativamente ai Dati Personali ed alle procedure e tecnologie usate dal Responsabile nel trattamento degli stessi, si impegna ad effettuare analisi che esplicitino i rischi e le eventuali possibili misure di attenuazione degli stessi da proporre al Titolare, propedeutiche a valutazioni di impatto, informando quest’ultimo e fornendo copia degli elaborati finali.

1. **SOGGETTI AUTORIZZATI AL TRATTAMENTO**

Il Responsabile è tenuto a identificare per iscritto il proprio personale autorizzato a trattare i Dati Personali tramite apposite lettere di incarico, individuando l’ambito di trattamento consentito e fornendo le istruzioni idonee allo scopo, in particolare vincolando alla riservatezza su tutte le informazioni acquisite nello svolgimento dell’attività, anche per il periodo successivo alla cessazione del rapporto di lavoro. Il Responsabile è tenuto, inoltre, a curarne la formazione, vigilarne l’operato e a comunicare al Titolare, su specifica richiesta, l’elenco aggiornato dei soggetti autorizzati al trattamento.

1. **AMMINISTRATORI DI SISTEMA**

Il Responsabile si impegna a conformarsi al Provvedimento Generale dell’Autorità Garante del 27 novembre 2008 “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”, così come modificato dal Provvedimento dell’Autorità Garante del 25 giugno 2009 “Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento”, così come eventualmente ulteriormente modificato o sostituito dall’Autorità Garante e a ogni altro pertinente provvedimento dell’Autorità stessa.

Il Responsabile si impegna, in particolare, a:

1. designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui sono effettuati trattamenti di Dati Personali;
2. predisporre e conservare l’elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
3. comunicare al Titolare, su sua esplicita richiesta, l’elenco aggiornato degli amministratori di sistema;
4. verificare annualmente l'operato degli amministratori di sistema, informando il Titolare, qualora esplicitamente richiesto, circa le risultanze di tale verifica;
5. mantenere i file di log previsti in conformità a quanto previsto nel suddetto provvedimento.
6. **RAPPORTI CON LE AUTORITÀ**

Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest’ultimo nella difesa in caso di procedimenti dinanzi all’Autorità Garante o all’Autorità Giudiziaria.

1. **ISTANZE DEGLI INTERESSATI**

Il Responsabile si obbliga ad assistere il Titolare e a fornire ogni informazione e/o documento utile o opportuno per supportarlo nel dare riscontro ai diritti esercitati dagli interessati di cui al capo III del Regolamento.

1. **ULTERIORI OBBLIGHI**

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all’art. 28 del Regolamento e delle istruzioni del Titolare di cui al presente contratto e consente al Titolare l’esercizio del potere di controllo e ispezione, prestando ogni necessaria collaborazione alle attività di audit effettuate direttamente dal Titolare o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l’adempimento degli obblighi e delle istruzioni di cui al presente contratto. Qualsiasi verifica condotta ai sensi del presente articolo deve essere eseguita in maniera tale da non interferire con il normale corso delle attività del Responsabile e fornendo a quest’ultimo un ragionevole preavviso.

Il Responsabile si impegna altresì a:

1. effettuare, previa richiesta del Titolare, un rendiconto in ordine all’esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) e delle conseguenti risultanze;
2. collaborare, se richiesto, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l’intero processo di trattamento dei dati personali;
3. realizzare quant’altro sia ragionevolmente utile e/o necessario al fine di garantire l’adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dell’incarico di cui alla presente designazione;
4. informare prontamente il Titolare di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che risulti violata la normativa in materia di protezione dei dati personali, ovvero che il trattamento presenti rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell’interessato, nonché qualora, a suo parere, un’istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati personali.
5. **ULTERIORI RESPONSABILI**

Il Titolare autorizza il Responsabile a ricorrere a ulteriori responsabili per l'esecuzione delle attività di trattamento (o parte delle stesse) oggetto del presente contratto.

In considerazione della normativa sugli appalti pubblici che il Responsabile è tenuto ad applicare al momento della selezione dei fornitori, l’individuazione dei sub-responsabili è subordinata ad una preventiva attività di selezione volta a garantire che gli stessi presentino i requisiti di adeguatezza e conformità alle specifiche disposizioni del RGPD applicabili e che siano imposti agli stessi i medesimi obblighi in materia di protezione dei dati cui è soggetto il Responsabile, in particolare in relazione alle misure di sicurezza; come elemento di potenziale preferenza ed ove possibile rispetto all’affidamento, l’individuazione è subordinata ad una valutazione in merito al rispetto dei controlli previsti dalla certificazione ISO/IEC 27001.

Su richiesta del Titolare, il Responsabile fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il Responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.

Il Responsabile risponde nei confronti del Titolare per l'adempimento degli obblighi da parte del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il Responsabile medesimo.

1. **LUOGO DI TRATTAMENTO DEI DATI E TRASFERIMENTO DE DATI FUORI DELLA UE**

Il Responsabile dichiara che i dati personali saranno trattati e archiviati nel territorio dello Spazio Economico Europeo.

Il Titolare conviene che, qualora il Responsabile ricorra a un sub-responsabile per l'esecuzione di specifiche attività di trattamento (per conto del Titolare) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del GDPR, il Responsabile e il sub-responsabile possono garantire il rispetto del capo V del GDPR utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del GDPR, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

1. **MANLEVA**

Il Responsabile si impegna a mantenere indenne il Titolare da ogni contestazione, azione o pretesa avanzate da parte degli interessati e/o di qualsiasi altro soggetto e/o Autorità a seguito di eventuali inosservanze da parte del Responsabile stesso delle istruzioni di cui alla presente designazione, del Regolamento e delle relative disposizioni specificamente dirette al Responsabile.

1. **CLAUSOLA DI RINVIO**

Per quanto non espressamente previsto nella presente designazione, si fa rinvio alle norme del RGDP, al Codice Civile e alle disposizioni legislative e regolamentari, nazionali e comunitarie vigenti in materia.

1. **DURATA**

Il presente incarico decorre dalla data della sua sottoscrizione e mantiene validità ed efficacia pari alla durata del Protocollo di Intesa sottoscritto con la Regione Autonoma Friuli Venezia Giulia, valido fino al 31 dicembre 2028, prorogabile per un anno.

Il Responsabile, all’atto della cessazione – per qualunque causa - dell’efficacia del presente contratto, salvo la sussistenza di un obbligo di legge o di regolamento nazionale e/o comunitario che preveda la conservazione dei Dati Personali, dovrà interrompere ogni operazione di trattamento degli stessi e dovrà provvedere, a scelta del Titolare, all’immediata restituzione dei Dati Personali allo stesso oppure alla loro integrale cancellazione, in entrambi i casi rilasciando contestualmente un’attestazione scritta che presso lo stesso Responsabile non ne esiste alcuna copia. In caso di richiesta scritta del Titolare, il Responsabile è tenuto a indicare le modalità tecniche e le procedure utilizzate per la cancellazione/distruzione.

1. **DISPOSIZIONI FINALI**

Resta inteso che la presente designazione non comporta alcun diritto per il Responsabile a uno specifico compenso o indennità o rimborso per l’attività svolta.

|  |  |
| --- | --- |
| **IL TITOLARE DEL TRATTAMENTO**  **Ente** | **IL RESPONSABILE DEL TRATTAMENTO**  **Insiel S.p.A.** |