CONTRATTO DI COLLABORAZIONE PROFESSIONALE
CIG: ZBE356A9CA

TRA

CIVITAVECCHIA SERVIZI PUBBLICI S.R.L., con sede legale in Civitavecchia, Via delle Terme di Traiano 42, codice fiscale e partita IVA n. 14105271002, in persona del Presidente e legale rappresentante *pro-tempore* Avv. Fabrizio Lungarini, qui di seguito brevemente indicata anche quale **"Cliente",**

E

DOTT. CARLO ROMANO

indicato quale **"Consulente".**

PREMESSO CHE

- con delibera del Cda del 17/07/2018 è stato approvato il "Modello di organizzazione, gestione e controllo della Società Civitavecchia Servizi Pubblici S.r.l." di cui al D.Lgs. 231/2001;
- è stato deciso di optare per la composizione monocratica dell'organismo di vigilanza, da selezionare tramite un avviso pubblico finalizzato alla raccolta di manifestazioni d'interesse da parte di professionisti di comprovata esperienza per l'incarico monocratico di Organismo di Vigilanza.
- il consulente si è dichiarato disponibile a formalizzare un rapporto di collaborazione generale, da espletarsi come consulenza con carattere continuativo;
- che CIVITAVECCHIA SERVIZI PUBBLICI S.R.L. in data 28.02.2022 con verbale di gara n. 2 ha determinato di approvare l'affidamento diretto *ex* art. 1, comma 2 lett. a) L. 120/20 come sostituita dall'art. 51, comma 1, lettera a), sub. 2.1), legge 108/21], in favore del professionista, all'esito di avviso pubblico di manifestazione di interesse pubblicato il 29.10.2021;
- Il consulente, del quale la cliente ha acquisito il curriculum vitae e valutato l'esperienza, risulta iscritto all'Ordine dei Commercialisti di Roma;

Tutto ciò premesso, che forma parte integrante e sostanziale del presente contratto, nonché suo presupposto logico e giuridico, tra le suddette pari, si conviene e si stipula quanto segue:

ARTICOLO 1
OGGETTO DEL CONTRATTO

1.1 Il consulente, anche attraverso propri collaboratori, colleghi e/o consulenti dei quali si assumerà gli eventuali costi, si impegna a prestare, a favore della cliente, **assistenza professionale**, con carattere continuativo, afferente l'incarico, avente natura di prestazione d'opera intellettuale, in ottemperanza alle disposizioni di cui al D.Lgs. 231/2001, art. 6, lett. b), ovvero l'espletamento di tutte

le attività di vigilanza sul funzionamento, l'aggiornamento e l'osservanza del "Modello di organizzazione, gestione e controllo" ("Modello 231").

L'incarico oggetto della presente manifestazione di interesse è di tipo fiduciario.

In particolare, il professionista avrà il compito:

- di vigilare sull'effettività del Modello;
- di verificare l'adeguatezza del Modello, ossia la sua efficacia nel prevenire i comportamenti illeciti;
- di verificare il mantenimento, nel tempo, dei requisiti di solidità e funzionalità del Modello e promuovere il necessario aggiornamento, nell'ipotesi in cui le analisi rendano necessario effettuare correzioni e adeguamenti;
- di assicurare i flussi informativi di competenza

Su un piano più specificamente operativo, all'OdV saranno affidati i seguenti compiti:

- assicurare il mantenimento e l'aggiornamento del sistema di identificazione, mappatura e classificazione delle aree di rischio ai fini dell'attività di vigilanza;
- attivare le procedure di controllo previste dal Modello, effettuando verifiche (periodiche e a campione) sulle aree a rischio;
- controllare la regolare tenuta della documentazione richiesta dal Modello;
- promuovere e assicurare l'elaborazione di direttive e i contenuti dei flussi informativi verso l'Organismo di Vigilanza;
- segnalare alla Direzione Aziendale le violazioni del Modello e monitorare l'applicazione delle sanzioni disciplinari;
- promuovere e monitorare le iniziative per la diffusione della conoscenza del Modello, nonché per la formazione del personale e la sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello;
- elaborare le risultanze delle attività effettuate e la relativa reportistica.

Il professionista sarà tenuto ad aggiornare ed informare su base continuativa il Consiglio di Amministrazione in merito all'attuazione del Modello e all'emersione di eventuali aspetti critici: controlli effettuati ed esito, eventuale necessità di aggiornamento del Modello, sanzioni disciplinari applicate;

1.2 Nello specifico, il consulente fornirà la propria assistenza a supporto del Consiglio di Amministrazione e della Direzione Aziendale di CIVITAVECCHIA SERVIZI PUBBLICI S.R.L. o anche attraverso personale dagli stessi formalmente delegato, che rappresenteranno di volta in volta al consulente le problematiche da esaminare.
1.3. Il consulente potrà, comunque, utilizzare la struttura organizzativa del cliente e potrà contare, presso gli uffici sociali, sull'opera dei collaboratori facenti parte dell'organico del cliente ed a spese dello stesso cliente.

ARTICOLO 2
RAPPRESENTANZA, RISERVATEZZA ED OBBLIGHI DELLE PARTI

2.1. L'attività del "Consulente" sarà svolta nell'interesse e per conto del "Cliente", senza tuttavia dover o poter rendere dichiarazioni impegnative nei confronti di terzi in nome del "Cliente" stesso se non esplicitamente autorizzato.
2.2. Oltre che nel rispetto dei principi generali dettati dal Codice Civile (Libro V, Titolo III, artt. da 2222 a 2238) e delle regole di comportamento (codice deontologico professionale) che disciplinano la materia, l'attività del "Consulente" dovrà essere espletata con diligenza, correttezza, professionalità - con particolare riguardo ai tempi e termini di realizzazione delle singole pratiche - e con riservatezza, con l'impegno a non divulgare notizie inerenti i rapporti in essere ed intercorsi con il "Cliente" e tra il "Cliente" e terzi, mantenendo riservati i nominativi di questi ultimi, i metodi di lavoro e la struttura organizzativa del "Cliente".
2.3. Il Cliente ha l'obbligo di mettere a conoscenza e far pervenire tempestivamente al Consulente tutta la documentazione e le informazioni necessarie all'espletamento dell'incarico.

ARTICOLO 3
DURATA DEL CONTRATTO

Il presente incarico avrà durata di 36 mesi dalla sottoscrizione (28.02.2025), salva l'interruzione per gravi motivi e sempre che la stessa non abbia a pregiudicare il regolare svolgimento del lavoro.

ARTICOLO 4
COMPENSI E SPESE

4.1. Il Consulente, valutato altresì il grado di complessità dell'incarico e tenuto conto degli oneri ipotizzabili fino alla conclusione dello stesso, concorda con il Cliente, per le prestazioni professionali indicate all'articolo 1 del presente contratto, un compenso omnicomprensivo di € 7.000,00 (settemila,00) annui, oltre accessori di legge.
4.2. Tutte le spese che il "Consulente" dovesse sopportare nell'esecuzione del presente contratto resteranno a carico dello stesso.
4.3. I pagamenti dovranno essere effettuati da parte del "Cliente" a fine mese dalla data di emissione detta fattura o del preavviso di parcella.
4.4. Tutte le eventuali prestazioni accessorie a quelle oggetto del presente contratto rese dai "Consulente" non potranno comunque comportare diritto ad ulteriori compensi, dovendosi intendere ricomprese nei compensi come sopra determinati.

ARTICOLO 5
EFFETTI DELLA CESSAZIONE DEL CONTRATTO

In caso di cessazione, a qualsiasi titolo, del presente contratto si conviene quanto segue: il Consulente dovrà restituire al Cliente tutto il materiale contrattuale, gli elaborati, i documenti e gli atti. I compensi maturati a favore del Consulente verranno fatturati contestualmente alla data di cessazione del rapporto.

ARTICOLO 6
CONDIZIONI DI INCOMPATIBILITÀ

6.1. Il Consulente dichiara formalmente di impegnarsi ad esercitare il mandato con il massimo zelo e scrupolo professionale, nel pieno rispetto delle norme di legge e delle disposizioni deontologiche che

regolano la professione nonché di non avere ragioni di incompatibilità con l'assunzione del presente incarico.
6.2. Il Consulente si impegna a comunicare tempestivamente alla Cliente l'insorgere di eventuali condizioni di incompatibilità.

ARTICOLO 7
CONTROVERSIE

7.1. Per quanto non previsto dal presente contratto, le parti rinviano alle norme del codice civile ed a quelle proprie dell'Ordinamento professionale dei commercialisti.
7.2. La sottoscrizione del presente disciplinare d'incarico costituisce accettazione integrale delle condizioni e delle modalità in esso contenute o richiamate.
7.3. Eventuali controversie tra la Cliente ed il Consulente saranno devolute, previo un obbligatorio tentativo di conciliazione da svolgersi presso l'Organismo di Mediazione dell'Ordine dei Commercialisti di Civitavecchia, al Tribunale di Civitavecchia.
7.4. E' escluso il ricorso a Fori alternativi.

ARTICOLO 8
POLIZZA ASSICURATIVA

Si dà atto che il Consulente è attualmente assicurato per la responsabilità civile contro i rischi professionali con apposita polizza n.50 15437TB SARA ASSICURAZIONI S.p.A., massimale 1.500.000,00 di euro, e con scadenza il 20/08/2022, che si impegna a rinnovare alla scadenza e a tenere attiva per tutta la durata dell'incarico o a sostituire con altra analoga.

ARTICOLO 9
COMUNICAZIONI

Qualunque comunicazione da farsi in merito al presente contratto dovrà essere inviata a mezzo P.E.C. ai seguenti riferimenti:

Quanto alla Committente:

CIVITAVECCHIA SERVIZI PUBBLICI S.R.L.

Via Terme di Traiano 42

00053 CIVITAVECCHIA (RM)

Pec: civitavecchiaservizipubblicisrl@legalmail.it

RUP: ing. Fernando Ferluga cell 348 1549238

Quanto al Consulente:

dott. Carlo Romano

PEC: carlo.romano@legalmail.it

ARTICOLO 10

NEGOZIAZIONE E ACCETTAZIONE DELL'ACCORDO

Le parti si danno reciprocamente atto di avere dettagliatamente negoziato il presente Accordo e ciascuna clausola del medesimo, e che il presente Accordo è frutto della libera determinazione negoziale di ciascuna delle parti, in assenza di qualsiasi imposizione dell'una parte sull'altra.

ARTICOLO 11

SOSTITUZIONE DI ACCORDI PRECEDENTI E FORMA SCRITTA

La sottoscrizione del presente Accordo fa cessare ed annulla qualsiasi precedente intesa o rapporto eventualmente intercorso fra le parti.

Eventuali modifiche alle previsioni di cui al presente Accordo saranno validi e vincolanti tra le Parti solo se effettuate per iscritto e da queste debitamente sottoscritte.
Il presente contratto sarà registrato solamente in caso d'uso ai sensi dell'art. 5, comma 2 del D.P.R. 131/1986 e relative spese saranno a carico della parte che ne farà richiesta.

ARTICOLO 12

ULTERIORI DISPOSIZIONI INERENTI IL TRATTAMENTO DEI DATI

PREMESSO CHE

- *in virtù del rapporto professionale e/o del contratto di servizio stipulato tra il Cliente e il Fornitore in data 25 febbraio 2021, quest'ultimo si assume l'obbligo di fornire al Cliente le prestazioni pattuite (di seguito i "Servizi");*
- *la prestazione dei Servizi può di volta in volta comportare l'accesso del Fornitore o la comunicazione a quest'ultimo di informazioni del Cliente configurabili quali dati personali ai sensi del Regolamento (UE) 2016/679 del Consiglio e del Parlamento Europeo del 27 Aprile 2016 sulla protezione e la libertà di circolazione dei dati personali delle persone fisiche (di seguito "GDPR") e da ulteriori disposizioni e leggi applicabili in materia di protezione dei dati;*
- *le Parti convengono che i trasferimenti dei dati disciplinati dal presente contratto rientrano nell'ambito di applicazione dell'articolo 28 del GDPR e che il Fornitore si qualifica quale responsabile del trattamento ai sensi del GDPR, nonché è intenzione delle Parti di utilizzare il contratto quale accordo contrattuale per disciplinare il trattamento dei dati;*
- *il Fornitore è stato individuato tra soggetti che presentano 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 dell'interessato, così come previsto dall'art. 28, par. 1, GDPR;*
- *le Parti dichiarano:*

  - che l'oggetto del trattamento è l'assistenza legale in materia di affidamenti ed appalti pubblici al titolare;

  che la finalità del trattamento è unicamente la corretta e completa esecuzione delle attività descritte nel "Contratto di affidamento incarico professionale consulenza legale", limitato ai soli fini degli obbiettivi di tutela, consulenza e difesa del Titolare, sottoscritto tra le parti;

  - che i dati personali trattati riguardano le seguenti categorie: dati personali, dati identificativi, tra cui:

- ✓ *dati comuni, ad es. nome, cognome, ragione sociale, indirizzo ecc.;*
- ✓ *ulteriori dati di contatto quali il numero di telefono, l'indirizzo di posta elettronica.;*

- che i dati personali trattati riguardano, altresì, le seguenti categorie speciali:

- ✓ *origine etnica e razziale;*
- ✓ *opinioni politiche;*
- ✓ *convinzioni religiose o filosofiche;*
- ✓ *appartenenza a sindacati;*
- ✓ *dati genetici;*
- ✓ *dati relativi alla salute o la vita sessuale o l'orientamento sessuale;*
- ✓ *dati personali inerenti a reati, condanne penali e relative misure di sicurezza;*

- che i dati personali trattati riguardano le seguenti categorie di soggetti interessati: dipendenti, collaboratori, clienti/utenti, fornitori del Titolare.

i quali hanno diritto di esercitare quanto previsto dal GDPR, dalle vigenti disposizioni aventi valore di legge e dagli specifici accordi e limitazioni che ciascuno possa avere legittimamente posto o porrà in essere nel corso od anche successivamente al rapporto;

- *le Parti concordano di sostituire ogni eventuale precedente atto di nomina con il presente contratto di nomina a Responsabile del trattamento dei dati personali.*

Tutto ciò premesso e considerato, al fine di prestare garanzie sufficienti sulla tutela della vita privata, delle libertà e dei diritti fondamentali delle persone fisiche circa il trasferimento dal Titolare al Responsabile dei dati personali che potrà avvenire in virtù del rapporto professionale e/o del contratto di servizi in essere, le Parti convengono quanto segue:

1. *le Parti concordano che, ai sensi della normativa applicabile, il Cliente è il solo titolare del trattamento dei dati che saranno messi a disposizione del Fornitore ai fini dell'esecuzione del contratto scaturente dal rapporto professionale e/o del contratto di servizi (i "Dati condivisi") e, di conseguenza, che quest'ultimo svolgerà i trattamenti connessi all'adempimento dei Servizi esclusivamente nella veste di responsabile qui espressamente conferita dal Titolare;*
2. *con la sottoscrizione del presente accordo, il Fornitore accetta la designazione quale responsabile del trattamento e conferma di possedere i requisiti di esperienza, capacità ed affidabilità richiesti dalla Normativa privacy, essendo in grado dunque di mettere in atto, tra l'altro, misure tecniche e organizzative adeguate a garantire che i trattamenti dei Dati condivisi saranno eseguiti in conformità ai principi di legge, con particolare riferimento alla tutela dei diritti degli interessati. Tenuto conto che le tecniche di protezione dei Dati personali, su ogni tipo di supporto, sono e saranno in continua evoluzione, le misure e raccomandazioni riportate in questo accordo contrattuale devono necessariamente interpretarsi in maniera dinamico-evolutiva;*
3. *il Fornitore si impegna ad osservare – e a fare in modo che tutti coloro che agiscono sotto la propria direzione a loro volta rispettino – gli obblighi stabiliti dalla normativa vigente in materia di protezione dei dati personali e, in particolare, a fare quanto segue:*

   a) *svolgere esclusivamente le operazioni di trattamento delegate da parte del Titolare e, per l'effetto, non utilizzare i Dati condivisi per finalità diverse da quelle collegate alla sola esecuzione del presente Contratto e del rapporto professionale e/o del contratto di servizi in essere tra le Parti;*

   b) *trattare i Dati condivisi in piena conformità alle istruzioni qui fornite da parte del Titolare, o di quelle ulteriori che quest'ultima dovesse in un secondo momento ritenere opportuno fornire per la migliore e più efficiente esecuzione dei Servizi;*

   c) *garantire che tutte le persone agenti sotto la propria autorità alle quali sia consentito di accedere o trattare i Dati condivisi abbiano sottoscritto idoneo impegno – o siano altrimenti comunque adeguatamente vincolate – a mantenere totale riservatezza rispetto a tali dati e che, a tal fine, gli stessi agiscano sotto il costante controllo del responsabile ed in conformità alle istruzioni da quest'ultimo fornite;*

   d) *definire e mettere in atto, tenendo conto anche delle best practices di settore, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità delle operazioni di trattamento connesse all'adempimento del contratto scaturente dal rapporto professionale e/o del contratto di servizi, oltre che dei rischi che tali trattamenti possono determinare per i diritti e le libertà degli interessati, misure tecniche e organizzative adeguate a garantire un idoneo livello di sicurezza dei Dati condivisi;*

e) implementare misure e processi, nell'ottica di cui al punto che precede, che garantiscano l'attuazione dei principi di privacy-by-design e privacy-by-default e, più in generale, la minimizzazione e la sicurezza dei trattamenti, come ad esempio:

i. l'adozione di sistemi di pseudonimizzazione o cifratura dei Dati condivisi;

ii. la capacità di assicurare con continuità la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, oltre che quella di ripristinare tempestivamente la disponibilità e l'accesso ai Dati condivisi in caso di incidente fisico o tecnico;

iii. l'attivazione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative messe in atto al fine di garantire la sicurezza dei trattamenti;

f) adottare le misure necessarie a prevenire, o quantomeno minimizzare, ogni rischio ragionevolmente prevedibile connesso alla distruzione, alla perdita, alla modifica, alla divulgazione non autorizzata o all'accesso, in modo accidentale o illegale, ai Dati condivisi;

g) fornire al Titolare evidenza della procedura adottata per gestire eventuali violazioni della sicurezza da cui derivino, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati condivisi e, laddove la stessa sia, ad esclusiva discrezione del Titolare medesimo, ritenuta inidonea a garantire i necessari livelli di sicurezza ai sensi della Normativa privacy, conformarsi e dare adeguata attuazione alla corrispondente procedura adottata dal Titolare, prestando in ogni caso la massima collaborazione nei confronti di quest'ultimo al fine di eliminare o quantomeno ridurre al minimo gli impatti derivanti da eventi di questo tipo;

h) fermo l'obbligo di comunicare senza ingiustificato ritardo al Titolare ogni possibile evento qualificabile come data breach ai sensi della normativa applicabile, informare prontamente il Titolare medesimo riguardo a qualsiasi ulteriore evento, fatto o circostanza, prevedibile o meno, da cui possa derivare un rischio elevato per i diritti e le libertà fondamentali degli interessati coinvolti nelle operazioni di trattamento. In caso di violazione dei dati personali (ai sensi del GDPR) il Responsabile deve darne comunicazione immediata al Titolare e comunque entro un massimo di 4 (quattro) ore. Entro le successive 20 (venti) ore il Responsabile deve altresì raccogliere e fornire al Titolare le seguenti informazioni di dettaglio:

i. il tipo di violazione[1];
ii. la natura, la sensibilità e il volume dei dati personali interessati;
iii. la pseudonimizzazione e/o la cifratura dei dati violati (indicare se applicata);
iv. la facilità di identificazione della lista delle persone impattate;
v. la gravità delle conseguenze per gli interessati (es. danni fisici, materiali o immateriali, quali furto o usurpazione di identità, perdite finanziarie, pregiudizio alla reputazione);
vi. l'elenco delle persone interessate dalla violazione dei dati personali (se disponibili), incluse le informazioni di contatto;
vii. le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di record di dati personali interessati;
viii. le probabili conseguenze, per il Titolare, della Violazione dei dati personali subita dal Responsabile e/o dai Sub-responsabili;
ix. le misure adottate o da adottare per affrontare la violazione dei dati personali, per attenuare gli effetti e ridurre al minimo i danni derivanti dalla violazione medesima.

i) non affidare alcun trattamento connesso all'esecuzione del contratto scaturente dal rapporto professionale e/o dal contratto di servizi ad eventuali sub-responsabili non autorizzati dal Cliente. Il Titolare ha sempre il diritto di opporsi. Anche in caso di accettazione, espressa o tacita, in presenza di motivi legittimi, il Titolare potrà revocare in ogni momento la nomina di qualsiasi sub-responsabile. Resta inteso che il Responsabile sarà obbligato a fare in modo che i sub-responsabili autorizzati ad operare siano vincolati al rispetto degli stessi obblighi applicabili al Responsabile in virtù del presente atto e, ovviamente, della normativa di volta in volta vigente. Allo stesso modo, qualsiasi dovesse essere il numero dei sub-responsabili eventualmente coinvolti da parte del Responsabile, previa autorizzazione del Cliente, qualsiasi violazione o inadempimento

---

[1] Tipi di violazioni dei dati personali:

- "Violazione della riservatezza" - in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.
- "Violazione della disponibilità" - in caso di perdita accidentale o non autorizzata di accesso o distruzione di dati personali.
- "Violazione dell'integrità": in caso di alterazione non autorizzata o accidentale dei dati personali.

Esempi di perdita di disponibilità si hanno nei casi in cui i dati sono stati cancellati accidentalmente o da una persona non autorizzata oppure, in caso di dati criptati, quando si perde la chiave di decifratura. Nel caso in cui il Titolare non possa ripristinare l'accesso ai dati, ad esempio tramite un backup, ciò viene considerato come una perdita permanente di disponibilità.

commesso da tali terze parti, o dai loro dipendenti o collaboratori, ricadrà in ogni caso sotto la sola ed esclusiva responsabilità del Responsabile medesimo;

j) adottare misure tecniche ed organizzative che, anche in considerazione della natura dei trattamenti svolti per conto e nell'interesse del Titolare, consentano al Responsabile di assistere il Cliente nell'adempimento del proprio obbligo di fornire adeguato riscontro alle richieste di esercizio dei diritti avanzate da parte degli interessati, con particolare riferimento alle istanze di portabilità, di limitazione del trattamento e di cancellazione ("oblio") dei dati;

k) collaborare con il Titolare, limitatamente ai trattamenti relativi ai Dati condivisi, nell'assolvimento degli obblighi di:

i. notifica delle violazioni di dati all'Autorità Garante per la protezione dei dati personali (il "Garante") o ad altre autorità di controllo competenti e, laddove richiesto in ragione dell'elevato livello di rischio per i diritti e le libertà degli interessati, anche a questi ultimi;

ii. esecuzione, in tutti i casi in cui ciò sia necessario, di idonea valutazione di impatto sulla protezione dei dati (privacy impact assessment) oltre che nello svolgimento delle procedure di consultazione preventiva con il Garante o le altre autorità competenti.

l) predisporre e mantenere costantemente aggiornato, in formato elettronico o cartaceo, un registro di tutte le operazioni di trattamento svolte ai fini dell'esecuzione del contratto scaturente dal rapporto professionale e/o del contratto di servizi, contenente in particolare:

i. i propri dati di contatto, oltre a quelli del Titolare e, ove applicabile, del proprio responsabile della protezione dei dati (data protection officer);

ii. le categorie dei trattamenti effettuati per conto del Titolare;

iii. i dettagli relativi ad eventuali trasferimenti dei Dati condivisi al di fuori dello Spazio Economico Europeo, con indicazione del paese terzo o dell'organizzazione verso cui i dati sono trasmessi e, qualora il trasferimento non sia basato su una decisione di adeguatezza della Commissione UE o su altri meccanismi di garanzia (quali ad esempio Clausole Contrattuali Standard o Binding Corporate Rules) e non sia applicabile nessuna delle deroghe previste dalla normativa vigente, le misure implementate a tutela dei dati;

iv. una descrizione generale delle misure di sicurezza tecniche e organizzative adottate in conformità al presente accordo e, più in generale, alla normativa applicabile.

m) fermo l'obbligo di collaborazione di cui alla precedente lett. j), mettere il Titolare al corrente di qualsiasi richiesta di esercizio di diritti inviata da parte degli interessati, entro un termine massimo di 24 ore dal ricevimento della stessa;

n) non trasferire i Dati condivisi al di fuori dello Spazio Economico Europeo se non previa autorizzazione da parte del Titolare ed in presenza di idonee garanzie ai sensi di legge (quali ad esempio decisioni di adeguatezza della Commissione UE, Clausole Contrattuali Standard o Binding Corporate Rules);

o) non comunicare a terzi e, più in generale, non diffondere i Dati condivisi, se non in presenza di adeguati presupposti di liceità per tali ulteriori trattamenti;

p) prestare nei confronti del Titolare ogni necessaria collaborazione nell'assolvimento di richieste che dovessero pervenire dal Garante o da altre autorità competenti o in relazione a procedure o ispezioni che dovessero essere avviate nei confronti del Titolare, dando altresì immediata esecuzione alle istruzioni ricevute e fornendo copia di ogni documento richiesto.

4. *Fermo tutto quanto sopra, il Titolare potrà fornire ulteriori specifiche scritte alle istruzioni riportate nel presente Contratto e nel contratto scaturente dal rapporto professionale e/o del contratto di servizi, nonché ulteriori istruzioni, sempre in forma scritta, evidenziando opportunamente l'importanza della comunicazione. Qualsiasi ulteriore istruzione che esula da quelle riportate nel presente Contratto e/o in quello scaturente dal rapporto professionale e/o di servizi dovranno rientrare nell'oggetto del presente contratto e/o quello scaturente dal rapporto professionale e/o di servizi. In caso contrario, ossia in tutti i casi in cui le nuove istruzioni possano qualificarsi in ambito contrattuale quale "novazione oggettiva", le ridette ulteriori istruzioni necessiteranno di una richiesta di modifica ai sensi del contratto scaturente dal rapporto professionale e/o del Contratto di Servizi. Le istruzioni sono sempre fornite per iscritto, a meno che l'urgenza o altre circostanze del caso richiedano una forma diversa (e.g. orale) sempre seguita da una conferma scritta entro le dodici ore successive. Oltre agli obblighi di comunicazione previsti dal presente Contratto, il Responsabile è tenuto a comunicare immediatamente al Titolare eventuali istruzioni che ritiene siano in violazione del GDPR o di altra norma di legge e a fornire evidenza di tali leggi applicabili. A seguito di tale comunicazione il Responsabile sarà libero di adottare il comportamento che riterrà più opportuno.*

5. *Il Responsabile dovrà mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto dei propri obblighi, cooperando altresì ad eventuali attività di audit, revisioni o controlli che il Titolare medesimo dovesse ritenere*

opportuni per monitorare il mantenimento, da parte del Responsabile, dei dovuti livelli di sicurezza dei Dati condivisi per l'espletamento del contratto scaturente dal rapporto professionale e/o del contratto di servizi.

6. *Qualsiasi inadempimento o violazione degli obblighi sopra stabiliti e di ogni ulteriore norma di legge applicabile, con particolare riguardo ai necessari livelli di sicurezza, anche in tema di data breach management, ricadrà sotto l'esclusiva responsabilità del Responsabile. Ne consegue che quest'ultimo risponderà in via esclusiva, tranne casi di dolo o colpa grave da parte del Titolare nella verificazione dell'inadempimento o della violazione rilevante, di ogni richiesta di risarcimento, danno o sanzione che dovesse derivare dal mancato puntuale assolvimento dei propri obblighi, qui espressamente manlevando il Titolare da ogni relativa conseguenza.*

7. *La presente nomina avrà la medesima durata del contratto scaturente dal rapporto professionale e/o del contratto di servizi. Pertanto, salvo il caso in cui lo stesso non venga prorogato su intesa delle parti, o che queste ultime non decidano di sciogliere il presente accordo prima della scadenza del contratto scaturente dal rapporto professionale e/o del contratto di servizi, le disposizioni qui stabilite cesseranno di produrre ogni effetto nel momento stesso in cui il Responsabile avrà completato l'esecuzione dei Servizi.*

8. *Al termine – per qualsiasi causa ciò avvenga – del contratto scaturente dal rapporto professionale e/o del contratto di servizi, il Responsabile dovrà restituire al Titolare tutti i Dati condivisi, provvedendo altresì alla definitiva cancellazione di ogni copia degli stessi, in qualsiasi formato (back-up, cartacea, su supporto mobile, in cloud, etc.). La cancellazione di tali Dati da parte del Responsabile dovrà essere certificata al Titolare, tranne quando la conservazione degli stessi sia richiesta da norme di legge o in ragione di prescrizioni dettate dal Garante o da altre Autorità competenti. In quest'ultimo caso, il Responsabile si impegna a garantire la riservatezza dei Dati condivisi trasferiti e di non trattare tali Dati se non per finalità imposte dalla legge o da un ordine della Pubblica Autorità.*

9. *Il presente Contratto è disciplinato dalla legge italiana, fatto salvo quanto previsto dalla legge applicabile in materia di protezione dei dati. Il foro competente per qualsiasi eventuale controversia relativa al presente Contratto viene stabilito nel contratto scaturente dal rapporto professionale e/o del contratto di servizi, fatto salvo quanto previsto dalla legge applicabile in materia di protezione dei dati. In mancanza di espressa previsione nel contratto scaturente dal rapporto professionale e/o del contratto di servizi, per le controversie nascenti dal presente Contratto sarà competente in via esclusiva il Foro di Civitavecchia.*

10. *L'inapplicabilità o l'invalidità di una o più disposizioni del presente Contratto non pregiudica le restanti parti del medesimo. La disposizione invalida o inapplicabile potrà all'occorrenza essere (i) modificata al fine di garantirne validità ed opponibilità, rispettando il più fedelmente possibile l'intenzione delle Parti o - qualora questo non sia possibile – (ii) interpretata come se la stessa non fosse mai stata parte del presente Contratto. Quanto precede si applica anche nel caso in cui il presente Contratto presenti lacune.*

Il Titolare del trattamento dichiara che tutte le comunicazioni inerenti i compiti, le funzioni e gli obblighi derivanti dalla presente scrittura, gli potranno essere trasmesse, a seconda dell'urgenza e delle necessità, ai seguenti riferimenti:

ALLEGATO

Descrizione delle misure tecniche e organizzative di sicurezza implementate dal Responsabile (e dai suoi Sub-responsabili ove nominato).

Il Responsabile è tenuto ad implementare, applicare e tenere costantemente aggiornate le misure tecniche ed organizzative di sicurezza riportate nella seguente tabella, oltre a quelle previste dalla normativa primaria e secondaria, tempo per tempo vigente, in materia di protezione dei dati personali, applicabile ai Servizi resi dal Responsabile, nonché quelle ulteriori necessarie per garantire un livello di sicurezza adeguato al rischio, prima di procedere al trattamento dei dati personali per conto del Titolare. La seguente tabella, infatti, riporta un'elencazione non esaustiva e pertanto il Responsabile si impegna ad implementare, applicare e tenere costantemente aggiornate tutte le ulteriori misure 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.

Fermo quanto sopra statuito, si citano a titolo meramente esemplificativo e non esaustivo, ove applicabili ai Servizi, le disposizioni definite dal Provvedimento del Garante n. 192/2011 nonché il Provvedimento del Garante recante le "Misure ed accorgimenti

prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – 27 novembre 2008" così come modificato in base al provvedimento del 25 giugno 2009.

ID	MISURE DI SICUREZZA ESSENZIALI PER LA PROTEZIONE DEI DATI PERSONALI
1.1	Firewall e router devono essere configurati al fine di limitare il traffico, in entrata e in uscita, da reti e sistemi "non attendibili" (inclusi wireless). E' necessario altresì negare tutto il resto del traffico ad eccezione dei protocolli necessari all'ambiente che tratta dati personali.
1.2	I Web Application Firewall devono essere configurati davanti ai server appartenenti all'ambiente che tratta dati personali, al fine di verificare e convalidare il traffico che è diretto al server. Qualsiasi servizio o traffico non autorizzato deve essere bloccato e deve essere generato un avviso che va poi gestito in modo adeguato (analisi e remediation).
1.3	Devono essere applicati template di configurazione sicuri (tramite hardening) per gli asset ICT (es. database, applicazioni, sistemi operativi) che trattano dati personali in modo da lasciare disponibili solo i servizi strettamente necessari per le attività previste.
1.4	I dati personali devono essere protetti contro il rischio di intrusione e malware mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale (es. antivirus).
1.5	Gli aggiornamenti periodici del software devono essere effettuati almeno ogni 6 mesi (es. patching dei sistemi operativi dei client e dei server e degli applicativi di base) e le patch critiche di sicurezza devono essere installate tempestivamente.
1.6	I Vulnerability Assessment (VA) e/o eventuali Penetration Test (PT) devono essere pianificati ed eseguiti almeno una volta l'anno dal Responsabile, sui sistemi utilizzati per fornire i servizi al Titolare. Le vulnerabilità scoperte ed i finding devono essere gestiti in modo adeguato (analisi e rimedio).
2.1	Il periodo di conservazione dei dati personali deve essere limitato nella misura necessaria richiesta da ogni singolo servizio erogato, nel rispetto degli obblighi legali e/o regolamentari vigenti.
2.2	Per la cancellazione dei dati non più necessari al singolo servizio erogato e per la dismissione degli asset ICT devono essere messe in atto procedure di pulizia sicura ed irreversibile, al fine di rimuovere tutti i dati personali e/o sovrascrivere in modo sicuro e non reversibile prima dello smaltimento o del riutilizzo. Nel caso in cui questo non sia possibile i supporti devono essere distrutti o resi inutilizzabili.
2.3	I documenti cartacei che contengono dati personali devono essere fisicamente distrutti prima di essere cestinati attraverso dispositivi specifici quali distruggi documenti.
2.4	Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri.
2.5	I dati personali devono essere resi illeggibili (ad esempio sfruttando la crittografia) se archiviati su supporti digitali portatili, di backup, log files.
2.6	Il numero degli archivi di dati personali (database, file, copie, archivi) deve essere ridotto al minimo, evitando inutili duplicazioni.
2.7	La trasmissione di dati personali su reti aperte, pubbliche o non attendibili, deve essere protetta mediante sistemi crittografici e l'utilizzo di protocolli sicuri. Nel caso in cui la crittografia del canale non sia possibile, i file e gli allegati contenenti dati personali devono essere protetti mediante crittografia ogni volta che vengono trasmessi su reti aperte, pubbliche o non attendibili.
2.8	Devono essere utilizzati strumenti di sicurezza per monitorare e controllare il flusso di dati personali attraverso gli endpoint e verso le reti esterne.
2.9	La crittografia dei database/archivi di dati deve essere basata su una classificazione appropriata degli asset in ambito, in base al livello di criticità. Il Responsabile, in mancanza di una specifica richiesta del Titolare, decide se implementare o meno la crittografia e con quale granularità applicarla (ad esempio a livello di database/files o di tabella), e la applica ogni volta che il Titolare ne fa richiesta.
2.10	I dati personali non devono essere copiati su supporti rimovibili, ad eccezione dei supporti espressamente autorizzati dal Responsabile per attività specifiche.
2.11	I dati personali presenti nello/negli storage devono essere protetti mediante crittografia quando vengono memorizzati dai fornitori di servizi cloud e/o da altri sub-responsabili.
2.12	I supporti (rimovibili e non rimovibili) contenenti dati personali devono essere protetti contro l'accesso non autorizzato attraverso adeguate misure di sicurezza fisica e logica.
2.13	I dipendenti devono essere adeguatamente istruiti e formati sulle corrette regole di condotta da adottare per la protezione dei dati personali contenuti nei documenti cartacei (es. in caso di allontanamento dalla postazione di lavoro assicurarsi

ID	MISURE DI SICUREZZA ESSENZIALI PER LA PROTEZIONE DEI DATI PERSONALI
	che nessuno possa accedere alle informazioni riservate, proteggere i documenti originali e le fotocopie da furto o uso non autorizzato, conservare la documentazione in cassetti e armadi chiusi alla fine della sessione di lavoro).
3.1	*Devono essere messe in atto procedure adeguate a garantire la disponibilità dei dati personali (come diritto dell'interessato) in modo tempestivo. Le procedure di backup devono garantire copie dei dati personali almeno settimanalmente.*
4.1	*L'autorizzazione ad accedere agli ambienti di produzione contenenti dati personali deve essere fornita secondo i principi del "need to know" e del "least privilege".*
4.2	*Le policy e le procedure devono essere implementate per garantire la corretta identificazione degli utenti e degli amministratori che accedono alle componenti di sistema che gestiscono i dati personali. A ogni utente deve essere assegnato un nome utente prima di consentire l'accesso ai sistemi di autenticazione e ai dati personali. Ogni nome utente deve identificare solo una persona.*
4.3	*Gli accessi amministrativi remoti individuali ai sistemi che gestiscono i dati personali devono essere protetti mediante un meccanismo di autenticazione che richiede modifica della password ogni 90 giorni. Inoltre, si consiglia di dotarsi di strumenti per la gestione delle password (tool ad hoc) per garantire la sicurezza delle credenziali.*
4.4	*Le password per i sistemi e i dispositivi che gestiscono dati personali devono essere complesse (almeno otto caratteri e ad esempio una combinazione di lettere maiuscole o minuscole, numeri e caratteri speciali) non facilmente attribuibili all'utente e devono essere modificate almeno ogni 3 mesi.*
4.5	*Le risorse di sistema e il diritto di accesso devono essere assegnati in modo univoco ad ogni user account.*
4.6	*L'accesso da remoto (da reti esterne) all'ambiente che tratta dati personali deve essere protetto mediante autenticazione a più fattori.*
4.7	*Tutti gli accessi ai database contenenti dati personali devono essere protetti / controllati al fine di garantire i principi di "need to know", "least privilege" e la tracciabilità.*
4.8	*I diritti di accesso ai dati personali degli utenti devono essere rivisti e nuovamente certificati a intervalli regolari e, in ogni caso, almeno una volta all'anno, secondo il corretto processo di Identity and Access Management.*
5.1	*L'accesso agli ambienti di produzione contenenti dati personali e in generale l'accesso ai dati personali devono essere monitorati e loggati al fine di tracciare con precisione il collegamento tra l'accesso e l'utente che accede ai dati personali. Inoltre il monitoraggio deve essere effettuato al fine di prevention e detection di minacce alla sicurezza dei dati personali.*
5.2	*Ogni accesso ai dati personali (consultazione, modifica, cancellazione, inserimento) deve essere tracciato registrando le informazioni minime richieste per ricostruire le modalità di accesso effettuato e permettere il monitoraggio sul sistema, registrando almeno:* *- Identificazione dell'utente* *- Tipo di evento* *- Data e ora* *- Indicazione di successo o fallimento* *- Fonte dell'evento* *- Identità dei dati interessati (identificativo del soggetto interessato), dei componenti di sistema o risorse.*
5.3	*Il Responsabile (e/o i Sub-responsabili), a seguito di richiesta del Titolare, ha il dovere di fornire i log degli accessi per il trattamento dei dati personali.*
6.1	*Devono essere messe in atto procedure adeguate a garantire la disponibilità continua di dati personali; il personale di back up deve essere identificato per garantire la continuità del servizio all'interessato che desidera accedere ai propri dati personali.*
6.2	*È necessario attuare un programma formale di sensibilizzazione sulla sicurezza per rendere consapevole tutto il personale delle politiche e procedure relative alla sicurezza dei dati personali.*
6.3	*Devono essere stipulati chiari accordi contrattuali con eventuali sub-fornitori dei servizi, al fine di pattuire la loro responsabilità in merito alla sicurezza dei dati personali che elaborano / memorizzano / trasmettono per conto del Titolare. Tali accordi devono riflettere almeno le istruzioni e misure indicate in questo documento.*
6.4	*Le responsabilità e i doveri dei dipendenti relative alla riservatezza dei dati personali devono essere chiaramente esplicitate come valevoli anche dopo la cessazione o il cambio di impiego.*
7.1	*I processi e gli strumenti per il Secure Software Development Lifecycle (SDLC) devono essere integrati con controlli e requisiti di sicurezza appropriati, al fine di garantire che i nuovi software/applicazioni ICT siano progettati e sviluppati tenendo in considerazione i requisiti della sicurezza integrata.*
7.2	*I processi di gestione delle modifiche ICT devono essere integrati con controlli e requisiti di sicurezza appropriati, al fine di garantire la protezione continua del software / applicazioni ICT in vigore subito dopo modifiche rilevanti.*

ID	MISURE DI SICUREZZA ESSENZIALI PER LA PROTEZIONE DEI DATI PERSONALI
8.1	*I processi e gli strumenti per la gestione degli incidenti devono essere correttamente implementati e/o migliorati al fine di consentire il rilevamento e la classificazione delle violazioni dei dati personali in modo che siano correttamente comunicati al Titolare affinché possa provvedere entro i termini stabiliti nel paragrafo "Obblighi di comunicazione e Violazione dei dati personali".*
8.2	*Deve essere creato e mantenuto aggiornato uno specifico registro delle violazioni dei dati personali.*

Il presente contratto, redatto su 13 (TREDICI) pagine, viene emesso in 2 (due) originali, uno per la Cliente ed uno per il Consulente

Letto, approvato e sottoscritto.

Civitavecchia, lì 01/03/2022

IL CONSULENTE

dott. Carlo Romano

CIVITAVECCHIA SERVIZI PUBBLICI S.R.L.

Il Presidente del CdA

Avv. Fabrizio Lungarini

Ai sensi e per gli effetti degli artt.1341 e 1342 C.C. le parti dopo attenta e separata rilettura approvano specificamente gli articoli 1) *Oggetto del contratto*, 2) *Rappresentanza, riservatezza ed obblighi delle parti;* 3) *Durata del contratto*; 4) *Compensi e spese;* 5) *Effetti della cessazione del contratto;* 6)*Condizioni di incompatibilità*; 7) *Controversie;* 8) *Polizza assicurativa*; 10) *Negoziazione e accettazione dell'accordo* e 11) *Sostituzione di accordi precedenti e forma scritta* del presente contratto.

Civitavecchia, lì 11.01.2022

IL CONSULENTE

dott. Carlo Romano

CIVITAVECCHIA SERVIZI PUBBLICI S.R.L.

Il Presidente del CdA

Avv. Fabrizio Lungarini