AGENZIA REGIONALE PROTEZIONE AMBIENTALE DELLA CAMPANIA

DELIBERAZIONE DEL DIRETTORE GENERALE N. 642 DEL 06/10/2025

IL RUP LA VIA

OGGETTO: AVVISO PUBBLICO ACN N. 08/2024 - PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5, CUP E64F24000280006_AQ ID 2296, LOTTO 2 "SERVIZI DI COMPLIANCE E CONTROLLO"_APPROVAZIONE SCHEMA DI MANLEVA PER ATTIVITA' DI VA/PT IN AMBIENTE DI TEST.

L'anno duemilaventicinque, il giorno sei del mese di Ottobre presso la sede dell'A.R.P.A.C. alla stregua dell'istruttoria compiuta dal RUP e della dichiarazione di completezza e regolarità resa dal medesimo

PREMESSO CHE:

- con deliberazione n. 532 del 14.11.2018 l'ARPAC ha nominato il Responsabile per la Transizione al Digitale, ai sensi dell'articolo 17, del rinnovato decreto legislativo 82/2005 (Codice dell'Amministrazione Digitale), individuandolo nella dott.ssa Loredana La Via, dirigente della UO Sistemi Informativi e Informatici, cui sono affidati i compiti di conduzione del processo di transizione alla modalità operativa digitale e dei conseguenti processi di riorganizzazione, finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità;

- tra i compiti affidati al RTD rientra quello inerente indirizzo, pianificazione, coordinamento e monitoraggio della *sicurezza informatica* relativamente ai dati, ai sistemi ed alle infrastrutture, anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, c. 1 del citato CAD;
  - il tema della cybersicurezza è quanto mai attuale e fortemente attenzionato anche a livello UE;
  - la nuova direttiva europea NIS 2 (Direttiva n. 2022/2555, entrata in vigore il 17 gennaio 2023 << … *relativa a misure per un livello comune elevato di cybersicurezza nell'Unione,….* > che abroga la precedente Direttiva (UE) 2016/1148 - "Direttiva NIS 1" - recepita in Italia attraverso il D. Lgs. n. 65/2018 e da cui di fatto la nuova NIS 2 prende forma e sostanza) che introduce, tra l'altro, misure più stringenti e specifiche in termini di cyber risk management e di segnalazione e *condivisione* delle informazioni relative agli incidenti di sicurezza, è in vigore in Italia a partire dal 16.10.2024, a seguito del D. Lgs. n. 138 del 04.09.2024;
  - secondo l'Osservatorio Cybersecurity & Data Protection la protezione contro i rischi di tipo cyber sta diventando sempre più una priorità di investimento in Italia, con il 67% delle imprese italiane ad aver segnalato un incremento dei casi di attacchi malevoli;
  - con nota prot. n. 23488 del 12.04.2024 ARPAC ha presentato domanda di partecipazione all'Avviso pubblico ACN n. 8/2024 per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità

del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente a valere sul Piano Nazionale di Ripresa e Resilienza;

- con deliberazione n. 512 del 17.10.2024 l'Ente prende atto dell'ammissione del suo progetto al finanziamento di cui sopra;
- il citato progetto si pone l'obiettivo di migliorare la postura cyber dell'Ente attraverso un articolato piano strategico, avvalendosi di una attività di assessment e potenziamento della resilienza cyber, e rafforzandosi così in termini di compliance e formazione;
- per fare ciò occorre perseguire la roadmap di iniziative che prevedono di identificare lo stato di esposizione alle vulnerabilità, gestire gli eventuali incidenti di sicurezza, eseguire attacchi simulati per sfruttare le vulnerabilità e, di conseguenza, effettuare le dovute 'remediation', e migliorare la compliance normativa;
- con deliberazione n. 584 del 26.11.2024 l'Agenzia ha aderito all'Accordo Quadro CONSIP per "*l'Affidamento di Servizi di Sicurezza da Remoto, di Compliance e Controllo per le Pubbliche Amministrazioni" – ID2296 – Lotto 2 "Servizi di Compliance e Controllo"*, per un periodo pari a n. 13 mesi (01.12.2024 – 31.12.2025) per l'acquisizione dei seguenti servizi, opportunamente dimensionati come da Piano Operativo:
  - L2.S16: Security Strategy
  - L2.S17: Vulnerability assessment
  - L2.S21: Supporto all'analisi e gestione degli incidenti
  - L2.S22: Penetration testing
  - L2.S23: Compliance normativa,

individuando il RTI composto da

- *Deloitte Risk Advisory S.r.L.*
- *EY Advisory S.p.A.*
- *Teleco S.r.L.*

quale Fornitore per la realizzazione esecutiva delle esigenze agenziali in materia di Cybersicurezza, come su delineate;

- con nota prot. n. 67993/2024 del 31.10.2024 l'Ente ha trasmesso all'ACN l'avvio delle attività e le modifiche al progetto finanziato relativamente al cronoprogramma, atto dovuto essendo trascorsi svariati mesi prima dell'esito della valutazione da parte della Commissione ACN;
- nell'ambito dunque delle attività di cui sopra, la linea L2.S17 "*Vulnerability Assessment*" prevede un'attività di verifica preliminare dei sistemi di sicurezza adottati da alcuni sistemi informativi che, per la loro criticità per il business istituzionale, sono stati identificati come 'perimetro' di analisi, al mero ed esclusivo fine di rilevare ed analizzare eventuali punti di criticità (intendendosi, per tali, vulnerabilità che possono compromettere la confidenzialità o l'utilizzo illegittimo dei dati e/o impattare in maniera rilevante sull'attività di *business* dell'Agenzia) ed avere indicazione, conseguentemente, dei necessari interventi correttivi e/o migliorie da apportare dal punto di vista tecnico e tecnologico;
- come da vincoli dell'AQ ID 2296, propedeutico allo svolgimento delle attività di cui sopra (in particolare per le prove di cui alla linea L2.S22 "*Penetration testing*", ossia la simulazione di attacchi informatici per valutare la protezione del sistema) è la sottoscrizione, tra le parti, di un "*Accordo per l'esecuzione di attività di verifiche interne ed esterne di sicurezza a*

valere sul perimetro dei sistemi informativi di titolarità di Agenzia Regionale per la Protezione Ambientale della Campania (ARPAC), concordato nel corso d'ingaggio", il cui schema è allegato alla presente;

CONSIDERATO CHE

- il Piano Operativo prevede di migliorare la postura Cyber dell'Agenzia anche mediante attività mirate di VA/PT (Vulnerability Assessment/Penetration Testing) finalizzate ad identificare ed a verificare l'efficacia delle difese di sicurezza della infrastruttura IT, simulando attacchi reali per scoprire e correggere le vulnerabilità prima che vengano sfruttate da attacchi di tipo Cyber;
- il RTI Fornitore ha predisposto e trasmesso all'Agenzia uno schema di "*Accordo per l'esecuzione di attività di verifiche interne ed esterne di sicurezza a valere sul perimetro dei sistemi informativi di titolarità di Agenzia Regionale per la Protezione Ambientale della Campania (ARPAC), concordato nel corso d'ingaggio*" che deve essere sottoscritto da entrambe le parti;
- lo schema approvato non comporta spese e non produce oneri a carico del bilancio dell'Agenzia;
- l'art. 11 dello schema prevede che, al fine di garantire una migliore gestione ed esecuzione dell'Attività di Verifica di Sicurezza, le Parti nominino propri Referenti;

RITENUTO CHE

- l'Agenzia, in quanto Pubblica Amministrazione, rimane soggetta a tutto quanto disposto dalla Circolare AgID n. 2/2017, recante *"Misure minime di sicurezza ICT per le pubbliche amministrazioni"* ed alla Direttiva NIS2, pertanto al D. Lgs. n. 138 del 04.09.2024;
- con il progetto ammesso a finanziamento con fondi PNRR ARPAC ha l'opportunità di identificare lo stato di salute della sicurezza del sistema informativo dell'Ente, al fine di garantire la corretta postura cyber sulla base della roadmap delle attività da svolgere e colmare, così, le eventuali vulnerabilità presenti;
- si debba procedere, pertanto, alla esecuzione delle attività previste dalle linee L2.S17 'Vulnerability assessment' e L2.S22 'Penetration testing' e quindi all'approvazione dello schema di "*Accordo per l'esecuzione di attività di verifiche interne ed esterne di sicurezza a valere sul perimetro dei sistemi informativi di titolarità di Agenzia Regionale per la Protezione Ambientale della Campania (ARPAC), concordato nel corso d'ingaggio*" ed alla individuazione del Referente per l'Agenzia, di cui all'art. 11 del citato Accordo;

ATTESO CHE tutti gli atti richiamati nella presente deliberazione sono depositati presso l'ufficio proponente;

VISTI

- il Regolamento Europeo sulla Protezione dei Dati (UE 679/2016);
- la Direttiva NIS2 – Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14.12.2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del Regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972;

- il D. Lgs. 36/2023;
- il D. Lgs. n. 138 del 04.09.2024;
- la Determina di ACN di concessione del finanziamento e contestuale rifinanziamento e approvazione della graduatoria finale e di destinazione delle risorse con aggiornamento del circuito finanziario – n. protocollo 30550 del 23.09.2024;
- la Circolare AgID n. 2/2017, recante *"Misure minime di sicurezza ICT per le pubbliche amministrazioni";*
- la L. R. 10/98 ed il vigente Regolamento sull'Organizzazione di ARPAC;
- la deliberazione n. 657/2024 di approvazione di Bilancio di previsione esercizio 2025 e pluriennale per il triennio 2025/2027.

Per tutto quanto premesso e considerato si propone di adottare la seguente

DELIBERAZIONE

Per le motivazioni espresse in narrativa che qui si intendono integralmente riportate e trascritte:

- di approvare lo schema di "*Accordo per l'esecuzione di attività di verifiche interne ed esterne di sicurezza a valere sul perimetro dei sistemi informativi di titolarità di Agenzia Regionale per la Protezione Ambientale della Campania (ARPAC), concordato nel corso d'ingaggio*" inerente l'esecuzione delle attività di VA/PT come previste dalle linee L2.S17 'Vulnerability assessment' e L2.S22 'Penetration testing' del Piano Operativo e che, allegato alla presente, ne costituisce parte integrante e sostanziale;
- di confermare che lo schema approvato non comporta spese e non produce oneri a carico del bilancio dell'Agenzia
- di nominare quale Referente di cui all'art. 11, la dott.ssa Loredana La Via, già Responsabile per la Transizione Digitale e Responsabile del progetto PNRR de quo;
- di trasmettere il presente atto al referente dott.ssa Loredana La Via.

Napoli, 26 settembre 2025

Il RUP
Dott.ssa Loredana La Via

La proposta di deliberazione è accolta.

Napoli, 06/10/2025

Il Direttore Generale
Avv. Luigi Stefano SORVINO

OGGETTO: AVVISO PUBBLICO ACN N. 08/2024 - PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5, CUP E64F24000280006_AQ ID 2296, LOTTO 2 "SERVIZI DI COMPLIANCE E CONTROLLO"_APPROVAZIONE SCHEMA DI MANLEVA PER ATTIVITA' DI VA/PT IN AMBIENTE DI TEST.

PARERE DI REGOLARITA' AMMINISTRATIVA

Sulla suesposta proposta, avente ad oggetto "AVVISO PUBBLICO ACN N. 08/2024 - PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5, CUP E64F24000280006_AQ ID 2296, LOTTO 2 "SERVIZI DI COMPLIANCE E CONTROLLO"_APPROVAZIONE SCHEMA DI MANLEVA PER ATTIVITA' DI VA/PT IN AMBIENTE DI TEST. ", in ordine alla regolarità amministrativo-contabile ed alla copertura finanziaria, si esprime parere favorevole.

Data **06/10/2025**

Il Direttore Amministrativo

Luca Antonio Esposito / InfoCert S.p.A.

DELIBERAZIONE N° 642 DEL 06/10/2025

ATTESTAZIONE DI PUBBLICAZIONE

Si dichiara che la presente deliberazione è stata affissa all'Albo di questa Agenzia dal giorno 06/10/2025 e vi resterà per gg 15 (quindici) .

Napoli, **06/10/2025**

Il Funzionario Incaricato
Valeria Torella / InfoCert S.p.A.

DELIBERAZIONE N° 642 DEL 06/10/2025

ATTESTAZIONE DI IMMEDIATA ESEGUIBILITA'

La presente Deliberazione è stata dichiarata immediatamente eseguibile per l'urgenza

Napoli data **06/10/2025**

Il Direttore Generale
Avv. Luigi Stefano SORVINO

Luigi Stefano Sorvino / InfoCert S.p.A.

Oggetto: Accordo per l'esecuzione di attività di verifiche interne ed esterne di sicurezza a valere sul perimetro dei sistemi informativi di titolarità di Agenzia Regionale per la Protezione Ambientale della Campania (ARPAC), concordato nel corso d'ingaggio

SCRITTURA PRIVATA TRA

- **Agenzia Regionale per la Protezione Ambientale della Campania (ARPAC)**, con sede legale in Via Vicinale S. Maria del Pianto - Centro Polifunzionale, Torre 1, 80143 Napoli, C.F. n° 07407530638 nella persona di Rappresentante Legale, , in qualità di Direttore Generale, giusta i poteri conferitigli da Decreto della Giunta Regionale della Campania n° 25 in data 10/04/2024 (nel seguito per brevità anche "ARPAC" o l'"Amministrazione"),

e

- **Deloitte Consulting S.r.l. S.B.,** sede legale in Milano, Via Santa Sofia n. 28, Capitale Sociale deliberato Euro 4.700.000,00 – sottoscritto e versato per Euro 3.715.283,48, iscritta al Registro delle Imprese di Milano al n. 03945320962, P. IVA 03945320962, domiciliata ai fini del presente atto in Milano, Via Santa Sofia n.28, in persona del Procuratore , nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa le mandanti:
- **EY Advisory S.p.A.** *con* sede legale in Milano, Via Meravigli n.14, capitale sociale Euro 2.250.000,00=, iscritta al Registro delle Imprese di Milano al n. 13221390159, P. IVA 13221390159, domiciliata ai fini del presente atto in Milano, via Tortona n.25;
- **Teleco S.r.l.**, con sede legale in Roma, Via Rosazza n. 26, capitale sociale Euro 950.000,00=, iscritta al Registro delle Imprese di Milano al n. 02856220922, P. IVA 02856220922, domiciliata ai fini del presente atto in Milano, via Tortona n.25, giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in Roma repertorio n. 14.339 del 3 febbraio 2022;

(ARPAC ed il Raggruppamento Temporaneo d'Imprese tra la mandataria Deloitte Consulting S.r.l. S.B. e le mandanti EY Advisory S.p.A. e Teleco S.r.l. sono definiti singolarmente, di seguito, anche una "**Parte**" e, congiuntamente, le "**Parti**").

PREMESSE

A. Il Raggruppamento Temporaneo d'Imprese tra la mandataria Deloitte Consulting S.r.l. S.B. e le mandanti EY Advisory S.p.A. e Teleco S.r.l. (di seguito anche "RTI") e ARPAC hanno intrapreso contatti per la definizione e la esecuzione di servizi come indicato di seguito.

B. ARPAC, anche in merito alla disciplina in materia di data breach introdotta dal Regolamento (UE) 2016/679, intende avvalersi della qualificata collaborazione di un *player* di consolidata esperienza a livello internazionale in ordine ad un'attività di verifica preliminare dei sistemi di sicurezza da esso adottati in relazione ai sistemi informativi che saranno identificati come perimetro di analisi, al mero ed esclusivo fine di rilevare ed analizzare eventuali punti di criticità (intendendosi per tali, vulnerabilità che possono compromettere la confidenzialità o l'utilizzo illegittimo dei dati, impattare in maniera rilevante sull'attività di *business* di ARPAC e che dovrebbero essere risolte non appena possibile e/o mitigate con opportune soluzioni tecnologiche durante l'esecuzione delle operazioni di risoluzione delle anomalie e/o criticità riscontrate) - ed indicare, conseguentemente, a ARPAC i necessari interventi correttivi e/o eventuali migliorie da apportare dal punto di vista tecnico e tecnologico.

C. Il RTI possiede le competenze specifiche per l'esecuzione dell'attività descritta alla premessa B.

D. ARPAC, dopo aver valutato la disponibilità ricevuta dal RTI al riguardo, intende (i) concedere a quest'ultima ed al suo personale, selezionato in base ad appropriati requisiti di etica professionale e vincolato tramite apposito accordo di riservatezza, l'autorizzazione all'esecuzione dell'attività di cui alla precedente premessa B per la finalità ivi esplicitata, avvalendosi della comprovata esperienza, delle specifiche competenze e della professionalità maturata dal RTI nel suddetto contesto, nonché (ii) definire le condizioni, di carattere tecnico e regolamentare, che troveranno applicazione per l'esecuzione della predetta attività da parte del RTI medesimo. Per l'esecuzione di tale attività ARPAC non fornirà al RTI informazioni e chiavi di accesso ad aree private del Sistema Informativo di ARPAC se non reso strettamente necessario dalla natura delle attività previste, in particolare – al fine di svolgere l'attività in oggetto – ARPAC fornirà:

   - Accesso VPN con utenza dedicata creata appositamente per svolgere l'attività e per raggiungere gli applicativi/sistemi non raggiungibili dall'esterno
   - Credenziali applicative necessarie per lo svolgimento dei test in modalità autenticata (Grey box) riuscendo in tal modo a ricoprire più casistiche e dunque una maggiore superficie di attacco

E. Corrisponde al comune intendimento delle Parti addivenire alla stipula di un accordo volto a disciplinare compiutamente le modalità, i termini e le condizioni di esecuzione dell'attività di verifica di sicurezza di cui alla precedente premessa B.

TUTTO CIÒ PREMESSO, sulla base delle precedenti premesse e delle reciproche pattuizioni, dichiarazioni, garanzie e obbligazioni di seguito riportate, le Parti concordano e stipulano quanto segue (di seguito, l'"**Accordo**").

Articolo 1. Le premesse costituiscono parte integrante e sostanziale dell'Accordo.

Articolo 2. Le norme e le condizioni dell'Accordo sono state singolarmente negoziate tra le Parti e costituiscono il frutto di un'intesa raggiunta con la reciproca collaborazione; pertanto, in relazione al presente Accordo, non trova applicazione quanto disposto dagli articoli 1341 e 1342 del codice civile. L'Accordo di erogazione del servizio vede applicazione nell'attività di Penetration Testing (in ambiente di test) in modalità Grey box, basata su OWASP Web Testing Guide, la quale esclude attacchi di tipo DoS/DDoS

Articolo 3. Le Parti prendono atto del carattere fiduciario del rapporto nascente dall'Accordo e del fatto che lo stesso richiede un elevato grado di collaborazione tra le Parti medesime. Pertanto, le Parti si impegnano, in aggiunta agli altri obblighi previsti a carico di ciascuna di esse ai sensi dell'Accordo, a:

(i) eseguire l'Accordo secondo correttezza, buona fede e con la professionalità richiesta, anche ai sensi dell'art. 1176, secondo comma, del codice civile, dalla natura delle prestazioni che ciascuna di esse è tenuta ad eseguire,

(ii) eseguire prestazioni non descritte nell'Accordo o a tollerare eventuali modifiche alle modalità di esecuzione delle prestazioni di cui all'Accordo qualora, secondo criteri di ragionevolezza, tali prestazioni o modifiche appaiano utili o necessarie per assicurare

la corretta, continuativa e coerente attuazione dello stesso, in ogni caso entro l'ambito prestazionale definito dal Contratto esecutivo stipulato tra le Parti avente CIG B457DB055E.
Possibili implicazioni sottese potrebbero implicare dei periodi di downtime, tuttavia le attività saranno svolte in ambiente di test pertanto si escludono disservizi e il fornitore si impegna a escludere test di tipo Denial of Service e altre tipologie di tecniche che potrebbero causare disservizi più frequentemente. Il fornitore, inoltre, si impegna a comunicare tempestivamente al referente tecnico di ARPAC eventuali comportamenti anomali riscontrati durante la fase di testing, comportamenti che potrebbero causare impedimenti ad altri utenti,

(iii) comunicarsi reciprocamente con tempestività qualsiasi circostanza che possa influire sull'esecuzione delle prestazioni a carico di ciascuna di esse ai sensi dell'Accordo,

(iv) determinare, di comune accordo, eventuali modifiche od interventi correttivi alle attività oggetto dell'Accordo (anche, eventualmente, in relazione all'espletamento di attività originariamente non previste), idonee a consentire il perseguimento - nella fase di esecuzione del medesimo - degli obiettivi e delle aspettative di ciascuna Parte e di una migliore realizzazione di determinate attività in capo alle Parti, in ogni caso entro l'ambito prestazionale definito dal Contratto esecutivo stipulato tra le Parti avente CIG B457DB055E.

Articolo 4. Con la stipula dell'Accordo, ARPAC autorizza e presta il proprio consenso all'RTI, anche ai sensi dell'art. 50 del codice penale, affinché quest'ultima possa, per il tramite del personale di cui al successivo art. 7, punto (i), :

(i) accedere ai sistemi informativi di ARPAC utilizzati per l'erogazione dei servizi il cui perimetro verrà stabilito nel corso dell'ingaggio della durata contrattuale, nonché di copertura del presente e, conseguentemente,

(ii) eseguire, l'attività di verifica di sicurezza dei sistemi informativi di cui al precedente punto (i), che saranno puntualmente definiti tra le parti per il tramite di specifiche comunicazioni con riferimento al presente accordo, in ambiente di test, mediante collegamento Internet, sotto il coordinamento di ARPAC, che sarà aggiornata dall'RTI sullo stato avanzamento delle attività e sulla configurazione degli strumenti di analisi della sicurezza,

(a.) preliminarmente, attraverso l'esecuzione di una fase di analisi delle funzionalità dei predetti sistemi informativi tesa ad individuare le tipologie e le modalità di attacco/intrusione da intentare in esecuzione della predetta attività di sicurezza, e

(b.) in subordine alla predetta attività di analisi, mediante la conduzione delle tipologie di attacco e/o intrusione precedentemente individuate ai sensi del precedente punto (a), in modalità "grey box" ovvero avendo la disponibilità di informazioni tecniche relative agli applicativi oggetto di indagine e di credenziali/*user* autorizzative di accesso (di seguito, l'"**Attività di Verifica di Sicurezza**") - al solo ed esclusivo scopo di cui alla precedente premessa B,

A tal fine, è importante considerare che in ambiente di test eventuali disservizi non causerebbero impatti sulla normale attività degli altri utenti, esonerando, e manlevando RTI ed il proprio personale impiegato da quest'ultima per l'esecuzione dell'Attività di Verifica di Sicurezza, da ogni forma di responsabilità (ivi comprese eventuali richieste di tipo risarcitorio che dovessero pervenire da soggetti terzi in ragione delle attività di verifica eseguite), ed, in particolare, dalla possibile configurazione delle fattispecie di cui all'art. 24-*bis* ("*Delitti informatici e trattamento illecito di dati*") del decreto legislativo 8 giugno 2001, n. 231 e successive modifiche ed integrazioni e all'art. 615-*ter* del codice penale ("*Accesso abusivo ad un sistema informatico o telematico*").
Tale manleva è dunque da considerarsi necessaria, e di normale prassi, per lo svolgimento delle attività in Accordo che saranno svolte in ambiente di test e pertanto non causerebbero disservizi. Con il medesimo documento, le attività – nonostante siano eseguite con la massima diligenza e professionalità – punite dal codice penale e DC, sono espressamente autorizzate da parte di ARPAC e quindi non perseguibili ai fini di legge.

ARPAC dichiara di avere tutte le necessarie approvazioni, autorizzazioni e/o permessi incluse eventuali approvazioni, autorizzazioni e/o permessi di terze parti, richieste per eseguire le attività di cui al punto (i) e (ii) del presente articolo, relativamente ai sistemi informativi già identificati come parte del perimetro di analisi nonché a quelli che lo saranno seguendo le modalità descritte al precedente punto (ii). ARPAC terrà indenne e manleverà il RTI da qualsiasi pretesa, danno o spesa che dovesse derivare in capo a quest'ultima o essere avanzata nei confronti di RTI, causate dalla mancanza di tali approvazioni, autorizzazioni e/o permessi.

Nel caso in cui una qualsiasi Autorità (comprese quelle di Polizia e giudiziarie) rilevi le nostre attività di intrusione nei vostri sistemi, la informerete del fatto che eravate pienamente a conoscenza dello svolgimento di tali attività, espressamente richieste da ARPAC e che pertanto l'accesso da parte nostra è da considerarsi espressamente autorizzato da ARPAC.

Articolo 5. Le Parti convengono che l'Attività di Verifica di Sicurezza:

(i) verrà espletata dal RTI con il coinvolgimento di personale altamente specializzato e dotato delle necessarie qualifiche, che svolgerà tali attività con la diligenza di cui all'art. 1176, secondo comma, del codice civile, sotto la supervisione del Referente Tecnico di ARPAC medesimo (come infra definito), in orario lavorativo nel corso delle seguenti giornate:

a. dal giorno 01/10/2025 al giorno 31/12/2025 per le attività di vulnerability assessment;

b. dal giorno 01/10/2025 al giorno 31/12/2025 per le attività di penetration testing;

(ii) non prevede alcuna verifica di tipo "DoS (*Denial of Service*)" e/o "DDoS (*Distributed Denial of Service*)" da parte del RTI e non avrà come obiettivo l'interruzione intenzionale dei servizi offerti dai siti che saranno individuati come perimetro di analisi e/o di altri servizi e/o siti residenti sull'infrastruttura informatica di ARPAC. In merito al punto, ARPAC è tuttavia consapevole che le attività di verifica espletate potrebbero, nonostante le appropriate cautele adottate, comportare una interruzione dei servizi; in tale evenienza il RTI ed il proprio personale coinvolto sono sin d'ora manlevati ai sensi e per gli effetti di quanto previsto al precedente articolo 4, ricordando sia che la manleva sia necessaria e di normale prassi per lo svolgimento delle attività in Accordo nonché che le attività saranno svolte in ambiente di test senza la possibilità di causare disservizi. Tale documento manleva dunque le attività dalla persecuzione ai fini di legge che tali attività prevedono solitamente, come indicato dal codice penale e DC;

(i) l'esecuzione dell'"**Attività di Verifica di Sicurezza**" è eseguita a titolo oneroso secondo quanto descritto nella proposta di collaborazione per servizi professionali c.d. "Piano Operativo" del 13/11/2024 protocollato ARPA Campania N. 0071773/2024 del 18/11/2024 e pubblicato con Deliberazione del Direttore Generale di ARPA Campania N. 584 DEL 26/11/2024.;

(ii) le Attività di Verifica di Sicurezza condotte dall'esterno avranno origine dagli indirizzi , e che tali indirizzi sono stati comunicati a ARPAC in modo che quest'ultima possa distinguere e monitorare il traffico di rete da essi generato.

(iii) Nell'ambito dell'intervento, il personale dell'RTI non effettuerà alcuna attività di modifica, implementazione, cancellazione e/o impostazione direttamente sui sistemi informativi oggetto dell'attività.

Nell'attività di testing che verrà concordata con il team del Cliente e condotta, verranno tassativamente escluse le tecniche il cui scopo primario è:

- degradare le performance del sistema o della rete (Denial of service sia locale che distribuito) o portare all'interruzione del servizio,
- creare alterazioni o distruzioni permanenti dei dati,

- inserire codice potenzialmente dannoso a titolo permanente negli ambienti di test degli applicativi, negli apparati di rete e nei sistemi operativi,
- esporre gli applicativi, la rete ed i server ad attacchi di soggetti esterni ed estranei all'ambito dell'analisi (es. backdoor, trojan horse, rootkit).

Altresì il personale dell'RTI si impegna a non utilizzare né divulgare informazioni, dati e qualsiasi altro elemento, di cui verrà a conoscenza nel corso delle operazioni di testing, inerenti alla struttura e all'accesso ai sistemi del Cliente.

Ai fini dello svolgimento del nostro incarico, è essenziale che i dati, le informazioni e le spiegazioni da noi acquisite non ci siano comunicate fraudolentemente o, deliberatamente o negligentemente, occultate o distorte. Di conseguenza, ove il Cliente subisca qualsivoglia perdita, che avrebbe potuto essere evitata qualora i dati, le informazioni o le spiegazioni non ci fossero state comunicate fraudolentemente o, deliberatamente o negligentemente, occultate o distorte, è sin d'ora pattuito che l'RTI sia sollevata da qualsiasi responsabilità e/o passività che potesse emergere nei confronti del Cliente.

Articolo 6. Al termine dell'Attività di Verifica di Sicurezza, il RTI dovrà:

(i) sviluppare e consegnare al Referente Tecnico di ARPAC (come infra identificato), da trasmettere all'indirizzo di cui al successivo art. 12, un "executive summary" dedicato al Security Manager di ARPAC, contenente le seguenti evidenze:

(a.) il riepilogo delle caratteristiche tecniche dei sistemi oggetto dell'Attività di Verifica di Sicurezza, inclusivo della descrizione dello scopo che la predetta si prefigge di raggiungere,

(b.) la descrizione dettagliata della metodologia adottata dalla stessa RTI per la conduzione dell'Attività di Verifica di Sicurezza;

(c.) l'elencazione completa delle caratteristiche tecniche delle eventuali vulnerabilità rilevate in occasione dell'Attività di Verifica della Sicurezza espletata,

(d.) qualora per la conduzione dell'Attività di Verifica di Sicurezza fossero state attuate da RTI simulazioni di attacco e/o intrusione complesse, l'evidenza delle modalità utilizzate in tale occasione;

(e.) qualsiasi informazione utile per supportare il Referente Tecnico di ARPAC nell'attività di eliminazione e/o di mitigazione delle vulnerabilità riscontrate, nonché ogni indicazione valida (inclusa l'individuazione di eventuali riferimenti esterni a cui rivolgersi) per approfondire eventuali tematiche di rilievo emerse in occasione dell'Attività di Verifica di Sicurezza conclusa;

(ii) restituire prontamente a ARPAC ogni dato/documento/supporto/flusso eventualmente ricevuto e/o elaborato ai fini dell'esecuzione dell'Attività di Verifica di Sicurezza. Pur non essendo previsto alcuno scambio d'informazioni e dati tra ARPAC ed il RTI ai fini della conduzione delle attività di verifica, fatto salvo per il rapporto di verifica o "executive summary", il RTI porrà in essere ogni attività di carattere tecnico ed organizzativo finalizzata alla cancellazione, dai propri archivi fisici e/o informatici dei Dati Riservati (come infra definiti) incidentalmente raccolti, elaborati e memorizzati ai sensi dell'Accordo e di qualsiasi altro dato, documento, supporto, flusso ricevuto od elaborato. Qualora questa attività non fosse possibile, tali dati saranno considerati Dati Riservati e tutelati dall'obbligo confidenzialità nei termini di cui all'art. 9 dell'Accordo.

Articolo 7. In relazione all'esecuzione dell'**Attività di Verifica di Sicurezza**, il RTI si impegna nei confronti di ARPAC ad:

(i) impiegare personale proprio altamente specializzato o dotato delle necessarie qualifiche, che svolgerà tale Attività con la più volte richiamata diligenza di cui all'art. 1176, secondo comma, del Codice civile,

(ii) applicare uno specifico presidio sulle attività eseguite, attraverso il monitoraggio delle configurazioni dei sistemi di analisi di sicurezza utilizzati, al fine di garantire l'impossibilità a nuocere ai Sistemi Informativi di ARPAC,

(iii) informare tempestivamente ARPAC di tutti gli eventi e le circostanze che potrebbero, per qualsiasi motivo, pregiudicare la corretta esecuzione dell'Attività di Verifica di Sicurezza restando fermo l'obbligo del RTI, in questa ipotesi, di formulare e segnalare a ARPAC tempestivamente ogni possibile soluzione per consentire il tempestivo ripristino dell'Attività di Verifica di Sicurezza.

Articolo 8. ARPAC, dal canto suo, si impegna nei confronti del RTI, per tutta la durata dell'Attività di Verifica di Sicurezza, a collaborare col RTI al fine di garantire a quest'ultimo la corretta esecuzione dell'Attività di Verifica di Sicurezza, fornendo al medesimo le informazioni all'uopo necessarie, informando al proprio interno le strutture dedicate alla gestione dei servizi erogati tramite i range IP e le URL oggetto di analisi e a comunicare tempestivamente al RTI ogni fatto o circostanza, a sua conoscenza, che possa ostacolare o ritardare l'esecuzione dell'Attività di Verifica di Sicurezza.

Articolo 9. Il RTI, anche promettendo il fatto del terzo ai sensi dell'art. 1381 cod. civ., si impegna a mantenere riservatezza, confidenzialità e segretezza su tutti i dati riservati - intendendosi per tali qualsiasi informazione, notizia, dato e documento (compresi idee, progetti, disegni, *know how*, processi, fotografie, dati contabili, video, ecc.) relativi a ARPAC o a terzi, di cui il medesimo sia venuto o venga in possesso o a conoscenza, o che comunque abbia raccolto, nel corso ed a seguito dell'esecuzione dell'Attività di Verifica di Sicurezza e che, per normativa primaria e secondaria, regola deontologica, intrinseca natura od altra circostanza, siano da ritenere coperti da riservatezza (di seguito, i "**Dati Riservati**"). In particolare, il RTI, salvo solo obblighi di legge o ordini di competenti Autorità, non copierà, tratterà, comunicherà, diffonderà, divulgherà, né comunque utilizzerà i Dati Riservati, in qualsiasi modo o forma e anche in via indiretta, per fini diversi da quelli previsti nell'Accordo e direttamente funzionali all'esecuzione del medesimo in conformità al grado di diligenza professionale previsto dal precedente articolo 7, punto (i).

Salvo documentate eccezioni finalizzate, in ogni caso, a dare esecuzione alle obbligazioni derivanti dall'Accordo, qualsiasi tipo di supporto cartaceo, magnetico o di altro tipo contenente *software*, dati e/o informazioni di ARPAC ed utilizzato per l'espletamento dell'Attività di Verifica di Sicurezza non potrà uscire dai locali del RTI e/o di ARPAC, se non dietro specifica autorizzazione da parte di quest'ultima.

L'obbligo di riservatezza rimarrà fermo anche successivamente alla cessazione dell'Attività di Verifica di Sicurezza, fino a quando i Dati Riservati saranno divulgati da parte del legittimo titolare o diverranno legittimamente di pubblico dominio.

Il RTI si obbliga, in conformità con le disposizioni di legge applicabili, ad adottare tutte le misure necessarie per non pregiudicare la riservatezza di tuti i Dati Riservati acquisiti ai sensi dell'Accordo; a tal scopo il RTI dovrà attuare, in particolare, misure di sicurezza, logica e fisica, idonee ad impedire l'accidentale o incontrollata eliminazione, alterazione, consultazione, esportazione, lettura, copiatura dei Dati Riservati da parte di terzi.

ARPAC, anche promettendo il fatto del terzo ai sensi dell'art. 1381 cod. civ., si impegna a mantenere la massima riservatezza, confidenzialità e segretezza sul contenuto dei report di cui al precedente articolo 6, punto (i) e delle "Metodologie" di RTI intendendosi, con tale termine, qualsiasi know how e/o segreto commerciale (incluso, ma non limitato, alla descrizione delle metodologie, standard report, agli strumenti utilizzati ai fini dell'esecuzione dell'Attività di Verifica di Sicurezza oggetto dell'Accordo). In particolare, ARPAC, salvo solo obblighi di legge o ordini di competenti Autorità, non copierà, tratterà, comunicherà, diffonderà, divulgherà, né comunque utilizzerà quanto sopra indicato, in qualsiasi modo o forma e anche in via indiretta, per fini diversi da quelli previsti nell'Accordo e direttamente funzionali all'esecuzione del medesimo, restando espressamente esclusa la possibilità, per ARPAC, di divulgare in favore di soggetti ed imprese terze il contenuto e/o i risultati recati dai predetti documenti predisposti dal RTI in esecuzione del presente Accordo, salvo diversa autorizzazione scritta del RTI medesima.

Articolo 10. L'attività di verifica di sicurezza disciplinata dal presente accordo può comportare il trattamento di dati personali connessi agli utenti o agli amministratori che accedono ai sistemi in ambito.

Articolo 11. Al fine di garantire una migliore gestione ed esecuzione dell'Attività di Verifica di Sicurezza, le Parti nominano come propri referenti:

per il RTI:

Società: Deloitte Consulting s.r.l. S.B.

e-mail:

numero di telefono: (di seguito, il "**Referente Tecnico di RTI**"),

per ARPAC:

Responsabile per la Transizione al Digitale di ARPAC

e-mail:

numero di telefono: (di seguito, il "**Referente Tecnico di ARPAC**").

Articolo 12. Lo scambio fra le Parti di comunicazioni o documentazione ai sensi dell'Accordo dovrà avvenire per iscritto ai seguenti indirizzi che le Parti eleggono come proprio domicilio *ex* art. 1335 del Codice civile:

per il RTI:

Società: Deloitte Consulting s.r.l. S.B.

e-mail:

numero di telefono:

per ARPAC:

Responsabile per la Transizione al Digitale di ARPAC

e-mail:

numero di telefono:

È fatta salva la facoltà del RTI e di ARPAC di modificare i suddetti indirizzi, dandone idonea preventiva comunicazione, a pena di inopponibilità, l'una all'altra, secondo quanto disposto dal successivo comma del presente articolo; comunicazione nella quale dovrà essere indicato il termine da cui il nuovo indirizzo diverrà efficace.

Salvo che sia diversamente previsto in altre disposizioni dell'Accordo, le comunicazioni aventi ad oggetto l'ordinaria operatività potranno essere scambiate tra le Parti con ogni mezzo, anche telematico (compresa la posta elettronica), purché documentabile su supporto duraturo, agli indirizzi di cui sopra ovvero a quelli che le Parti si renderanno noti nel corso dell'esecuzione dell'Accordo.

Articolo 13. L'Accordo è disciplinato dalla legge italiana. Qualsiasi controversia derivante dall'interpretazione o dall'esecuzione dell'Accordo sarà devoluta in via esclusiva alla competenza del Foro di Milano.

****

Distinti saluti.

Milano, data della firma digitale

Per ARPAC

Il Rappresentante Legale di ARPAC

(firmato digitalmente)

Per il Raggruppamento Temporaneo d'Imprese tra la mandataria Deloitte Consulting S.r.l. S.B. e le mandanti EY Advisory S.p.A. e Teleco S.r.l.

Il procuratore della mandataria Deloitte Consulting S.r.l. S.B.

(firmato digitalmente)

Allegato A all'Accordo VAPT tra Agenzia Regionale per la Protezione Ambientale della Campania (ARPAC) e RTI.

DETERMINAZIONE CONTRATTUALE PER L'ATTRIBUZIONE DELLA RESPONSABILITÀ DEL TRATTAMENTO

TRA

Agenzia Regionale per la Protezione Ambientale della Campania (ARPAC), con sede legale in Via Vicinale S. Maria del Pianto - Centro Polifunzionale, Torre 1, 80143 Napoli, C.F. n° 07407530638 nella persona del Rappresentante Legale, Avv. Luigi Stefano Sorvino, in qualità di Direttore Generale, giusta i poteri conferitigli da Decreto della Giunta Regionale della Campania n° 25 in data 10/04/2024 (nel seguito per brevità anche "ARPAC" o l'"Amministrazione"),

e

- **Deloitte Consulting S.r.l. S.B.,** sede legale in Milano, Via Santa Sofia n. 28, Capitale Sociale deliberato Euro 4.700.000,00 – sottoscritto e versato per Euro 3.715.283,48, iscritta al Registro delle Imprese di Milano al n. 03945320962, P. IVA 03945320962, domiciliata ai fini del presente atto in Milano, Via Santa Sofia n.28, in persona del Procuratore Dott. Fabio Battelli, nella sua qualità di impresa mandataria capo-gruppo del Raggruppamento Temporaneo oltre alla stessa le mandanti:
- **EY Advisory S.p.A.** *con* sede legale in Milano, Via Meravigli n.14, capitale sociale Euro 2.250.000,00=, iscritta al Registro delle Imprese di Milano al n. 13221390159, P. IVA 13221390159, domiciliata ai fini del presente atto in Milano, via Tortona n.25;
- **Teleco S.r.l.**, con sede legale in Roma, Via Rosazza n. 26, capitale sociale Euro 950.000,00=, iscritta al Registro delle Imprese di Milano al n. 02856220922, P. IVA 02856220922, domiciliata ai fini del presente atto in Milano, via Tortona n.25, giusta mandato collettivo speciale con rappresentanza autenticato dal notaio in Roma dott. Lorenzo Cavalaglio repertorio n. 14.339 del 3 febbraio 2022;

Disgiuntamente definite anche come "Parte" o congiuntamente come le "Parti"

LE SUDDETTE PARTI PREMETTONO CHE

- sono attualmente in corso contatti tra la Società e RTI concernenti la seguente attività di verifica preliminare dei sistemi di sicurezza adottati dalla Società in relazione ai range IP, i quali verranno stabiliti nel corso della durata contrattuale, al mero ed esclusivo fine di rilevare ed analizzare eventuali punti di criticità (intendendosi per tali vulnerabilità, elementi che possono compromettere la confidenzialità dei dati, impattare in maniera rilevante sull'attività di *business* della Società e che dovrebbero essere risolte non appena possibile e/o mitigate con opportune soluzioni tecnologiche durante l'esecuzione delle operazioni di risoluzione delle anomalie e/o criticità riscontrate) - ed indicare, conseguentemente, alla Società i necessari interventi correttivi e/o eventuali

migliorie da apportare dal punto di vista tecnico e tecnologico (di seguito “Attività Principale”).

- RTI gode di competenza e conoscenze tecniche per svolgere l’Attività Principale, alla quale RTI intende dare esecuzione.
- In relazione alle operazioni connesse all’Attività Principale aventi ad oggetto dati personali, RTI gode di competenza e conoscenze tecniche in relazione alle finalità e modalità delle stesse, come previsto dalla normativa in materia di tutela dei dati personali.
- La Società svolge il ruolo di Titolare del trattamento dei dati personali da esso operato, in quanto decide sulle finalità e modalità dello stesso.
- RTI adotta, nell’ambito della propria organizzazione, misure di sicurezza adeguate, sia a livello tecnico che organizzativo, alla specificità delle operazioni sui dati personali connesse alle prestazioni contrattuali, in modo tale da dare le più ampie garanzie che le attività di trattamento appaltate siano conformi alla disciplina rilevante posta a tutela dei dati personali.
- La Società nella qualità di Titolare del trattamento sopra riportata intende conferire a RTI – che accetta – l’incarico di Responsabile del trattamento oggetto del presente mandato.

Le Parti, in relazione a tale incarico, intendono regolare con il presente mandato i loro reciproci rapporti in tema di disciplina dei trattamenti di dati personali effettuati da RTI per conto della Società.

Articolo 1: PREMESSE ED ALLEGATI

Le premesse e gli allegati, insieme agli articoli, costituiscono parte integrante e sostanziale del presente contratto.

Articolo 2: AMBITI DI COMPETENZA

Le Parti si danno reciprocamente atto di conoscere ed applicare, nell’ambito delle proprie organizzazioni, tutte le vigenti norme in materia di trattamento dei dati personali, sia primarie che secondarie, rilevanti per la corretta gestione del Trattamento.

Articolo 3: RISPETTO DEI PRINCIPI

Le Parti individuano le più opportune modalità e precauzioni affinché le operazioni inerenti al Trattamento avvengano nel rispetto dei principi generali fissati dall’articolo 5 del Generali Data Protection Regulation (GDPR) e dal diritto interno dello Stato membro in cui si esplica il Trattamento, con particolare riferimento ai principi di liceità, correttezza e trasparenza nei confronti degli interessati, nonché di limitazione delle finalità, minimizzazione dei dati ed esattezza del trattamento.

Articolo 4: OGGETTO

Con la stipula del presente contratto, redatto in conformità al GDPR, la Società designa RTI – che con la firma del presente contratto, accetta - quale soggetto “Responsabile” del trattamento dei dati personali – secondo la definizione di cui all’art. 4, nr. 8) ed ai sensi dell’art. 28 del GDPR.

Articolo 5: OPERAZIONI DI TRATTAMENTO, TIPOLOGIA DI DATI TRATTATI E CATEGORIE DI INTERESSATI

Il trattamento oggetto del presente contratto (per brevità “Trattamento” o “Operazioni di Trattamento”) consta delle operazioni effettuate sui dati personali tra cui, a titolo esemplificativo,

raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione cancellazione dei dati personali implicati dalla Attività Principale.

I dati oggetto di trattamento possono riguardare sia dati comuni che sensibili e sono costituiti, a titolo esemplificativo e non esaustivo, dalle informazioni contenute dai sistemi informativi della Società che costituiscono il target dell'Attività Principale.

Le categorie di interessati ai quali i dati si riferiscono sono le categorie di soggetti cui si riferiscono i dati personali di cui sopra.

Particolare cura e diligenza dovrà prestare RTI nello svolgimento delle operazioni di trattamento che prevedono l'utilizzo di dati sensibili e di quelli relativi a condanne penali e reati.

Articolo 6: DIRITTI ED OBBLIGHI RECIPROCI

Il Responsabile – per quanto di propria competenza – è tenuto per sé, per i propri dipendenti e per chiunque collabori con la sua attività – a garantire la riservatezza, integrità e qualità dei dati e ad utilizzarli esclusivamente per le finalità sopra specificate e nell'ambito delle istruzioni impartite dal Titolare del trattamento.

Il Titolare si riserva il diritto di verificare in ogni momento la conformità dell'operato del Responsabile alle istruzioni impartite e di sottoporre a specifici audit, le misure tecniche ed organizzative implementate dal Responsabile al fine di garantire un livello adeguato di sicurezza dei dati e dei trattamenti operati per conto del Titolare. Nel valutare l'adeguato livello di sicurezza assicurato dal Responsabile, il Titolare tiene conto, in special modo, dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati per suo conto.

Articolo 7: VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Il Responsabile è tenuto a dare immediata notizia al Titolare di ogni eventuale illegittimo trattamento dei dati personali operato in esecuzione del presente contratto nell'ambito della propria organizzazione, al fine di consentire al Titolare la notifica tempestiva della violazione di dati personali all'Autorità di controllo e all'interessato, nei casi in cui tali adempimenti siano dovuti dal titolare del trattamento, ai sensi degli art. 33 e 34 del GDPR.

Articolo 8: REGISTRO DEL TRATTAMENTO

Le Parti provvedono reciprocamente alla registrazione delle informazioni descrittive del Trattamento ("Registro") nelle forme e secondo le modalità indicate dall'articolo 30 del GDPR nonché alla pertinente mappatura dei dati.

Il Registro aggiornato dovrà essere esibito su richiesta dell'Autorità di controllo ad opera della Parte che riceve la richiesta.

Articolo 9: MISURE DI SICUREZZA

Il Responsabile rispetta le misure di sicurezza prescritte dal Titolare ed adottate nei locali dove si effettuano i trattamenti, ai sensi e per gli effetti degli articoli da 32 a 36 del GDPR.

Inoltre, il Responsabile garantisce:

- La corretta tenuta ed archiviazione dei dati comuni e sensibili presenti presso gli uffici in cui avvengono le operazioni di trattamento;
- L'individuazione nominativa per iscritto degli Incaricati del trattamento di cui al successivo articolo 10;

- La limitazione degli accessi ai locali in cui sono presenti gli archivi di settore.

In relazione alle possibili variazioni nelle operazioni o nei dati trattati – oggetto delle Operazioni di Trattamento - il Responsabile adotta – secondo criteri di efficienza e con modalità da comunicare al Titolare con congruo anticipo – quelle misure urgenti idonee a salvaguardare la riservatezza, l'integrità e la completezza dei dati oggetto delle Operazioni di Trattamento.

Il Responsabile deve, comunque, assicurarsi che tali misure di sicurezza siano idonee a ridurre al minimo i rischi di:

- Distruzione o perdita intenzionale o accidentale dei dati;
- Accesso non autorizzato;
- Trattamento non consentito;
- Trattamento non conforme alla finalità delle Operazioni di Trattamento.

Articolo 10: SUB-RESPONSABILI E INCARICATI DEL TRATTAMENTO

Il Responsabile ha facoltà di individuare in autonomia gli Incaricati del trattamento che agiscono sotto la sua autorità. L'individuazione deve essere nominativa.

Contestualmente alla designazione, il Responsabile si fa carico di fornire istruzioni scritte e dettagliate agli Incaricati circa le modalità del trattamento, in ottemperanza a quanto disposto dall'articolo 29 del GDPR, dalla Legge nazionale applicabile, dall'Accordo e dal presente contratto.

Sarà cura del Responsabile vincolare i propri Incaricati al segreto, anche per il periodo successivo all'estinzione del rapporto di lavoro intrattenuto con il Responsabile, in relazione alle Operazioni di Trattamento da essi eseguite.

Articolo 11: SUPERVISIONE E CONTROLLO DEGLI INCARICATI

Il Responsabile esercita supervisione e controllo diretto su coloro che egli avrà individuato quali incaricati del trattamento e organizza – anche consultando il Titolare – le proprie attività in modo compatibile e funzionale alle prescrizioni della legge e del presente contratto.

Articolo 12: DURATA E CESSAZIONE DEL TRATTAMENTO

La durata del trattamento è in stretta relazione a quella dell'Accordo salvo disdetta anticipata del presente contratto comunicata per iscritto dal Titolare al Responsabile. All'atto della cessazione, per qualsiasi causa, delle Operazioni di Trattamento da parte del Responsabile, questi sarà tenuto, a discrezione del Titolare:

a) a restituire al Titolare i dati personali oggetto delle Operazioni di Trattamento

oppure

b) a provvedere alla loro integrale distruzione,

in entrambi i casi rilasciando contestualmente un'attestazione scritta che presso lo stesso Responsabile non ne esiste alcuna copia.

Articolo 13: RESPONSABILITA'

Fermo restando il riparto delle responsabilità verso terzi danneggiati previsto a carico del Titolare e del Responsabile dall'art. 82 del GDPR, nei rapporti reciproci il Titolare mantiene indenne RTI – per qualsiasi danno, incluse spese legali – da pretese di qualsiasi tipologia avanzate nei suoi confronti nei casi le normali operazioni di trattamento richieste dal servizio dovessero comportare un danno al cliente o agli interessati del trattamento. Per contro, nel caso di trattamenti non coerenti con il mandato ricevuto o non conformi con le previsioni normative, RTI

mantiene indenne il cliente, o risponde in solido con il cliente per danni a individui come richiesto dal GDPR.

Articolo 14: RAPPORTI CON IL GARANTE

Il Responsabile – previa tempestiva consultazione con il Titolare – adempie, a norma di legge, alle prescrizioni del Garante privacy.

In particolare:

- fornisce informazioni o integrazioni di informazioni richieste sulle Operazioni di Trattamento;
- consente l'effettuazione di controlli;
- consente l'accesso alle raccolte e alle banche di dati oggetto delle Operazioni di Trattamento;
- compie quanto necessario per una tempestiva esecuzione dei provvedimenti inibitori, di natura temporanea.

Articolo 15: VIGILANZA

Al fine di garantire che l'assetto organizzativo predisposto e che le misure tecniche adottate dal Responsabile siano un costante ed efficace presidio del complesso sistema posto dalla normativa vigente a tutela dei dati personali, il Responsabile consente al Titolare di verificare in ogni momento, anche attraverso specifiche attività di audit, l'adeguatezza dell'assetto organizzativo e tecnico predisposto dalla stessa, per garantire che le attività del Trattamento siano conformi a norma.

Articolo 16: FLUSSI ESTERI

Nel caso in cui talune operazioni del Trattamento comportino un flusso transfrontaliero di dati personali verso Paesi non appartenenti all'Unione Europea, la Parte esportatrice si farà carico di verificare la sussistenza dei requisiti di legittimità del trasferimento secondo quanto previsto dalle disposizioni del Capo V del GDPR.

Articolo 17: DECORRENZA

Il presente contratto ha efficacia dalla data della sottoscrizione ad opera di entrambi, Titolare e Responsabile.

Articolo 18: RISOLUZIONE E RECESSO

Le ipotesi di risoluzione fanno riferimento a quanto indicato nel Contratto esecutivo – LOTTO 2 CIG Accordo Quadro 8884642E81, CIG "derivato": B457DB055E del 11/02/2025. Le modalità di recesso sono disciplinate, rispettivamente, agli artt. 14 e 15 dell'Accordo Quadro, cui si rinvia, nonché agli artt. "SUBAPPALTO" "TRASPARENZA DEI PREZZI", "TRACCIABILITÀ DEI FLUSSI FINANZIARI" e "TRATTAMENTO DEI DATI PERSONALI" del documento Contratto esecutivo succitato.