SCHEMA DI ACCORDO PER LA NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679

Tra

Regione del Veneto-Giunta Regionale, Titolare del trattamento ai sensi del Regolamento (UE) 2016/679, (di seguito "Regione" o "Titolare"), con sede legale in Venezia, Dorsoduro 3901, Codice Fiscale 80007580279 e Partita IVA 02392630279, che interviene al presente atto in persona del Direttore pro-tempore della Direzione regionale Prevenzione, Sicurezza Alimentare, Veterinaria, dott/ssa……, nato/a a…….. il……, incarico conferito con D.G.R. n.…..del……, e domiciliato per la carica presso la Regione del Veneto, Direzione Prevenzione, Sicurezza Alimentare, Veterinaria, sita in Venezia, Dorsoduro n. 3493

e

Azienda per il Governo della Sanità della Regione del Veneto - Azienda Zero, in persona del legale rappresentante pro-tempore, con sede in Padova, Passaggio Gaudenzio 1, Codice Fiscale e Partita IVA: 05018720283, in qualità di Responsabile del trattamento dei dati personali ai sensi del Regolamento (UE) 2016/679 (di seguito "Azienda" o "Responsabile")

premesso che

- l'art. 99 co. 1 del D.Lgs. n. 81/2008 prevede che: "*Il committente o il responsabile dei lavori, prima dell'inizio dei lavori, trasmette all'azienda unità sanitaria locale e alla direzione provinciale del lavoro nonché, limitatamente ai lavori pubblici, al prefetto territorialmente competenti la notifica preliminare elaborata conformemente all'allegato XII, nonché gli eventuali aggiornamenti nei seguenti casi: (1)*
  - *a) cantieri di cui all'articolo 90, comma 3;*
  - *b) cantieri che, inizialmente non soggetti all'obbligo di notifica, ricadono nelle categorie di cui alla lettera a) per effetto di varianti sopravvenute in corso d'opera;*
  - c) *cantieri in cui opera un'unica impresa la cui entità presunta di lavoro non sia inferiore a duecento uomini-giorno"*;
- l'art. 54 del citato D.Lgs n. 81/2008 dispone che: "*1. La trasmissione di documentazione e le comunicazioni a enti o amministrazioni pubbliche, comunque previste dal presente decreto legislativo possono avvenire tramite sistemi informatizzati, nel formato e con le modalità indicati dalle strutture riceventi*";
- in adempimento delle disposizioni di cui agli artt. 54 e 99 del D.Lgs. n. 81/2008 è necessario provvedere all'inserimento nel Portale Notifiche Cantieri dei dati contenuti nell'All. XII;
- con Deliberazione della Giunta di Regione del Veneto n. 1144 del 31 luglio 2018 è stato approvato lo Schema di Protocollo di Intesa tra Regione del Veneto, Ispettorato Interregionale del Lavoro di Venezia, Associazione nazionale Costruttori Edili (ANCE) Veneto, Federazione Nazionale Lavoratori Edili Affini e del Legno (FENEAL), Unione Italiana del lavoro (UIL) Veneto, Federazione Italiana Costruzioni e Affini (FILCA), Confederazione Italiana Sindacati lavoratori (CISL) Veneto, Federazione italiana lavoratori legno ed affini (FILLEA), Confederazione Generale Italiana del Lavoro (CGIL) Veneto, per la condivisione delle fonti informative ai fini della programmazione efficace degli interventi nei cantieri e di una migliore copertura del territorio da parte degli organi di ispezione e di assistenza;
- con Deliberazione della Giunta Regionale n. 145 del 15 febbraio 2022, nell'ambito del Nuovo Piano Strategico 2021-2023 per la Tutela della Salute e della Sicurezza sul Lavoro, Azienda Zero è stata individuata quale Responsabile del Trattamento inerente al Portale Notifiche Cantieri per conto di Regione del Veneto;

- il Portale Notifiche Cantieri è un uno specifico applicativo web ideato per semplificare la trasmissione delle notifiche cantieri e dei suoi aggiornamenti ai destinatari previsti dal D.Lgs. n. 81/2008 e s.m.i. (Aziende ULSS e INL) e garantire un approccio unitario e condiviso delle fonti informative per la tutela della salute e sicurezza sul lavoro nei cantieri, oltre a rendere possibile una programmazione efficace degli interventi nei cantieri e una migliore copertura del territorio in termini di controllo, inteso nel suo più ampio significato, da parte degli organi di ispezione e di assistenza;
- il Portale di inserimento in argomento, unico per tutta la Regione del Veneto, è sviluppato e messo a disposizione da Azienda Zero su richiesta e per conto di Regione del Veneto;
- Azienda Zero non persegue alcuna finalità propria tramite il Portale Notifiche Cantieri, pertanto, tutte le attività da essa eseguite in tale ambito ed oggetto del presente Accordo, sono da intendersi svolte esclusivamente per conto di Regione del Veneto, compresa la generazione delle credenziali di accesso agli utenti autorizzati;
- l'art. 4, paragrafo 1, n. 7 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»* (di seguito "GDPR"), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018, individua il Titolare del trattamento ne *«la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali …»,* e visto altresì l'art. 4, paragrafo 1, n. 8) del Regolamento che identifica il Responsabile del trattamento ne *«la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento»;*
- l'art 28, paragrafo 3, del predetto Regolamento, che dispone: "*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento";*
- l'art. 29 dello stesso Regolamento che prevede: "*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri";*
- con il presente atto l'intestata Regione del Veneto-Giunta Regionale, in qualità di Titolare del trattamento, intende provvedere a declinare i contenuti dell'incarico effettuato con DGR n. 145/2022 ad Azienda Zero, che accetta, quale Responsabile del Trattamento dei dati personali relativi al Portale Notifiche Cantieri, ai sensi di quanto disposto dall'art. 28 del GDPR;
- con la sottoscrizione del presente documento le parti, come meglio specificate in epigrafe, intendono regolare i reciproci rapporti in relazione al trattamento dei Dati Personali effettuato dal Responsabile del trattamento per conto della Regione del Veneto ai sensi dell'art. 28, paragrafo 3 del Regolamento.

Tenuto conto dei compiti e responsabilità specifici del Responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'Interessato**.**

Considerato che con il presente Accordo la Giunta Regionale e Azienda Zero intendono regolare i reciproci rapporti in relazione al trattamento dei Dati Personali di cui al precedente capoverso, accettando tutti i termini in essa indicati;

SI CONVIENE E STIPULA QUANTO SEGUE

1. Oggetto e definizioni

Con la sottoscrizione del presente Accordo Azienda Zero, nella persona del proprio legale rappresentante pro tempore, incaricata con Deliberazione della Giunta regionale nr. 145 del 15 febbraio 2022 quale Responsabile del trattamento dei dati con il compito di effettuare le operazioni di trattamento sui dati personali espresse in premessa per conto della Giunta regionale di Regione del Veneto, titolare del trattamento, conferma di essere a conoscenza degli obblighi che si assume e si impegna a trattare i dati attenendosi a quanto previsto nel presente accordo e a tutte le ulteriori istruzioni impartite dal Titolare, nel rispetto delle regole GDPR e della normativa nazionale e regionale. Tali dati saranno trattati con strumenti elettronici, in conformità ai principi di proporzionalità, necessità e indispensabilità del trattamento.

Fatta eccezione per i termini e le espressioni altrimenti definiti nel presente Accordo, i termini e le espressioni contrassegnate da iniziali maiuscole avranno il significato di seguito specificato:

"GDPR"	indica il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 206 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
"Autorità di Controllo"	indica il Garante per la protezione dei Dati Personali.
"Autorizzati"	le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile e che agiscono sotto l'autorità del Titolare o del Responsabile ai sensi dell'art. 29 del GDPR.
"Accordo di trasferimento dei dati"	indica ogni accordo stipulato tra le parti e finalizzato al trasferimento legittimo dei Dati Personali.
"Categorie Particolari di Dati"	indica ogni Dato Personale idoneo a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
"Codice"	il D.Lgs. n. 196/2003 "Codice in materia dei dati personali" così come successivamente integrato e modificato (da ultimo del D.Lgs. n. 101/2018).
"EDPB"	indica il Comitato Europeo per la protezione dei dati, organismo dell'Unione Europea dotato di personalità giuridica istituito ai sensi degli artt. 68 e ss. del GDPR.
"Comunicazione"	dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, del responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'art. 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione.

"Contratto"	indica l'accordo in essere tra le Parti.
"Dato/i Personale/i"	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
"Dati Giudiziari"	indica ogni Dato Personale relativo a condanne penali e ai reati o a connesse misure di sicurezza ovvero relativo a provvedimenti giudiziari, sanzioni penali, o carichi pendenti, o la qualità dell'imputato o indagato ai sensi degli articoli 60 e 61 del Codice di Procedura Penale.
"Diffusione"	Indica il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
"Gruppo di Lavoro Articolo 29"	indica il Gruppo di lavoro istituito in virtù dell'articolo 29 della direttiva 95/46/CE fino al 25 maggio 2018, data della sua cessazione.
"Interessato"	la persona fisica identificata o identificabile cui si riferiscono i Dati Personali.
"Responsabile del trattamento"	Indica chi effettua un trattamento dati per conto del titolare del trattamento.
"Sub-responsabile"	indica qualsiasi soggetto, persona fisica o giuridica, a cui il Responsabile ricorra per l'esecuzione di specifiche attività di Trattamento per conto del Titolare a cui sono imposti gli stessi obblighi del Responsabile.
"Terze Parti o Terzi"	indica la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non siano l'interessato, il Titolare, il Responsabile e gli incaricati autorizzati al trattamento dei Dati Personali sotto l'autorità diretta del titolare o del responsabile.
"Titolare del trattamento"	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
"Trattamento"	Indica qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica. L'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

2. Finalità del trattamento e tipologia dei dati trattati

Il Responsabile è autorizzato a trattare, per conto del Titolare, i dati personali inerenti l'applicativo web Portale Notifiche Cantieri secondo quanto di seguito descritto:

Categoria di dati Trattati	Finalità del Trattamento	Modalità del Trattamento	Categoria di interessati	Trattamento
Dati personali - anagrafici (*nome e cognome, codice fiscale);* - di contatto (*indirizzo civico e di peo)*	Notifica preliminare ex art. 99 co. 1, D.Lgs. n.81/2008 (Allegato XII)	Informatica	Committenti, Responsabili dei Lavori, Responsabili della sicurezza e salute, Coordinatori della sicurezza e salute	Manutenzione e assistenza del Portale
Dati personali - anagrafici (*nome e cognome, codice fiscale);* - di contatto (*peo e recapito telefonico)*	Accesso all'applicativo per i fini di cui al D.Lgs. n.81/2008	Informatica	Dipendenti degli Enti destinatari previsti dal D.Lgs. n.81/2008	Apertura profilo account delle persone fisiche indicate dal Titolare

3. Nomina del Responsabile del trattamento

Con la sottoscrizione del presente atto, il Titolare conferma l'incarico di Azienda Zero, già effettuato a mente della DGR n.145/2022, quale Responsabile del Trattamento ai sensi dell'art. 28 del GDPR, con il compito di effettuare le operazioni di trattamento sui Dati Personali, di cui entra in possesso o ai quali ha comunque accesso.

Azienda Zero, con la sottoscrizione del presente Accordo, accetta tutti i termini sotto indicati, conferma la diretta e approfondita conoscenza degli obblighi che si assume e si impegna a procedere al trattamento dei Dati Personali attenendosi alle istruzioni ricevute dal Titolare attraverso la presente nomina o a quelle ulteriori che saranno conferite nel corso delle attività prestate in suo favore.

4. Garanzie

Il Responsabile del trattamento conferma di possedere le garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli Interessati.

Il Responsabile si impegna, pertanto, ad operare secondo il principio di *accountability*, fin dall'inizio del trattamento e per progettazione predefinita, per ridurre al minimo i rischi connessi al trattamento e per garantire il pieno rispetto delle disposizioni vigenti in materia di trattamento dei dati personali.

5. Diritti del Titolare

Il Titolare impartisce al Responsabile istruzioni documentate per il trattamento dei dati personali e ha diritto di ottenere dal Responsabile tutte le informazioni necessarie per verificare il rispetto delle istruzioni

impartite, l'adempimento degli obblighi del presente Accordo nonché della normativa in materia di protezione dei dati personali.

Il Titolare ha in particolare il diritto di ottenere le informazioni relative alle misure tecniche e organizzative adottate dal Responsabile che sono, nello specifico, indicate nell'allegato 1 *"Misure di sicurezza"* del presente atto, da intendersi a tutti gli effetti parte integrante dell'atto stesso.

Sono considerate istruzioni documentate le prescrizioni previste nel presente Accordo e in ogni altra eventuale comunicazione scritta del Titolare concernente le modalità di trattamento dei dati da parte del Responsabile.

Il Titolare esercita i poteri di verifica e controllo secondo le modalità stabilite all'articolo 14.

Qualora venga rilevato che un'istruzione impartita dal Titolare violi le disposizioni normative in materia di protezione dei dati personali, il Responsabile si obbliga ad informare immediatamente il Titolare.

6. Obblighi del Responsabile

Con la sottoscrizione del presente Accordo, il Responsabile si impegna a garantire la correttezza del trattamento e ad adottare adeguate misure tecniche e organizzative in modo tale che il trattamento soddisfi i requisiti del GDPR ed ogni altra istruzione impartita da Regione del Veneto, nonché a tener conto dei provvedimenti tempo per tempo emanati dall'Autorità di Controllo, dal Gruppo di Lavoro Articolo 29 e dall'EDPB, inerenti al trattamento svolto, garantendo la tutela dei diritti degli Interessati. A tal fine, il Responsabile opera secondo il principio di accountability, fin dall'inizio del trattamento e per progettazione predefinita, per ridurre al minimo i rischi connessi al trattamento e per garantire il pieno rispetto delle disposizioni vigenti in materia di trattamento dei dati personali.

Il Responsabile è tenuto a svolgere, con correttezza e buona fede, le seguenti attività:

a) rispettare i principi di liceità, correttezza, trasparenza, pertinenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione, tutela fin dall'inizio del trattamento e per progettazione definita, di cui al GDPR;

b) assicurare il rispetto dei principi contenuti nel GDPR nelle attività di raccolta, archiviazione, conservazione, collocazione ed accesso agli archivi e nel compimento delle operazioni di trattamento sui dati personali, custodendo gli stessi in maniera che ad essi non accedano persone non autorizzate;

c) eseguire operazioni di trattamento sui dati al solo scopo di eseguire le prestazioni oggetto del Rapporto e di adempiere ad altre previsioni normative, evitando qualsiasi ulteriore operazione che non sia strettamente necessaria a tale esecuzione;

d) rispettare le regole di organizzazione e le altre istruzioni impartite dal Titolare in merito al compimento delle operazioni di trattamento sui dati personali, avvisandolo qualora riscontri che taluna di dette regole e/o istruzioni possano contrastare con le norme del GDPR o della legislazione nazionale;

e) inserire nel proprio Registro dei Trattamenti tutte le categorie di attività relative al trattamento, svolte in esecuzione del presente Accordo, secondo quanto prescritto dall'articolo 30, paragrafo 2, del GDPR e, su richiesta, mettere tale registro a disposizione del Titolare e/o dell'Autorità di Controllo;

f) individuare e incaricare per iscritto i soggetti autorizzati a compiere operazioni di trattamento in nome e per conto del Responsabile e sotto la sua diretta supervisione e responsabilità, fornendo ai medesimi istruzioni operative per una corretta gestione del trattamento nel rispetto dei diritti degli Interessati;

g) mantenere la riservatezza delle informazioni, dei documenti e degli atti amministrativi dei quali venga a conoscenza in relazione al trattamento svolto per le funzioni affidategli, garantendo altresì che i propri dipendenti e/o le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza e, in ogni caso, che abbiano ricevuto la formazione necessaria;

h) il Responsabile si impegna, con riferimento ai propri dipendenti, a dare attuazione a quanto previsto nel Provvedimento Generale del Garante del 27 novembre 2008 e s.m.i., secondo quanto precisato nel successivo articolo 7 del presente accordo;

i) istituire un Registro delle violazioni dei dati personali (Data Breach) ai sensi dell'articolo 33 del GDPR e, su richiesta, mettere tale registro a disposizione del Titolare e/o dell'Autorità di Controllo;

j) laddove necessario, cooperare per l'adozione delle misure di reazione e di notifica nel caso di violazione di dati personali (data breach), ai sensi degli artt. 33 e 34 GDPR;

k) effettuare la comunicazione dei dati personali, laddove prevista, solo nei limiti consentiti dalle finalità del trattamento, dal contenuto del consenso prestato dall'Interessato, da disposizioni di legge o regolamenti, e in particolare dall'articolo 2 ter del Codice, nonché dai provvedimenti dell'Autorità di Controllo;

l) collaborare con il Responsabile della Protezione dei Dati (RPD) nominato dal Titolare;

m) al fine di evitare e/o ridurre il rischio di distruzione o perdita anche accidentale dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme, adottare in proprio le misure di sicurezza indicate nell'allegato 1 "*Misure di Sicurezza*", da considerarsi parte integrante del presente accordo, al fine di garantire un livello di sicurezza adeguato al rischio nel rispetto delle disposizioni contenute nel GDPR e, in particolare, dall'articolo 32;

n) assistere il Titolare nella soddisfazione delle richieste che gli Interessati avanzino nell'esercizio dei diritti conferiti dal GDPR, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile;

o) coadiuvare il Titolare del trattamento nella difesa in caso di procedimenti (relativi a trattamenti di dati connessi allo svolgimento dell'attività oggetto della convenzione) dinanzi all'Autorità di controllo o all'Autorità Giudiziaria, fornendo al Titolare del trattamento tutte le informazioni e/o i documenti necessari che potranno essere richiesti da quest'ultima;

p) non effettuare comunicazione di dati verso destinatari aventi sede al di fuori dello spazio economico europeo, se non previa autorizzazione da parte del Titolare;

q) non diffondere dati, se non nei casi previsti da Leggi e Regolamenti, e in particolare dall'articolo 2ter del Codice, nonché dai provvedimenti dell'Autorità di Controllo;

r) conservare, aggiornare e mettere a disposizione del Titolare e/o degli organi di controllo, l'elenco con i dati (nome, cognome, funzione e /o ambito di competenza) degli amministratori di sistema nominati e muniti dei necessari requisiti di esperienza, capacità ed affidabilità in conformità di quanto previsto dal Provvedimento 27 novembre 2008 del Garante per la protezione dei dati personali e s.m.i. e curare l'applicazione di tutte le ulteriori prescrizioni contenute nel suddetto provvedimento;

Il Responsabile si impegna a comunicare prontamente al Titolare eventuali situazioni sopravvenute che, per il mutare delle circostanze acquisite in base al progresso tecnico o per qualsiasi altra ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico.

7. Ulteriori prescrizioni poste a carico del Responsabile

Ai sensi del Provvedimento a carattere generale sugli Amministratori di Sistema dell'Autorità Garante Privacy del 27 Novembre 2008, il Responsabile è stato individuato dal Titolare del trattamento in base ad una scrupolosa valutazione dell'esperienza, della capacità, dell'affidabilità e preparazione e fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, con particolare riferimento al profilo relativo alla sicurezza nella custodia e nel trattamento dei dati personali.

Il Responsabile ha quindi, il potere e il dovere di compiere tutto quanto si renderà necessario ai fini del rispetto e della corretta applicazione delle vigenti disposizioni in materia di trattamento dei dati personali ivi compreso il profilo relativo alla sicurezza.

Il Responsabile garantirà al Titolare del trattamento che ciascun incaricato Amministratore di Sistema accederà con proprio utente e propria password.

Con l'accettazione di questa nomina il Responsabile si impegna a nominare individualmente - ai sensi del Provvedimento a carattere generale dell'Autorità Garante Privacy del 27 Novembre 2008 (G.U. N. 300 del 24 dicembre 2008) cosi come modificato dal Provvedimento a carattere generale dell'Autorità Garante Privacy del 25 giugno 2009 (G.U. N. 149 del 30 giugno 2009) - gli incaricati della sua struttura che rivestono il ruolo di Amministratori del Sistema informativo. La designazione quale Amministratore di Sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Annualmente il Responsabile fornirà al Titolare del trattamento l'elenco aggiornato degli Amministratori di sistema e provvederà a verificare l'attività dei soggetti individuati, come indicato dal Garante per la Protezione dei Dati Personali nel Provvedimento sugli Amministratori di Sistema sopra richiamato.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di sistema. Le 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.

Il Responsabile è tenuto a:

- garantire che le risorse vengano utilizzate dagli utenti che ne abbiano effettivamente diritto, utilizzando gli opportuni meccanismi di identificazione e autenticazione allo scopo di incrementare il livello di protezione e sicurezza dei trattamenti di dati personali effettuati con strumenti elettronici;

- essere responsabile della gestione dei propri sistemi di identificazione e autenticazione, usando la massima riservatezza e discrezione affinché il processo venga svolto in conformità alle disposizioni di legge, eseguendo controlli periodici sull'efficacia delle misure di sicurezza adottate;

- collaborare con il Titolare del trattamento dei dati alla definizione di idonee regole in ambito di Sicurezza del trattamento dei dati afferente ai sistemi oggetto della presente nomina;

- cooperare con il Titolare alla verifica dell'operato dei soggetti terzi idoneamente designati, qualora sia necessario, in caso di interventi tecnici che abbiano impatto sul sistema informativo del Titolare e sulla sicurezza del trattamento di dati;

- curare, per quanto concerne i propri sistemi informatici, l'adozione e l'aggiornamento delle più ampie misure di sicurezza volte a far sì che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

- aggiornare periodicamente, con frequenza adeguata, i programmi volti a prevenire la vulnerabilità dei propri strumenti elettronici e a correggerne i difetti o assicurarsi che ciò venga effettuato da soggetti idoneamente designati;

- coadiuvare, per quanto di competenza, il Titolare del trattamento, nell'attuazione di misure tecniche adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché 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.

8. Condizioni particolari per il caso di violazioni dei dati personali (data breach)

In caso di violazione dei dati personali consistente nella violazione di 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 e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati dal Responsabile per conto di Regione del Veneto (c.d. data breach), il Responsabile deve:

- informare il Titolare tempestivamente di ogni violazione dei dati personali trattati per conto di Regione del Veneto che presenti un rischio per i diritti e le libertà delle persone fisiche, indicando il Responsabile della Protezione dei dati (RPD) e relativi dati di contatto;
- nelle successive 48 ore, fornire tutti i dettagli completi della violazione subita: in particolare, fornendo una descrizione della natura della violazione dei dati personali, le circostanze in cui è avvenuta, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali e una stima degli interessati coinvolti, i provvedimenti adottati (o che si intendono adottare) per porvi rimedio o comunque mitigarne i possibili effetti negativi;
- attivarsi per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive al Titolare ed attuando tempestivamente tutte le azioni correttive approvate e/o richieste dalla stessa;
- fornire assistenza al Titolare per far fronte alla violazione e alle sue conseguenze soprattutto in capo agli interessati coinvolti.

9. Documentazione Privacy

Il Responsabile si impegna ad adottare la documentazione in materia di protezione dei Dati Personali prevista dalla normativa italiana ed europea e le relative procedure concernenti le adeguate misure tecniche e organizzative.

10. Condizioni particolari per il riscontro alle istanze degli Interessati

Tenendo conto della natura del trattamento, il Responsabile si obbliga a dare riscontro alle richieste, che pervengano allo stesso direttamente o che gli siano trasmesse dal Titolare, per l'esercizio dei diritti dell'interessato di cui alla Sezione 3 del GDPR nel rispetto dei termini previsti dall'articolo 12 del GDPR.

11. Condizioni particolari per l'adozione delle misure di sicurezza

Ferma restando l'applicazione delle misure tecniche e organizzative ai sensi dell'articolo 32 del GDPR, al fine di garantire un livello di sicurezza sempre adeguato al rischio, il Responsabile ha l'obbligo di assicurare la continuità operativa delle reti e dei sistemi informativi e a prevenire o ridurre al minimo l'impatto che eventuali incidenti potrebbero causare ai suddetti sistemi, informando tempestivamente il Titolare degli eventuali incidenti di sicurezza occorsi ai sensi dell'articolo 33, comma 2, del GDPR e dell'articolo 12, comma 7, della presente convenzione.
In particolare il Responsabile, per le misure tecniche ed organizzative atte a gestire i rischi è chiamato a conformarsi alla norma ISO 27799:2016, quale linea guida per la sicurezza delle informazioni, prevedendo la selezione, l'implementazione e la gestione dei controlli di sicurezza, in relazione al rischio valutato, nonché alla norma ISO 27701:2019 quale linea guida per gestire adeguatamente i rischi per la privacy relativi alle informazioni personali e per dare dimostrazione che il trattamento dei dati personali avviene nel rispetto delle prescrizioni del GDPR.

Il Responsabile è tenuto a presentare al Titolare i rapporti periodici delle attività di audit interni secondo un programma concordato e definito preventivamente volti a verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative implementate al fine di assicurare la loro adeguatezza in relazione al trattamento dei dati effettuato. E' comunque facoltà del Titolare condurre, con la collaborazione del Responsabile, degli audit di seconda e/o di terza parte sulle misure di sicurezza dalla stessa adottate.

Il Responsabile è inoltre tenuto ad adeguare i controlli e le misure di sicurezza adottate all'evoluzione tecnologica al fine di garantire costantemente la loro efficacia.

12. Sub Responsabili

Azienda Zero sarà tenuta, in sede di individuazione di ulteriori Responsabili, ad informare preventivamente il Titolare, al fine di consentire allo stesso, come previsto dall'art. 28 paragrafo 2 del GDPR, di poter manifestare eventuale formale opposizione alla nomina entro e non oltre il congruo termine di quindici giorni dalla ricezione della comunicazione.

Decorso tale termine, Azienda Zero potrà procedere all'effettuazione delle designazioni, normativamente previste, nei confronti degli ulteriori Responsabili del Trattamento individuati.

Tale nomina di un ulteriore Responsabile del trattamento da parte di Azienda Zero sarà possibile a condizione che su tale soggetto siano imposti gli stessi obblighi in materia di protezione dei dati contenuti nel presente atto, incluse garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti richiesti dalle leggi applicabili.

Azienda Zero rimane tuttavia responsabile nei confronti del Titolare con riguardo all'adempimento degli obblighi in materia di protezione dei dati da parte degli ulteriori Responsabili del trattamento.

Azienda Zero si impegna altresì a comunicare eventuali modifiche ed aggiornamenti dei trattamenti di competenza dei propri ulteriori Responsabili.

13. Autorizzazione alla nomina in qualità di Sub-Responsabili

Salvo quanto previsto all'articolo precedente, Azienda Zero, in qualità di Responsabile del Trattamento, deve ricorrere alla nomina di Ulteriori Responsabili del trattamento di dati personali ad essa subordinati

nell'ambito dei trattamenti di dati personali e ad essa delegati secondo lo schema rappresentato *nell'allegato 2 "RTI*" da considerarsi parte integrante del presente Accordo.

Il Responsabile assicura che i fornitori individuati offrono garanzie sufficienti ed adeguate, sia sotto il profilo delle misure tecniche che organizzative, a soddisfare i requisiti previsti dal GDPR per la tutela dei diritti dell'interessato e, qualora richiesto, si rende fin da ora disponibile a dare tutte le evidenze richieste.

Pertanto, con la sottoscrizione del presente Accordo, si autorizza sin d'ora Azienda Zero, nella sua qualità di Responsabile del trattamento, a nominare quali Ulteriori Responsabili del trattamento i fornitori come identificati nell'allegato 2 "RTI".

Azienda Zero darà tempestiva comunicazione circa eventuali sostituzioni, modifiche ed aggiornamenti riguardo ai suddetti responsabili dei trattamenti.

14. Controlli e attività di audit

Al fine di verificare il rispetto delle istruzioni impartite, l'adempimento degli obblighi del presente Accordo nonché della normativa in materia di protezione dei dati personali, il Titolare ha diritto di disporre verifiche e controlli e di svolgere specifiche attività di audit, avvalendosi anche di personale espressamente incaricato a tale scopo, nonché di svolgere ispezioni anche presso le sedi del Responsabile.

Il Responsabile si impegna a prestare ogni necessaria collaborazione alle attività di verifica, controllo, ispezione e alle attività di audit svolte dal Titolare o da altro soggetto da questi incaricato.

Le attività di verifica e controllo di cui al presente articolo saranno eseguite in maniera tale da non interferire con il normale corso delle attività del Responsabile del trattamento e fornendo a quest'ultimo un ragionevole preavviso.

15. Durata e Cessazione del Trattamento

La presente nomina cesserà al momento del completo adempimento o per diversa disposizione normativa di Regione del Veneto. Il trattamento, comunque, deve avere una durata non superiore a quella necessaria agli scopi per i quali i dati personali sono stati raccolti e tali dati devono essere conservati nei sistemi e nelle banche dati del Responsabile in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello in precedenza indicato.

A seguito della cessazione del trattamento affidato al Responsabile, o nei casi di cui al comma precedente, qualsiasi ne sia la causa, il Responsabile sarà tenuto a restituire i dati personali trattati, con impegno alla rimozione integrale degli stessi da ogni suo dispositivo salvo diversa indicazione del Titolare.

16. Condizioni particolari per il trasferimento dei dati all'estero

Il Responsabile si impegna a limitare gli ambiti di circolazione e trattamento dei Dati Personali (*es. memorizzazione, archiviazione e conservazione dei dati sui propri server o in cloud*) allo spazio economico europeo.

Eventuali trasferimenti al di fuori dell'ambito di cui al paragrafo precedente, saranno possibili solo previa autorizzazione del Titolare.

17. Responsabilità per violazione delle disposizioni

Il Responsabile, con l'accettazione della presente nomina, risponderà per le sanzioni inflitte e per il danno causato dal trattamento attuato in difformità alla disciplina vigente sulla protezione dei dati che gli siano attribuibili o in difformità rispetto alle legittime istruzioni del Titolare del trattamento.

Il Responsabile si impegna a comunicare prontamente al Titolare eventuali situazioni sopravvenute che, per il mutare delle conoscenze acquisite in base al progresso tecnico o per qualsiasi altra ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico.

In caso di violazione delle disposizioni contenute nel presente atto relativamente alle finalità e modalità di trattamento dei dati, di azione contraria alle istruzioni ivi contenute o in caso di mancato adempimento agli obblighi specificatamente diretti al Responsabile del trattamento dei dati dal GDPR, il Responsabile sarà considerato quale Titolare del trattamento e ne risponderà personalmente e direttamente.

Per quanto qui non disciplinato, si applica l'articolo 82, paragrafi 4 e 5 del GDPR.

18. Disposizioni finali

1. Trovano applicazione, ove non diversamente previsto, le norme del GDPR, del Codice Civile e delle disposizioni legislative e regolamentari nazionali e comunitarie vigenti in materia.

2. Il presente Accordo di nomina potrà essere integrato a seguito di successive disposizioni normative intervenute o di disposizioni ulteriori del Titolare del Trattamento.

3. La sottoscrizione della presente Accordo non comporta alcun diritto per il Responsabile del trattamento ad uno specifico compenso o indennità o rimborso per l'attività svolta.

4. Si dà atto che alla scadenza o cessazione del presente Accordo per qualsiasi causa, il Responsabile è comunque tenuto all'obbligo di riservatezza.

5. Qualora una o più delle clausole previste nel presente Accordo siano o divengano nulle in forza di legge, ovvero a fronte di un provvedimento del giudice, la validità delle altre disposizioni non sarà in alcun modo pregiudicata.

6. Il presente atto, sottoscritto con firma digitale ai sensi della normativa vigente, è soggetto ad imposta di bollo ai sensi di quanto disposto nell'allegato A – tariffa, articolo 2 del DPR 26.10.1972 n. 642, solo in caso d'uso ai sensi dell'art. 5 del DPR del 26.4.1986 n.131.

Data _____

Il Titolare del Trattamento

_____

Per integrale accettazione

Data _____

Il Responsabile del Trattamento

_____

Allegato 1 - Misure di Sicurezza

Misure di Sicurezza atte alla finalizzazione della nomina privacy

#	MISURE DI SICUREZZA	RISPOSTE
1	L'Organizzazione adotta un Sistema di gestione della Privacy, definisce e assegna ruoli e responsabilità delle figure coinvolte, adotta procedure e policies formalizzate e aggiornate in materia di protezione dei dati personali e di sicurezza delle informazioni.	Compliant
2	L'Organizzazione, coerentemente con il Sistema di gestione della Privacy adottato, adotta gli strumenti e i presidi previsti dalla normativa, tra cui, qualora ne ricorrano i presupposti, il Registro dei trattamenti.	Compliant
3	A livello organizzativo, sono individuate le aree responsabili della gestione degli aspetti relativi alla privacy (es. uffici / strutture preposte, personale dedicato, ecc.) e, nel caso in cui ricorrano i requisiti previsti dalla legge, è stato individuato e nominato un DPO/RPD in conformità con quanto previsto dal GDPR.	Compliant
4	Agli autorizzati al trattamento sono impartite istruzioni scritte che definiscano le modalità di gestione dei dati personali oggetto di trattamento.	Compliant
5	Sono previste e attuate attività di formazione sui temi di sicurezza e privacy nei confronti degli autorizzati al trattamento.	Compliant
6	Le attività di trattamento svolte dai Responsabili del trattamento sono disciplinate da appositi accordi scritti, e sono definite apposite attività di monitoraggio / riesame dei Responsabili esterni.	Compliant
7	L'Organizzazione, ove opportuno, definisce e adotta informative adeguate e conformi a quanto previsto dalla normativa vigente (es. espresse in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro).	Compliant
8	I sistemi sono configurati in modo tale che, per impostazione predefinita, siano visibili e accessibili da parte degli incaricati al trattamento solo i dati personali necessari per ogni specifica finalità del trattamento (c.d. principio di "privacy by default").	Compliant
9	La società ha definito una procedura per la valutazione degli impatti privacy delle attività/progetti svolti, incluse le attività di sviluppo/change (c.d. principio di "privacy by design").	Compliant

10	Sono individuati, designati e gestiti i soggetti che operano in qualità di Amministratori di Sistema in conformità con quanto previsto dal provvedimento del 27/11/2008 del Garante Privacy. Inoltre, è predisposto e aggiornato periodicamente un elenco degli stessi con le relative responsabilità e i compiti assegnati.	Compliant
11	Gli access log degli Amministratori di Sistema sono gestiti in conformità con quanto previsto dal provvedimento del 27/11/2008 dell'Autorità Garante sugli Amministratori di Sistema.	Compliant
12	I sistemi IT utilizzati dall'Organizzazione sono catalogati sulla base delle informazioni contenute negli stessi (classificazione dei dati).	Compliant
13	Alla fine del loro ciclo di vita, gli asset IT utilizzati per l'elaborazione dei dati sono dismessi in modo sicuro (sovrascrittura/cancellazione logica, etc.).	SI
14	Le attività di backup svolte dall'Organizzazione sono effettuate con frequenza predeterminata e adeguata a garantire la disponibilità dei dati in conformità al livello di criticità degli stessi.	SI
15	L'Organizzazione ha definito un piano di Disaster Recovery e un processo di Business Continuity, e questi sono periodicamente aggiornati.	Non sono formalizzati, ma sono presenti misure che garantiscono l'alta affidabilità e la protezione dei dati
16	È definito e documentato un processo di gestione delle utenze (es. creazione utenza, profilazione, variazione di mansione, dismissione utenza) che identifichi anche i relativi ruoli e responsabilità.	Compliant
17	L'Organizzazione assicura che le utenze dei dipendenti che lasciano la società siano disattivate in modo permanente.	Compliant
18	L'Organizzazione ha definito un processo per cui gli accessi agli applicativi (logon / logoff) sono tracciati e adeguatamente protetti da azioni/modifiche indesiderate.	Compliant
19	Il controllo accessi è basato su una politica che correla l'accesso alle informazioni alle effettive esigenze lavorative (principio need to know).	Compliant (è presente un unico profilo)
20	L'Organizzazione fornisce ad ogni utente un'utenza individuale, univoca e non riassegnabile ad altre persone.	SI
21	L'Organizzazione adotta adeguati presidi per la gestione degli accessi ai sistemi IT, tra cui la limitazione al numero di tentativi di accesso non andati a buon fine, valutazione sull'utilizzo di tecniche di autenticazione multifattore, etc.	Autenticazione tramite MyId (SPID/CIE3.0)
22	Le credenziali per l'accesso al sistema sono archiviate in maniera adeguatamente protetta (es. cifratura delle password di dominio).	SI

23	Le password utilizzate devono rispettare un livello di complessità conforme ai più recenti standard di sicurezza ed essere soggette ad una scadenza periodica almeno bimestrale.	Autenticazione tramite MyId (SPID/CIE3.0)
24	Esiste una procedura per la distribuzione sicura agli utenti delle password di accesso (es. invio delle password all'interno di buste sigillate, comunicazione delle stesse tramite un canale diverso da quello utilizzato per la comunicazione dell'utenza (email personale), ecc.).	SI
25	L'Organizzazione effettua attività di revisione periodica dei diritti di accesso ai dati affinché l'assegnazione dei profili sia coerente con le mansioni attribuite.	Compliant
26	L'Organizzazione utilizza ambienti di sviluppo e test separati dall'ambiente di produzione ed evita l'utilizzo di dati reali al di fuori dell'ambiente di produzione.	Compliant
27	Sono adottate le politiche previste per lo sviluppo sicuro del software (es. secure coding guidelines, politiche e procedure, ecc.), in coerenza con best practice e standard di settore internazionali.	Seguite le Linee Guida AGID per lo Sviluppo Sicuro del Software e le tecniche di sviluppo imposte da OWASP
28	L'Organizzazione svolge con cadenza periodica attività di vulnerability assessment e/o penetration test.	Parzialmente. Sono stati effettuati VA, senza una cadenza periodica
29	L'Organizzazione adotta misure di sicurezza fisica per l'accesso, il monitoraggio e il mantenimento in sicurezza di edifici e sala server (es. accesso con chiavi, badge, tornelli, telecamere, sistema di allarmistica antintrusione e antincendio, ecc.).	SI
30	L'Organizzazione ha definito una procedura per la gestione e archiviazione della documentazione cartacea.	Non applicabile
31	I locali che contengono gli armadi e i cassetti sono protetti con adeguate misure di sicurezza (es. chiusura a chiave, uso di armadi ignifughi, sistemi di rilevazione fumo) in considerazione del livello di criticità delle informazioni contenute).	Non applicabile
32	Sono adottati processi per l'identificazione, valutazione e gestione delle vulnerabilità delle risorse (es. sistemi, locali, dispositivi).	Non applicabile
33	L'Organizzazione ha definito un processo di gestione degli incidenti che consenta di rilevare, registrare, gestire e chiudere eventuali incidenti di sicurezza informatica.	Compliant
34	L'Organizzazione ha definito un processo di gestione degli incidenti di sicurezza che impattano sui dati personali (data breach), nel rispetto della normativa vigente e che preveda una comunicazione tempestiva degli incidenti ad organizzazioni terze nel caso in cui vengano svolte attività di trattamento di dati personali per loro conto.	Compliant

35	L'accesso wireless al sistema IT è consentito solo a utenti autorizzati dall'Organizzazione, utilizzando canali sicuri ed adeguatamente protetti (es. meccanismi di crittografia sicuri). Il traffico di rete è comunque monitorato e controllato attraverso Firewall e Intrusion Detection Systems.	Compliant
36	L'Organizzazione adotta procedure di gestione dei dispositivi mobili e portatili stabilendo regole chiare per il loro corretto utilizzo e individuando ruoli e responsabilità specifici relativi alla loro gestione.	Compliant
37	L'Organizzazione adotta e mantiene aggiornate soluzioni tecnologiche di protezione dalle minacce esterne (es. antivirus, antispam, content filtering, ecc.) sulle postazioni di lavoro e sulla rete dati.	Compliant
38	Sono garantite comunicazioni sicure secondo le best practices attuali (ad es. adozione di HTTPS, SSL e certificati EV (Extended Validation Certificate).	Compliant
39	L'Organizzazione considera la cifratura dei dati *at rest* (es. a livello di disco o di database) sulla base di una valutazione della criticità dei dati salvati.	Vista la natura pubblica dei dati, non si procede con cifratura *at rest*
40	L'Organizzazione definisce e attua un processo di monitoraggio periodico per identificare e installare tempestivamente le patch (anche provenienti da fornitori).	Compliant

Allegato 2 - RTI

il Titolare autorizza il Responsabile ad affidare parte delle operazioni di trattamento ai seguenti ulteriori Responsabili costituiti in RTI:

Paese in cui è stabilito l'ulteriore Responsabile	**Regione Sociale Ulteriori Responsabili**	**Sede legale e dati di contatto**	**Attività di trattamento affidata**
ITALIA	**GPI S.p.A.** (Mandataria)	Sede legale e amministrativa: Via Ragazzi del '99 n. 13 38123 Trento, Italia Tel. 0461381515 info@gpi.it gpi@pec.gpi.it Partita IVA 01944260221	- Manutenzione correttiva, evolutiva e adeguativa del sistema informativo SPISAL e Stili di Vita. - Assistenza help desk. - Formazione.
ITALIA	**Onit Group s.r.l.** (Mandante)	Sede legale: Via dell'Arrigoni n. 308 47522 - Cesena (FC), Tel. 0547 313110 Partita IVA 03240560403	

Qualora l'ulteriore Responsabile intendesse affidare ad ulteriori sub-responsabili trattamenti 'diversi' rispetto a quelli indicati in tabella e/o nell'offerta e/o nel contratto principale, o ingaggiare altri ulteriori sub-responsabili diversi da quelli comunicati, dovrà provvedere a comunicare tali variazioni al Responsabile.