**Allegato I**

**Nomina di Responsabile del trattamento di dati personali**

**Ai sensi dell’art. 28 del GDPR - General Data Protection Regulation**

La società Acquirente Unico S.p.A. con sede in Roma, in Via Guidubaldo del Monte n. 45 (di seguito anche la “**Società**” o il “**Titolare**”), in persona legale rappresentante *pro tempore*, in relazione al contratto n. \_\_\_\_\_\_\_\_\_\_\_ affidato alla Società \_\_\_\_\_\_\_\_\_\_\_\_ (d’ora innanzi, il ”**Contratto**”), concernente \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (di seguito l’ ”**Attività**”), con la presente lettera

**Nomina**

La Società \_\_\_\_\_\_\_\_\_\_\_\_\_\_ in persona del proprio legale rappresentante pro tempore, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, con sede in \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI** (di seguito il “**Responsabile**”)

nell’ambito del rapporto contrattuale instaurato con il Titolare in virtù del Contratto.

La presente nomina di Responsabile del trattamento di dati personali (di seguito la “**Nomina**”) è efficace a partire dalla data di protocollo del Contratto tra la Società e il Responsabile.

Le incombenze e le responsabilità oggetto della presente lettera di Nomina vengono affidate al Responsabile sulla base delle dichiarazioni dallo stesso fornite alla Società (e della successiva verifica da parte della Società, per quanto ragionevolmente possibile, della loro rispondenza al vero) circa le caratteristiche di esperienza, capacità e affidabilità che vengono richieste dalla legge (artt. 28 GDPR) per chi esercita la funzione di Responsabile del trattamento. Con la sottoscrizione della presente lettera, il Responsabile si dichiara disponibile e competente per la piena attuazione di quanto ivi disposto, accetta la Nomina, conferma la diretta ed approfondita conoscenza degli obblighi che assume in relazione al dettato del GDPR, conferma, altresì, di disporre di una propria organizzazione che dichiara idonea a consentire il trattamento dei dati nel pieno rispetto delle prescrizioni legislative, ivi compreso il profilo della sicurezza, e si impegna a procedere al trattamento dei dati personali attenendosi alle istruzioni impartite nel pieno rispetto di quanto imposto dall’art. 28, lettera a) del GDPR.

Nei limiti delle proprie competenze e attribuzioni, il Responsabile dovrà garantire l’osservanza degli obblighi di legge, sempre conformemente alle direttive e sotto la vigilanza del Titolare.

Onde consentire al Responsabile di espletare i compiti e le attribuzioni meglio specificati in seguito, con la presente lettera di Nomina vengono fornite le specifiche istruzioni per l’assolvimento del compito assegnato.

1. Definizioni. I seguenti termini utilizzati nella presente Nomina avranno i seguenti significati:
	* + 1. "**Normativa applicabile**": l’insieme delle norme rilevanti in materia di privacy alle quali il Titolare è soggetto incluso il Regolamento europeo 2016/679 in materia di protezione dei dati personali (General Data Protection Regulation e il D.Lgs. 101/2018 di adeguamento della normativa nazionale al Regolamento europeo (di seguito, unitamente “**GDPR**”), nonché in ogni tempo, ogni linea guida, norma di legge, codice o provvedimento rilasciato o emesso dagli organi competenti o da altre autorità di controllo, ivi inclusi i Provvedimenti del Garante per la protezione dei dati personali che resteranno in vigore.
			2. "**Titolare del trattamento**", "**responsabile del trattamento**", "**interessato**", "**dati personali**" e "**trattamento**" hanno il significato dato dalla Normativa applicabile.
			3. **“Misure tecniche e organizzative di sicurezza”:** sono le misure intese a proteggere i dati personali dalla distruzione accidentale o illegale o dalla perdita, alterazione, divulgazione o accesso non autorizzato, in particolare quando il trattamento comporta la trasmissione di dati su una rete, come previste dalla Normativa applicabile all’art. 32 GDPR e tutte le ulteriori misure tecniche ed organizzative necessarie a garantire un livello di sicurezza adeguato al rischio, tenuto conto della natura, dell’oggetto, del contesto e delle finalità del trattamento posto in essere, come del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Queste misure dovranno includere:

-la pseudonimizzazione e la cifratura dei dati personali;

-la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

-la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

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

* + - 1. **“Data breach”**: si intende l’ipotesi in cui si verifica una violazione dei dati personali secondo l’art. 33 GDPR.
			2. **“Garante”**: si intende l’autorità competente responsabile per la protezione dei dati.
			3. **“Sub-responsabile/i”:** si intende qualsiasi responsabile del trattamento incaricato dal (i) Responsabile o (ii) da qualsiasi altro "sub-responsabile" di trattare dati personali per conto del Responsabile, sempre in conformità alle istruzioni del Titolare.
1. Misure tecniche ed organizzative - Audit e diritti di verifica del Titolare del Trattamento

Il Responsabile del Trattamento si obbliga ad adottare ed implementare le Misure tecniche ed organizzative di sicurezza, oltre a quanto previsto dall’art. 4, numero 8, con l’obbligo di documentarle se richiesto dal Titolare del Trattamento.

Il Titolare si riserva la facoltà di effettuare, nei modi ritenuti più opportuni, anche tramite l’invio presso i locali del Responsabile di propri funzionari a ciò delegati, o tramite l’invio di apposite check list, verifiche tese a vigilare sulla puntuale osservanza delle disposizioni di legge e delle presenti istruzioni.

In alternativa a quanto sopra precisato, il Responsabile può fornire al Titolare copie delle relative certificazioni esterne (es. ISO 27001: 2013, SSAE 16 ecc.), audit report e/o altra documentazione sufficiente per il Titolare a verificare la conformità del Responsabile alle Misure tecniche e organizzative di sicurezza della presente Nomina.

1. Correzioni, cancellazione o blocco di dati

Il Responsabile può solamente correggere, cancellare o bloccare il trattamento dei dati personali a beneficio del Titolare del Trattamento e quando ha avuto istruzioni dal Titolare del Trattamento in tal senso. Se l’interessato fa richiesta direttamente al Responsabile del Trattamento per la correzione o la cancellazione dei propri dati personali, il Responsabile deve indirizzare la predetta richiesta al Titolare del Trattamento senza ritardo alcuno.

Alla scadenza della Nomina il Responsabile si obbliga a restituire al Titolare del trattamento tutti i dati in suo possesso.

1. Istruzioni generali del Responsabile del Trattamento

Il Responsabile, sebbene non in via esaustiva, avrà i compiti e le attribuzioni di seguito elencate, oltre agli ulteriori obblighi previsti al successivo articolo 5, e dunque dovrà:

1. effettuare la ricognizione delle banche dati, degli archivi (cartacei e non) relativi ai trattamenti effettuati in esecuzione dell’Attività;
2. tenere un registro, come previsto dall’art. 30 del GDPR, in formato elettronico, di tutte le categorie di attività relative al trattamento svolte per conto della Società, contenente:
* il nome e i dati di contatto del Responsabile e del Titolare e, laddove applicabile, del Responsabile della protezione dei dati;
* le categorie dei trattamenti effettuati per conto del Titolare;
* ove applicabile, i trasferimenti di dati personali verso un paese non appartenente all’Unione Europea, compresa l’identificazione di tale paese e, per i trasferimenti di cui al secondo comma dell’art. 49 del GDPR, la documentazione delle garanzie adeguate;
* ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate;
1. organizzare le strutture, gli uffici e le competenze necessarie e idonee a garantire il corretto espletamento dell’Attività;
2. astenersi dal contattare i nominativi trattati attraverso l’Attività così come dal trattarli per finalità proprie;
3. non diffondere o comunicare a terzi i dati trattati attraverso l’Attività;
4. garantire l'affidabilità di qualsiasi dipendente che accede ai dati personali del Titolare ed assicurare, inoltre, che gli stessi abbiano ricevuto adeguate istruzioni e formazione (quali incaricati del trattamento) con riferimento alla protezione e gestione dei dati personali, e che siano vincolati al rispetto di obblighi di riservatezza non meno onerosi di quelli previsti nella presente Nomina;
5. tenere i dati personali trattati attraverso l’Attività e di cui è titolare la Società separati rispetto a quelli trattati per conto di altre terze parti, sulla base di un criterio di sicurezza di tipo logico;
6. adottare le Misure tecniche ed organizzative di sicurezza, come previste al precedente articolo 2;
7. procedere alla nomina del proprio/i amministratore/i di sistema, in adempimento di quanto previsto dal provvedimento del Garante del 27.11.08, pubblicato in G.U. n. 300 del 24.12.2008, ove ne ricorrano i presupposti, comunicandolo prontamente al Titolare, curando, altresì, l’applicazione di tutte le ulteriori prescrizioni contenute nel suddetto provvedimento;
8. assistere tempestivamente il Titolare con misure tecniche e organizzative adeguate, al fine di soddisfare l’obbligo del Titolare di procedere ad un DPIA (Valutazione di impatto sulla protezione dei dati) ex art. 35 e ss del GDPR, con obbligo di notifica quando venga a conoscenza di un trattamento di dati che possa comportare un rischio elevato;
9. assistere il Titolare nel garantire il rispetto degli obblighi di cui agli artt. 32-36 GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile e garantire l’esercizio del diritto alla portabilità dei dati personali trattati attraverso l’Attività, ai sensi dell’art. 20 del GDPR, assicurando che gli stessi possano essere trasmessi in un formato strutturato, di uso comune e leggibile da qualsiasi dispositivo automatico;
10. notificare alla Società, senza ingiustificato ritardo e comunque non oltre le 24 ore da quando ne abbia avuto conoscenza, ai sensi dell’art.33 del GDPR, nel caso in cui si verifichi un *Data breach* anche presso i propri Sub-responsabili; la notifica deve contenere tutti i requisiti previsti dall’art. 33, 3° comma del GDPR (la natura delle violazioni, gli interessati coinvolti, le possibili conseguenze e le nuove misure di sicurezza implementate). Dovrà, inoltre, adottare, di concerto con la Società, nuove misure di sicurezza atte a circoscrivere gli effetti negativi dell’evento e a ripristinare la situazione precedente;
11. predisporre e aggiornare un registro che dettagli, in caso di eventuali *Data breach*, la natura delle violazioni, gli interessati coinvolti, le possibili conseguenze e le nuove misure di sicurezza implementate;
12. astenersi dal trasferire i dati personali trattati per conto della Società al di fuori dello Spazio Economico Europeo senza il previo consenso scritto della Società;
13. avvertire prontamente la Società, entro tre (3) giorni lavorativi, in merito alle eventuali richieste degli interessati che dovessero pervenire al Responsabile inviando copia delle istanze ricevute all’indirizzo e-mail: legale@acquirenteunico.it e collaborare al fine di garantire il pieno esercizio da parte degli interessati di tutti i diritti previsti dalla Normativa applicabile;
14. adottare adeguati processi e ogni altra misura tecnica idonea ad attuare le istruzioni fornite dal Titolare, incluse
	* 1. le procedure idonee a garantire il rispetto dei diritti e delle richieste formulate al Titolare dagli interessati relativamente ai loro dati personali, come indicato al precedente punto 15;
		2. l’adozione di adeguate interfacce o sistemi di supporto che consentano di garantire e fornire informazioni agli interessati così come previsto dalla Normativa applicabile;
		3. procedure atte a garantire l’aggiornamento, la modifica e la correzione, su richiesta del Titolare, dei dati personali di ogni interessato;
		4. procedure atte a garantire la cancellazione o il blocco dell’accesso ai dati personali a richiesta del Titolare;
		5. misure che consentano di contrassegnare i dati personali o gli account, per consentire al Titolare di poter applicare particolari regole ai dati personali dei singoli interessati; il Responsabile, dietro richiesta scritta del Titolare, collaborerà con questo per garantire il diritto degli interessati alla portabilità dei dati e di limitazione di trattamento;
15. avvisare immediatamente, e comunque entro tre (3) giorni lavorativi, il Titolare del trattamento, di qualsiasi richiesta o comunicazione da parte dell’Autorità Garante o di quella Giudiziaria eventualmente ricevuta inviando copia delle istanze all’indirizzo e-mail: legale@acquirenteunico.it per concordare congiuntamente il riscontro;
16. predisporre idonee procedure interne finalizzate alla verifica periodica della corretta applicazione e della congruità degli adempimenti posti in essere ai sensi della Normativa applicabile, attuate in accordo con il Titolare anche in applicazione delle Misure tecniche e organizzative di sicurezza;
17. mantenere un costante aggiornamento sulle prescrizioni di legge in materia di trattamento dei dati personali, nonché sull’evoluzione tecnologica di strumenti e dispositivi di sicurezza, modalità di utilizzo e relativi criteri organizzativi adottabili;
18. garantire la stretta osservanza dell’incarico ricevuto, escludendo qualsiasi trattamento o utilizzo dei dati personali non coerente con gli specifici trattamenti svolti in adempimento dell’incarico medesimo;
19. rispettare la Normativa applicabile e adempiere gli obblighi previsti dalla presente Nomina in modo da evitare che il Titolare incorra nella violazione di un qualunque obbligo previsto dalla Normativa applicabile;
20. ottemperare tempestivamente alle richieste del Titolare;
21. inviare tutte le comunicazioni al Titolare previste nel presente atto all’indirizzo soprariportato o a quello diverso che verrà eventualmente comunicato;
22. prima di iniziare il trattamento e, ove occorra, in qualsiasi altro momento, informare il Titolare se, a suo parere:
23. una qualsiasi istruzione fornita dal Titolare si pone in violazione di legge;
24. il Responsabile è soggetto al rispetto di previsioni di legge, che potrebbero rendere per lo stesso, in tutto o in parte, impossibile o illegale agire conformemente alle istruzioni impartite da Titolare o nel rispetto di quanto previsto dalla Normativa applicabile.
25. Ulteriori obblighi del Responsabile

Il Responsabile del trattamento, compatibilmente con quanto previsto dalla presente Nomina ed in conformità con le previsioni dell’art.28 del GDPR, sarà altresì soggetto al seguente obbligo di riservatezza; a tal fine ogni persona che abbia accesso ai dati personali appartenenti al Titolare del trattamento, sotto i termini della presente Nomina, si impegna a mantenere la riservatezza e deve essere informata di qualsiasi speciale necessità derivante dalla predetta Nomina e della limitazione d’uso a specifici scopi. Se i dati personali relativi alla Società vengono conservati, trattati o usati come parte della presente Nomina, le persone coinvolte nel trattamento saranno obbligate a mantenere l’obbligo di riservatezza.

1. Sub-responsabili
2. **Sub-responsabili autorizzati.** I Sub-responsabili autorizzati dal Titolare, a decorrere dalla data effettiva del presente Contratto, sono elencati all’Allegato 1 della stessa.
3. **Designazione di nuovi Sub-responsabili.** Seil Responsabile desidera incaricare nuovi Sub-responsabili, in aggiunta a quelli di cui al punto precedente, deve chiedere la relativa autorizzazione alla Società.
4. **Obblighi verso il Sub-responsabile**. Nel momento in cui il Titolare autorizza l’incarico di uno o più Sub-responsabili, il Responsabile:
5. limiterà l'accesso del Sub-responsabile ai dati personali a quanto strettamente necessario per soddisfare gli obblighi del Responsabile ai sensi del Contratto; al Sub-responsabile sarà vietato l'accesso ai dati personali per qualsiasi altro scopo;
6. imporrà per iscritto ad ogni Sub-responsabile il rispetto di obbligazioni ed istruzioni equipollenti a quelle previste nel presente Contratto nella sua totalità, nonché la possibilità di effettuare audit;
7. rimarrà pienamente responsabile nei confronti del Titolare per il rispetto degli obblighi derivanti dal presente Contratto per qualsiasi atto o omissione del Sub-responsabile che comporti una violazione degli stessi.

Il Sub-appalto nel significato della presente disposizione, non include servizi ausiliari richiesti dal Responsabile del trattamento da terze parti per assisterli nell’esecuzione dell’appalto. Questi possono essere ad esempio servizi di telecomunicazione, manutenzione e supporto agli utenti (se non è possibile l’accesso ai dati personali da parte del Titolare del trattamento), la pulizia, il controllo o l’eliminazione dei dati multimediali. Tuttavia, il Sub-appalto relativo all’eliminazione di documenti/dati multimediali deve essere comunicato al Titolare del trattamento se l'attività principale del trattamento commissionato comporta l'eliminazione di documenti/ dati multimediali. Per salvaguardare la protezione e la sicurezza dei dati personali del Titolare del trattamento, anche quando i servizi ausiliari sono resi da terze parti, il Responsabile del trattamento comunque stipula accordi contrattuali adeguati e legittimi e intraprende attività di monitoraggio.

1. Responsabilità

Il Responsabile tiene indenne e manlevata il Titolare (e ciascuno dei suoi rispettivi dipendenti e agenti) da ogni perdita, costo, spesa, multa e/o sanzione, danno e da ogni responsabilità di qualsiasi natura (sia essa prevedibile, contingente o meno) derivante da o in connessione con una qualsiasi violazione da parte del Responsabile degli obblighi della Normativa applicabile o delle disposizioni contenute nella presente Nomina. In particolare, il Responsabile tiene indenne il Titolare da qualsiasi perdita derivante: (a) da qualsiasi violazione (i) dei termini della presente Nomina o (ii) della Normativa applicabile, anche da parte di ogni Sub-Responsabile di cui si avvale; o (b) dalla subfornitura o all’esternalizzazione di qualsiasi Trattamento affidato a terzi soggetti.

1. Miscellanea

I dati personali devono essere trattati ed utilizzati esclusivamente nel territorio di uno Stato Membro dell’Unione Europea (EU) o di altro firmatario della presente Nomina nell’Area Economica Europea (AEE).

Il Responsabile non avrà diritto di rimborso delle eventuali spese che lo stesso potrebbe dover sostenere per essersi attenuto alle istruzioni impartite da Titolare per lo svolgimento dell’Attività, e/o di un qualsiasi altro suo obbligo previsto dalla Nomina.

1. Durata - Legge e foro competente

La Nomina decorre dalla data della sua sottoscrizione e rimarrà in vigore sino alla risoluzione oi scadenza del Contratto o cessazione dei servizi da eseguirsi in relazione all’Attività.

La presente Nomina o qualsiasi reclamo, pretesa o rivendicazione derivante da essa o in relazione ai soggetti della presente Nomina deve esser governata dalla Legge italiana. Si stabilisce la competenza esclusiva del Tribunale di Roma per qualsiasi controversia derivante dalla presente Nomina.

Le parti stabiliscono le seguenti persone di contatto per l’esecuzione della Nomina:

Per il Titolare del Trattamento: \_\_\_\_\_\_\_\_\_\_

Per il Responsabile del Trattamento: \_\_\_\_\_\_\_\_\_\_\_\_

Qualsiasi modifica relativa le sopramenzionate persone o la responsabilità delle persone di contatto deve essere immediatamente notificata all’altra parte.

\*\*\*

Sottoscrivendo la presente Nomina per accettazione, il Responsabile dichiara di aver compiutamente e analiticamente esaminato i trattamenti gestiti dalla Società e di averli trovati non in contrasto con le disposizioni della Normativa applicabile.

In particolare, il Responsabile dichiara di aver verificato che le finalità e le modalità di tali trattamenti sono legittimi e tali il Responsabile s'impegna a mantenerli nel tempo nell'espletamento delle proprie attività.

Distinti Saluti,

Il Titolare del Trattamento

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

Il Responsabile, per conferma e accettazione

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

\*\*\*

Allegato 1: Elenco dei Sub-Responsabili autorizzati

**ALLEGATO 1**

**Elenco dei Sub-responsabili autorizzati**

|  |  |  |
| --- | --- | --- |
| **Sub-responsabile**  | **Sede e dati di contatto / Luogo del trattamento** | **Attività di trattamento** |
|  |  |  |
|  |  |  |