**ALLEGATO “A”**

**ATTO DI DESIGNAZIONE DEL FORNITORE**

**QUALE RESPONSABILE DEL TRATTAMENTO**

Mediante il presente documento (di seguito, anche “Atto di Designazione”), redatto ai sensi dell’art. 28 del Regolamento (UE) 2016/679 del 27 aprile 2016 (di seguito, il “GDPR”), Trenord S.r.l., agente in qualità di titolare del trattamento (di seguito, anche il “Titolare”), intende nominare …………… (di seguito, anche il “Responsabile” o “Appaltatore”) quale Responsabile del trattamento con riferimento ai trattamenti di dati personali effettuati ai fini e nella misura di quanto previsto dal contratto stipulato tra le parti sopra identificate, sottoscritto contestualmente al Contratto (di seguito, anche il “Contratto”).

In particolare, per l’intera durata del Contratto, l’Appaltatore tratterà i dati personali relativi al Contratto per finalità di esecuzione dello stesso.

Il Responsabile si dichiara in grado di fornire garanzie sufficienti a porre in essere adeguate misure tecniche e organizzative al fine di rendere i trattamenti in linea con i requisiti del GDPR e di ogni ulteriore atto con forza di legge o regolamentare in materia di protezione dei dati personali. Il Responsabile si dichiara altresì in grado di offrire analoghe garanzie per quanto concerne la tutela dei diritti dell’interessato.

# **OBBLIGHI DEL RESPONSABILE**

Alla luce di quanto sopra il Responsabile si obbliga a:

1. dare esecuzione al Contratto trattando dati personali degli interessati nel rispetto dei criteri, le procedure operative e le misure di sicurezza stabiliti dal Titolare, che potrà integrarli o modificarli nel corso del rapporto contrattuale nelle modalità che risulteranno più opportune rispetto al caso concreto;
2. effettuare ogni operazione di trattamento di dati personali (i) ai sensi del Contratto e (ii) per il solo fine e nei soli limiti di quanto stabilito dal Titolare. Ogni ulteriore trattamento di dati per finalità differenti da quelle stabilite dal Titolare è tassativamente proibito;
3. trattare i dati personali all’interno del territorio di uno Stato Membro dell’Unione Europea, di uno stato appartenente allo Spazio Economico Europeo o di un territorio che la Commissione Europea ha identificato come in grado di garantire un livello adeguato di protezione dei dati personali ai sensi del GDPR. Ogni trasferimento di dati personali verso un paese terzo richiede la preventiva approvazione scritta del Titolare. In caso di ottenuta approvazione scritta del titolare il Responsabile dovrà: (i) garantire che il trasferimento dei dati sia soggetto a garanzie adeguate ai sensi dell’art. 46 del GDPR; (ii) assicurare che coloro i quali ricevono i dati siano vincolati contrattualmente almeno alle medesime obbligazioni del Responsabile ai sensi del Contratto; e (iii) rimanere interamente responsabile nei confronti del Titolare per ogni azione ed omissione di una terza parte.
4. garantire che i soggetti agenti sotto l’autorità del Responsabile, aventi accesso ai dati personali, (i) abbiano un vincolo giuridico raccolto per iscritto alla confidenzialità e alla riservatezza; (ii) non trattino i dati se non su indicazione e secondo le istruzioni del Responsabile.
5. rendere disponibile al Titolare tutte le informazioni necessarie a dimostrare il rispetto delle obbligazioni stabilite dal GDPR e permettere le attività di audit e di verifica, comprese le ispezioni, effettuate dal Titolare ai sensi del Contratto, contribuendo al corretto svolgimento delle stesse.
6. fornire al Titolare, su richiesta in forma scritta, un report avente ad oggetto le misure di sicurezza poste in essere per garantire il rispetto degli obblighi nei confronti del Titolare stesso. Tale report dovrà contenere i dettagli delle misure di sicurezza implementate e le caratteristiche in concreto dei trattamenti effettuati ai sensi del Contratto.
7. tenuta in considerazione la natura del trattamento e dei dati a disposizione per effettuarlo, assistere il Titolare nel garantire, in caso di esercizio dei diritti da parte dell'interessato, tutto il supporto necessario per adempiere alle attività in carico al Titolare e, in generale, il rispetto delle seguenti obbligazioni ai sensi del GDPR:
   1. ai sensi dell’art. 32 del GDPR, implementare adeguate misure tecniche e organizzative per assicurare un livello di sicurezza dell’informazione proporzionato al rischio, anche tenendo in considerazione lo stato dell’arte, i costi di implementazione, la natura, ambito applicativo e finalità dei trattamenti così come l’entità dei rischi per i diritti e le libertà delle persone fisiche;
   2. ai sensi degli artt. 33-34 del GDPR, supportare il Titolare nelle eventuali attività di notifica di una violazione di dati personali (data breach notification) all’Autorità di Protezione dei Dati competenti e agli interessati. A tale proposito, in via esemplificativa e non esaustiva, il Responsabile dovrà notificare al Titolare senza ritardo:
      1. ogni evento rilevante che abbia avuto ad oggetto il trattamento dei dati (ad es. accessi non autorizzati o tentativi in tal senso, circostanze di irregolarità o eventi che abbiano innalzato il rischio per i diritti degli interessati);
      2. ogni violazione di sicurezza dei propri sistemi IT;
      3. ogni tentativo di penetrare tali sistemi che potrebbe ragionevolmente compromettere la sicurezza dei dati personali;
      4. ogni atto o evento, a prescindere dall’identità dell’attore, che possa costituire una violazione delle istruzioni del Titolare, del Contratto, del presente atto di designazione ovvero della normativa in materia di protezione dei dati;
8. non effettuare copie di file, dati e documenti (indipendentemente dal supporto) di cui si è venuti in possesso in ragione dello svolgimento delle attività come dedotte nel Contratto, a meno che non sia necessario per lo svolgimento delle stesse. Inoltre, il Responsabile si obbliga a non alterare, modificare o intaccare in alcun modo i dati trattati a meno che ciò non sia necessario per lo svolgimento del contratto. Tutti i dati personali di cui il Responsabile entra in possesso in ragione del Contratto sono da considerarsi informazioni confidenziali, talvolta coperte dal segreto professionale, di conseguenza il Responsabile si obbliga a garantire la loro massima segretezza e confidenzialità, anche in ogni momento successivo al termine, per qualsiasi ragione, del rapporto contrattuale;
9. garantire che al termine del presente Contratto, i dati personali, in particolare per quanto riguarda la loro conservazione, restituzione e cancellazione finale, siano trattati secondo quanto ivi definito.

# **AMMINISTRATORI DI SISTEMA**

In riferimento ai sistemi e alle banche dati impiegate nelle operazioni di trattamento dei dati personali affidati, il Responsabile del trattamento – in ossequio al Provvedimento a carattere generale del 27 novembre del 2008 del Garante, recante “*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”* e successive modifiche e integrazioni – qualora applicabile – si obbliga a individuare ai sensi del citato Provvedimento i soggetti preposti quali Amministratori di Sistema e a valutarne le caratteristiche soggettive, accertando che sia prestata idonea garanzia circa il rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. L’elenco dei soggetti designati quali Amministratori di Sistema, comprensivo degli estremi identificativi e delle funzioni attribuite, dovrà essere costantemente aggiornato e conservato a cura del Responsabile e tenuto a disposizione del Titolare, il quale si riserva la facoltà di richiedere e ottenerne copia in qualsiasi momento.

In esecuzione del citato provvedimento, il Responsabile si obbliga inoltre ad adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) effettuati dagli Amministratori di Sistema. Tali registrazioni (*i.e.* *access log*) saranno conservate per un periodo non inferiore ai sei mesi e dovranno avere caratteristiche di completezza, inalterabilità e verificabilità della loro integrità adeguate a consentirne una completa verifica, e dovranno comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate.

Il Responsabile si obbliga altresì a sottoporre a verifica, con cadenza almeno annuale, l’operato degli Amministratori di Sistema in modo da controllarne e verificarne la rispondenza rispetto alle misure organizzative, tecniche e di sicurezza applicabili.

# **RICORSO AD UN ULTERIORE RESPONSABILE DA PARTE DEL FORNITORE**

Il Fornitore non potrà ricorrere ad un ulteriore responsabile del trattamento (di seguito, anche “Sub-responsabile”) senza aver precedentemente ottenuto autorizzazione scritta, specifica o generale, da parte del Titolare.

Nel caso di un’autorizzazione scritta generale, il Responsabile dovrà informare il Titolare di ogni richiesta di modifica che abbia ad oggetto l’aggiunta, la sostituzione o la rimozione di sub-responsabili, dando conseguentemente al Titolare l’opportunità di opporsi a tali modifiche.

Laddove il Responsabile sia autorizzato a ricorrere ad un Sub-responsabile per effettuare specifiche attività di trattamento per conto del Titolare, il Sub-responsabile dovrà essere soggetto contrattualmente alle medesime obbligazioni in materia di “data protection” assunte dal Responsabile nel Contratto. In particolare, il Sub-responsabile dovrà fornire sufficienti garanzie circa l’implementazione di adeguate misure di sicurezza tecniche ed organizzative, in modo da rispettare i requisiti imposti dal GDPR.

Nel caso in cui il Sub-responsabile risultasse inadempiente rispetto ai suoi obblighi in materia di “data protection”, il Fornitore rimarrà interamente responsabile nei confronti del Titolare, rispondendo per l’intero, per gli obblighi assunti dal Sub-responsabile.

1. **DIRITTI DEGLI INTERESSATI**

Il Responsabile dovrà notificare al Titolare senza indugio ogni richiesta di esercizio dei diritti che abbia ricevuto da parte degli interessati ai sensi della legislazione in materia di “data protection”.

Il Responsabile dovrà fornire assistenza al Titolare rispetto ad ogni richiesta effettuata dagli interessati, nei limiti in cui sia in grado di dare seguito, o comunque rispondere, a tale richiesta.

1. **COOPERAZIONE CON LE AUTORITÀ DI PROTEZIONE DEI DATI**

Le parti convengono che ogni Autorità Europea per la Protezione dei Dati avrà diritto di condurre un’ispezione o comunque attività di verifica nei confronti del Responsabile.

Il Responsabile si impegna a cooperare con l’Autorità e ad informare senza ritardo il Titolare dell’esistenza di attività ispettive.

Luogo e Data: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Il Titolare Il Responsabile

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(il Delegato del Rappresentante Legale) (Rappresentante Legale)

**APPENDICE 1 ALL’ATTO DI DESIGNAZIONE**

1. **Controlli**: Il Responsabile implementerà o sarà comunque responsabile per l’implementazione da parte di terzi delle misure appropriate finalizzate al raggiungimento di quanto segue:
   1. Negare l’accesso ai soggetti non autorizzati rispetto ad ogni dispositivo utilizzato per le attività di trattamento di dati personali (controllo di accesso ai dispositivi);
   2. Evitare la lettura, copia, alterazione, rimozione non autorizzate di dati personali (controllo dei supporti);
   3. Evitare accessi, modifiche o cancellazioni di dati personali conservati (controllo della conservazione);
   4. Evitare l’uso di sistemi di trattamento dati automatizzato da parte di soggetti non autorizzati (controllo delle utenze);
   5. Limitare l’accesso ai dati personali ai soli soggetti autorizzati a trattarli nei limiti temporali e sostanziali della propria autorizzazione (controllo di accesso ai dati);
   6. Verificare i canali di comunicazione dei dati;
   7. Permettere la verifica dell’identità dei soggetti che hanno inserito i dati in sistemi di trattamento automatizzato e della data e ora dell’inserimento (controllo degli input);
   8. Evitare la lettura, copiatura, alterazione o cancellazione di dati personali durante il trasferimento degli stessi o durante il trasporto dei supporti fisici (controllo del trasferimento);
   9. In caso di interruzione del servizio, permettere il ripristino dei sistemi installati al fine di effettuare le operazioni di trattamento dati (controllo sulle procedure di ‘recovery’);
   10. Assicurare che le funzioni e i sistemi utilizzati per trattare i dati personali siano in funzione, che eventuali errori o criticità vengano inseriti in appositi report e che i sistemi siano protetti dal danneggiamento dei dati in seguito a malfunzionamenti dei sistemi stessi.
2. **Personale**: il Responsabile adotterà misure idonee ad assicurare che nessun soggetto tratti i dati a meno che lo stesso:
   1. Sia competente e qualificato ad effettuare le specifiche mansioni assegnate;
   2. Sia stato autorizzato dal Responsabile; e
   3. Sia stato specificamente istruito dal Responsabile circa i requisiti rilevanti al fine di rispettare gli obblighi del Contratto, in particolare con riguardo alla limitazione delle finalità del trattamento.
3. **Controllo delle copie**: il Responsabile adotterà misure idonee ad assicurare che non siano effettuate copie dei dati personali all’infuori di quelle strettamente necessarie per dar corso agli obblighi contrattuali e di legge.
4. **Controllo sulle intrusioni**: il Responsabile adotterà misure idonee ad assicurare che i sistemi utilizzati a fini di trattamento dei dati personali siano soggetti al monitoraggio di eventuali attività intrusive non autorizzate, per mezzo di dispostivi riconosciuti in linea agli standard di settore.
5. **Gestione degli incidenti**: il Responsabile adotterà misure idonee ad assicurare che ai dati personali conservati si applichino le policy e le procedure in materia di gestione degli incidenti di sicurezza. Il Responsabile informerà senza ritardo il Titolare di ogni incidente di sicurezza, sospettato o effettivo, avente ad oggetto l’integrità dei dati personali.
6. **Sicurezza Fisica**: il Responsabile adotterà misure idonee ad assicurare che ogni area in cui sono conservati i dati personali sia soggetta a controlli di sicurezza fisica degli accessi.
7. **Crittografia**: il Responsabile adotterà misure idonee ad assicurare che in caso di trasferimenti di dati personali siano utilizzati meccanismi di crittografia in linea con gli standard di settore generalmente accettati.
8. **Sicurezza Logica**: il Responsabile adotterà misure idonee ad assicurare che ogni software in cui sono conservati dati personali sia soggetto a controlli di sicurezza degli accessi.
9. **Modifiche e aggiornamenti dei sistemi**: Il Responsabile dovrà aggiornare e mantenere le misure di sicurezza durante l’intera durata delle prestazioni dedotte nel Contratto. A tali fini, potranno essere aggiunti o modificati controlli di sicurezza, procedure, policy e caratteristiche dei sistemi. Il Responsabile dovrà fornire un livello di sicurezza che non sia mai sostanzialmente inferiore rispetto a quello fornito *ab initio* del rapporto contrattuale.