CAPITOLATO TECNICO

ACQUISIZIONE DI LICENZA CLOUD DI UNA PIATTAFORMA SAAS QUALIFICATA ACN DI CYBERSECURITY XDR/MDR UNIFICATA E SOC, PER LA PROTEZIONE DELLE INFRASTRUTTURE IT DA ATTACCHI AVANZATI – DURATA QUADRIENNALE.

1. OGGETTO DEL SERVIZIO

L'appalto ha per oggetto l'acquisizione delle licenze e l'attivazione del servizio relativo alla piattaforma SaaS qualificata ACN di 2° livello (*https://www.acn.gov.it/portale/w/sa-5614*) di cybersecurity per la protezione delle infrastrutture IT da attacchi avanzati. Cynet fornisce una piattaforma nativamente unificata per il rilevamento, prevenzione, correlazione, indagine e risposta attraverso endpoint, dispositivi mobili, utenti, reti, applicazioni SaaS e cloud.

Il servizio di cybersecurity è fondamentale per l'Ente a salvaguardia delle postazioni di lavoro, server e dispositivi mobili da malware, ransomware e altre pericolose minacce informatiche con comprovati sistemi di protezione degli endpoint, controllo dei dispositivi, protezione mobile e gestione della postura di sicurezza degli endpoint per rilevare e risolvere le vulnerabilità e i rischi di configurazione.

2. SPECIFICHE TECNICHE MINIME OBBLIGATORIE

Nel presente Capitolato Tecnico sono riportate le Specifiche Tecniche Minime che dovranno essere soddisfatte, per tutti gli elementi componenti il servizio di cybersecurity e per tutte le attività necessarie per l'erogazione dei servizi.

Tutte le specifiche e le caratteristiche tecniche, indicate nel presente documento con i tag [SpecTech. xx], sono da intendersi *specifiche tecniche minime obbligatorie*.

[SpecTech 1.]
La piattaforma deve offrire una protezione completa ed efficiente per i team di sicurezza IT, garantendo una protezione superiore rispetto ai normali sistemi antivirus corporate. Il servizio deve anche fornire in modo nativo le tecnologie di sicurezza essenziali per la protezione dell'organizzazione in un'unica una piattaforma automatizzata e semplificata, con protezioni di livello Enterprise e un supporto di un team di esperti di sicurezza 24 ore su 24, 7 giorni su 7.
Le funzionalità incluse nella piattaforma dovranno operare in sinergia per offrire la migliore protezione possibile alla superficie d'attacco in continua espansione.

[SpecTech 2.]
Deve essere garantito un monitoraggio continuo del comportamento degli utenti per rilevare e bloccare gli insider malintenzionati e gli account compromessi, con l'analisi del comportamento dell'utente, le tecnologie di Deception e Domain Filtering.

[SpecTech 3.]
Il sistema deve rilevare e impedire agli aggressori furtivi di accedere alla rete e di muoversi al suo interno, oltre a bloccare le connessioni a siti dannosi con la Network Analytics ed il Port Scanning.

[SpecTech 4.]
Il sistema deve identificare automaticamente, dare priorità e correggere i rischi per la sicurezza in tutte le applicazioni SaaS e Cloud.

[SpecTech 5.]
Deve essere fornita una funzionalità di E-mail Security, per proteggere caselle e-mail istituzionali, ricercando allegati e link dannosi e bloccando i mittenti e i domini a rischio per ridurre al minimo il rischio di questo punto di ingresso per gli attacchi.

[SpecTech 6.]
La piattaforma deve essere in grado di rilevare e rispondere alle minacce attraverso integrazioni di terze parti, come Active Directory, Firewalls e applicazioni SaaS/Cloud.

Via Dante, 1 – 07026 OLBIA (OT) Tel. 0789/52220

[SpecTech 7.]
Deve essere garantito un **SOC** (***S**ecurity **O**perations **C**enter*) 24/7 per tutta la durata del contratto, con un un team di esperti di cybersecurity di altissimo livello che lavori 24 ore su 24 per proteggere e monitorare gli ambienti IT e affrontando immediatamente le minacce. Incluso nel SOC ci deve essere anche il monitoraggio e l'intervento proattivo degli analisti con un sevizio **MDR** (***M**anaged **D**etection and **R**esponse*) completo, che in caso di necessità dovranno lanciare remediation manuali dalla console della piattaforma in tempo reale per bloccare sul nascere gli attacchi Cyber.

[SpecTech 8.]
Deve essere garantito un Log Management e XDR per raccogliere dati di log ad alta priorità e scoprire in modo rapido e accurato le minacce all'ambiente.
In particolare, il sistema dovrà raccogliere i LOG dai 2 firewall Fortinet (*utilizzati dall'Ente per la difesa perimetrale*) e dai dispositivi di rete (*router, switch, wlc e AP*), rendendoli visibili in una console per 90 giorni e disponibili su richiesta per log che hanno più di 90 giorni; i log dovranno essere conservati e disponibili per tutta la durata del contratto.

[SpecTech 9.]
Si richiede una automazione End-to-End in grado di indagare e correggere automaticamente tutti i componenti dell'attacco all'interno dell'ambiente utilizzando le best practice di Incident Response con una tecnologia avanzata di automazione della risposta.

[SpecTech 10.]
Deve essere fornito il supporto all'installazione degli agent della piattaforma di cybersecurity e alla rimozione dell'attuale antivirus.

[SpecTech 11.] Reportistica su incidenti informatici
Il supporto tecnico e redazione di reportistica nel caso di un incidente informatico.

Inclusi nelle licenze, senza costi aggiuntivi, devono essere comprese le attività di Incident Response e i report tecnici di Incident Response (IR) redatti tramite il team di specialisti di Cybersecurity, in cui vengono inclusi tutti i dettagli critici necessari sia ai team tecnici per sanare l'infrastruttura ICT, sia al management per comprendere l'impatto del data breach, sia per le comunicazioni alle autorità competenti.

Il report tecnico deve includere le seguenti sezioni e informazioni chiave:

a. Sintesi Esecutiva (*Executive Summary*): impatto complessivo dell'attacco, ossia una panoramica ad alto livello sui danni stimati, sui sistemi compromessi e sulla gravità dell'evento.
b. Stato dell'incidente: il punto della situazione al momento della redazione (*es. se la minaccia è ancora attiva, parzialmente contenuta o completamente eradicata*).
c. Dettagli della Minaccia e Analisi della "Root Cause": vettore di ingresso (*Root Cause Analysis*), identificazione del punto debole o della vulnerabilità sfruttata dagli attaccanti per penetrare nella rete (*es. phishing, credenziali compromesse, vulnerabilità software non patchata*).
d. Mappatura della catena cinematica dell'attacco (***Attack Chain***): ricostruzione passo-passo dei movimenti dell'attaccante all'interno della rete, inclusi i tentativi di movimento laterale ed eventuale esfiltrazione di dati.
e. Indicatori di Compromissione (***IoC***): elenco tecnico di hash di file maligni, indirizzi IP degli attaccanti, domini di comando e controllo (***C2***) e chiavi di registro modificate rilevate durante l'analisi forense.
f. Timeline Visiva dell'Incidente: una cronologia dettagliata che ripercorre l'evento dal primo momento di compromissione ipotizzato (*Patient Zero*), passando per il rilevamento dei sistemi forniti dalla piattaforma di cybersecurity, fino alle prime azioni di contenimento e alla successiva bonifica.
g. Attività di Contenimento ed Eradicazione (*Containment & Eradication*), misure immediate applicate: quali azioni (*spesso automatizzate tramite playbook o eseguite manualmente dal team, degli esperti in cybersecurity*) sono state intraprese, come l'isolamento degli endpoint infetti, il blocco del traffico di rete malevolo o la disabilitazione di account utente compromessi.

Via Dante, 1 – 07026 OLBIA (OT) Tel. 0789/52220

h. Analisi dei file (File Analysis): esiti del reverse-engineering o dell'analisi di file e processi sospetti inviati alla piattaforma.
i. Eventuali Raccomandazioni e Gap di Controllo (*Lessons Learned*): identificazione delle eventuali lacune di sicurezza: Il report evidenzia i punti deboli nei controlli di sicurezza esistenti che hanno permesso il successo dell'attacco.
j. Piano d'azione per il recupero (*Recovery*) e la prevenzione: suggerimenti concreti e personalizzati per irrobustire le difese.

Se l'incidente è complesso o prolungato nel tempo, deve essere rilasciato un report ad interim (*per aggiornare tempestivamente gli stakeholder sulle direzioni dell'investigazione e sul successo del contenimento*) in attesa del report tecnico definitivo completo di analisi forense profonda. Questo documento permetterà di effettuare la prima notifica al Garante "con riserva", per poi inviare il report tecnico definitivo e completo elaborato dal fornitore come integrazione successiva.

Il report tecnico e l'analisi degli esperti CyOps devono fornire i dati oggettivi indispensabili per compilare la notifica ufficiale ed evitare pesanti sanzioni per omessa o tardiva comunicazione.

Il report definitivo deve includere evidenze formali specifiche per le autorità:
1) Perimetro del Breach ed Entità del Danno
2) Evidenze per l'Accountability (Principio di Responsabilità)
3) Mitigazione del Rischio Immediata

3. DURATA
La durata del contratto è di **4 anni**.

4. TEMPI DI ESPLETAMENTO DEL SERVIZIO
Il servizio dovrà essere attivato dalla data della stipula del contratto.

5. GARANZIA SUL SOFTWARE
Si richiede una garanzia, a copertura dei difetti software. Qualunque danno che dovesse derivare da tali difetti sarà a carico della ditta fornitrice.

6. SERVIZIO DI FORNITURA LICENZE SOFTWARE
Il servizio è relativo alla fornitura di:

Prodotti software, cloud computing e servizi
Cynet - Future-proof All in One platform **4** anni.
Cynet - Centralized Log management - CLM 60 GB mese con 90 Days + Cold Storage **4** anni.

7. SERVIZIO DI ASSISTENZA
Il servizio di assistenza è relativo a:
a. assistenza telefonica dal lunedì al venerdì nelle normali ore di lavoro dell'Ente o tramite e-mail che dovranno essere indicate dal Technical account manager italiano (TAM) di Cynet che assegnato all'Ente, a partire dall'evasione delle licenze Cynet;
b. fornitura degli aggiornamenti software in seguito a variazioni di legge; l'aggiornamento di tipo normativo dovrà essere tale da consentire l'utilizzo della procedura nei termini temporali e funzionali previsti dalle leggi;
c. fornitura di eventuali aggiornamenti migliorativi periodici; in caso di nuove release, l'aggiornamento deve essere eseguito direttamente dalla console cloud, qualificata ACN QC2, con la supervisione del TAM (*Technical Account Manager***)** assegnato e senza dover fare azioni specifiche su ogni singolo agent installato sugli endpoint dell'ente;
d. fornitura di nuove versioni/pacchetti, quando disponibili; nel caso di versioni/pacchetti di prodotto che comprendono nuove funzionalità il TAM dovrà informare il Servizio ICT dell'Ente;
e. ripristino del buon funzionamento dei programmi per eventuali difetti, o errori dovuti alla progettazione e/o realizzazione degli stessi; in caso di criticità dell'agent su alcuni hosts dell'ente il TAM assegnato, coinvolto

Via Dante, 1 – 07026 OLBIA (OT) Tel. 0789/52220

anche il team di supporto tecnico e se necessario il team Product saranno a disposizione per reinstallare l'agent, testare e trovare soluzioni in tempi rapidi senza rallentare le normali attività dell'ente.

8. COLLAUDO

Il collaudo consisterà nella verifica dell'attivazione del servizio richiesto.

9. VERBALE DI AVVIO DEL SERVIZIO

A seguito di collaudo positivo verrà redatto un verbale di avvio del servizio a cura del RUP.

10. PAGAMENTO

Il corrispettivo comprende la fornitura delle licenze e il servizio di manutenzione e assistenza tecnica relativo alla piattaforma SaaS Cynet e verrà effettuato sotto forma di **canone annuale anticipato per anno di competenza**.

Con tale corrispettivo la ditta si intende compensata di qualsiasi suo avere o pretendere dall'Amministrazione Comunale per il servizio e la fornitura di che trattasi, senza alcun diritto a nuovi o maggiori compensi.
Il pagamento verrà eseguito mediante bonifico bancario/postale previa presentazione di regolare fattura che dovrà pervenire obbligatoriamente in modalità elettronica mediante l'utilizzo del sistema informatico messo a disposizione sul sito www.fatturapa.gov.it.
La fattura, intestata al Comune di Olbia – Via Dante 1, 07026 Olbia – P.I. 00920660909, potrà essere emessa successivamente agli adempimenti descritti al successivo art. 9.

Sull'importo netto del servizio di manutenzione l'Ente applicherà una ritenuta dello 0,50 per cento. Tale ritenuta potrà essere svincolata soltanto in sede di liquidazione finale dopo l'approvazione del certificato di regolare esecuzione da parte del RUP e previo rilascio del DURC con esito positivo.
La fattura dovrà contenere i seguenti dati:

1. riferimento alla **TD (*Trattativa Diretta*)** sul MEPA cui si riferisce la fornitura/servizio;
2. descrizione dettagliata del servizio/fornitura;
1. numero e data della determinazione del Dirigente di Settore che verrà comunicata a seguito di affidamento;
2. il codice univoco ufficio: **J65OW6;**
3. il CIG;
4. la dicitura "scissione dei pagamenti – art. 17 ter del DPR n. 633/1972".

I pagamenti verranno effettuati, entro i termini di legge decorrenti dalla data di protocollazione della fattura, tramite bonifico su conto corrente bancario/postale.
In caso di fattura irregolare il termine di pagamento verrà sospeso dalla data di contestazione dell'Amministrazione. Dalle fatture saranno detratte le eventuali penalità applicate.

11. REVISIONE PREZZI

La stazione appaltante monitora semestralmente l'andamento degli indici di cui all'articolo 60 del codice, al fine di valutare se sussistono le condizioni per l'attivazione delle clausole di revisione prezzi. Al verificarsi di condizioni che determinino l'attivazione della clausola di revisione, la stazione appaltante comunica all'appaltatore i prezzi revisionati, da applicare alle prestazioni da eseguire.
La revisione dei prezzi si applica quando la variazione (in aumento o in diminuzione) del costo del servizio in oggetto supera il 5% dell'importo complessivo del contratto. La revisione opera nella misura dell'80% del valore eccedente la variazione del 5% applicata alle prestazioni da eseguire dopo l'attivazione della clausola di revisione.

Sulla base delle disposizioni contenute nell'allegato II.2-bis l D.Lgs. n. 36/2023, relativamente al CPV: 48730000-4 – "Pacchetti software di sicurezza" nella categoria "MEPA Beni - Licenze software", e dell'indice indicato nella Tabella D.2, ai fini della revisione, si utilizza il seguente indice ISTAT: PPS – ATECO 62 "Produzione di software, consulenza informatica e attività connesse";

La variazione è calcolata come differenza tra l'indice individuato al momento della rilevazione e il corrispondente valore al mese del provvedimento di affidamento. In caso di sospensione o proroga dei termini di affidamento nelle ipotesi di

cui all'articolo 1, commi 3, 4 e 5 dell'Allegato 1.3., il valore di riferimento per il calcolo della variazione è quello relativo al mese di scadenza del termine massimo per l'aggiudicazione, come individuato dall'articolo 1, commi 1 e 2 del predetto Allegato.
Qualora l'applicazione della revisione dei prezzi non garantisca il principio di conservazione dell'equilibrio contrattuale, è fatta salva la possibilità per la stazione appaltante o l'appaltatore di invocare la risoluzione per eccessiva onerosità sopravvenuta del contratto, ai sensi dell'art. 2, comma 2, dell'Allegato II.2-bis.

12. DIRETTORE DELL'ESECUZIONE

Il ruolo del direttore dell'esecuzione sarà ricoperto dal tecnico del Servizio ICT **Gianmarco Delogu**.

13. CONTROLLO TECNICO-CONTABILE E AMMINISTRATIVO

In caso di regolarità del DURC, il RUP emetterà lo Stato di Avanzamento del Servizio (SAS) ed il certificato di pagamento (CP) nel quale verrà indicato l'importo che dovrà essere riportato in fattura. Il SAS ed il CP verranno trasmessi alla ditta aggiudicataria la quale entro 5 giorni dal ricevimento dovrà restituirli firmati.
In caso di ottenimento del documento unico di regolarità contributiva negativo, il Punto Ordinante avrà il diritto di trattenere dal certificato di pagamento l'importo corrispondente all'inadempienza ai sensi dell'art. 11, comma 6 del D. Lgs. 36/2023.
All'atto della firma la Ditta aggiudicataria potrà aggiungere le eventuali contestazioni che ritiene opportune, rispetto alle operazioni di verifica.
Successivamente all'emissione del S.A.S. e del C.P. ed alla restituzione degli stessi debitamente firmati da parte della ditta aggiudicataria, quest'ultima potrà emetterà fattura.
Nel SAS sarà indicato:
1) gli estremi del contratto e degli eventuali atti aggiuntivi;
2) l'indicazione dell'esecutore;
3) il nominativo del direttore dell'esecuzione;
4) il tempo prescritto per l'esecuzione delle prestazioni e le date delle attività di effettiva esecuzione delle prestazioni;
5) l'importo totale ovvero l'importo a saldo da pagare all'esecuto.

14. GARANZIA DEFINITIVA

Al fine della stipula del contratto, dovrà essere costituita garanzia definitiva, a scelta del concorrente, sotto forma di cauzione o fideiussione, ai sensi dell'articolo 53 comma 4 e con le modalità di cui all'art. 117 commi 7 e 12 del D.lgs. 36/2023. La fideiussione può essere bancaria o assicurativa o rilasciata dagli intermediari finanziari iscritti nell'elenco speciale di cui all'articolo 107 del D.Lgs. 385/1993, che svolgono in via esclusiva o prevalente attività di rilascio di garanzie, a ciò autorizzati dal Ministero dell'economia e delle finanze.

15. PENALI

Nella tabella di seguito riportata, sono definiti i livelli di gravità delle possibili criticità che possono interessare la suite applicativa fornita:

Livello	Descrizione
Liv_01	**Anomalia bloccante**: l'intera suite è indisponibile agli utenti o gravemente degradata. Call and email the customer.
Liv_02	**Anomalia grave**: funzioni critiche della suite sono indisponibili agli utenti o gravemente degradate. Call and email the customer.
Liv_03	**Anomalia media**: funzioni non critiche della suite sono indisponibili agli utenti o gravemente degradate, oppure funzioni critiche sono lievemente degradate. Email Customer.
Liv_04	**Anomalia lieve**: funzioni non critiche della suite sono lievemente degradate. Email Customer
Liv_05	**manutenzione adeguativa**: criticità della suite fornita che comportano la necessità di aggiornamenti correttivi.

Via Dante, 1 – 07026 OLBIA (OT) Tel. 0789/52220

a. Indicatori temporali di intervento

Di seguito si riportano in tabella le definizioni degli indicatori temporali, che saranno utilizzati per la definizione degli SLA e delle penali.

Indicatore	Descrizione
TPC: **T**empo di **P**resa in **C**arico	Intervallo di tempo intercorrente fra la richiesta di intervento a fronte di un malfunzionamento e la conferma del Fornitore di aver recepito la richiesta e attivato le procedure necessarie per l'effettuazione dell'intervento; richiesta di intervento e conferma devono avvenire tramite mail, PEC o telefonata, con caricamento sul sistema di Trouble Ticketing del Fornitore.
TR: **T**empo **R**isoluzione	Intervallo di tempo intercorrente fra la conferma del Fornitore di aver preso in carico la chiamata e l'effettiva risoluzione del malfunzionamento segnalato mediante invio da parte del Fornitore tramite chiusura sul sistema di Ticketing del Fornitore e contestuale e-mail di un messaggio di chiusura intervento. Nel caso in cui l'Ente non ritenga il malfunzionamento risolto (e non emetta quindi il relativo certificato di accettazione, inviando al fornitore contestazione dell'intervento effettuato), l'intervento si riterrà non concluso e il tempo di risoluzione verrà nuovamente calcolato al momento in cui il Fornitore darà nuova segnalazione di chiusura intervento a cui segua l'accettazione da parte dell'Ente.

b. SLA e Penali

Livello	**SLA** (*ore consecutive*)				**Penali** (*‰ per mille*)			Importo
	TPC		TR		TPC + TC		Perc. Appl.	
Liv_01	≤	1	≤	4	>	5	0,10%	
Liv_02	≤	2	≤	6	>	8	0,05%	
Liv_03	≤	6	≤	24	>	32	0,04%	
Liv_04	≤	12	≤	48	>	60	0,04%	
Liv_05	≤	24	≤	168	>	192	0,03%	

**La percentuale si applica per ogni giorno successivo al superamento dello SLA.*

Nel caso di ritardo nell'attivazione del servizio, per ogni giorno di ritardo si applica una penale giornaliera pari a 1‰ (uno per mille) dell'importo di aggiudicazione, al netto dell'IVA.
Gli eventuali inadempimenti contrattuali che daranno luogo all'applicazione delle penali di cui ai precedenti commi, verranno contestati al Fornitore contraente dal RUP per iscritto. Il Fornitore contraente dovrà comunicare in ogni caso le proprie deduzioni al RUP nel termine massimo di 5 (cinque) giorni dalla stessa contestazione. Qualora dette deduzioni non siano accoglibili a giudizio del RUP ovvero non vi sia stata risposta o la stessa non sia giunta nel termine indicato potranno essere applicate al Fornitore contraente le penali come sopra indicate a decorrere dall'inizio dell'inadempimento.
Tutte le penali di cui al presente articolo sono contabilizzate in detrazione in occasione del pagamento immediatamente successivo al verificarsi della relativa condizione.
La richiesta e/o il pagamento delle penali di cui al presente articolo non esonera in nessun caso il Fornitore contraente dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale, fatta salva la facoltà per il RUP di risolvere il Contratto nei casi in cui questo è consentito.

16. TRATTAMENTO DEI DATI

Ai sensi del D.lgs n° 196/2003, si informa che i dati comunicati dalla ditta saranno oggetto di trattamento nel rispetto dei principi della vigente normativa.

17. INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

L'aggiudicatario dichiara di aver ricevuto prima della sottoscrizione del contratto di fornitura/servizio le informazioni di cui agli artt. 13 e 14 del regolamento UE n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche "Regolamento UE"), circa il trattamento dei dati personali, conferiti per la sottoscrizione e l'esecuzione del contratto stesso e di essere a conoscenza dei diritti riconosciuti ai sensi della predetta normativa. Tale informativa è contenuta nella lettera di richiesta conferma preventivo, che deve intendersi in quest'ambito integralmente trascritto.

Via Dante, 1 – 07026 OLBIA (OT) Tel. 0789/52220

Con la sottoscrizione del contratto, il rappresentante legale del fornitore acconsente espressamente al trattamento dei dati personali come sopra definito, si impegna ad adempiere agli obblighi di rilascio dell'informativa e di richiesta del consenso, ove necessario, nei confronti delle persone fisiche interessate di cui sono forniti dati personali nell'ambito dell'esecuzione del contratto per le finalità descritte nel disciplinare di gara e sopra richiamate;
La S.A. acconsente espressamente al trattamento da parte dell'aggiudicatario dei dati relativi alla fatturazione, rendicontazione e monitoraggio per le finalità connesse all'esecuzione del contratto.
Inoltre, in adempimento agli obblighi di legge che impongono la trasparenza amministrativa (art. 20 D.Lgs. 36/2023), il fornitore prende atto della pubblicazione e diffusione dei dati e/o della documentazione che la legge impone di pubblicare, tramite il sito internet www.comune.olbia.ot.it sezione amministrazione trasparente.

Con la sottoscrizione del contratto il fornitore acconsente espressamente al trattamento dei dati personali e si impegna a improntare il trattamento dei dati ai principi di correttezza, liceità e trasparenza nel pieno rispetto della normativa vigente (Regolamento UE 2016/679), ivi inclusi gli ulteriori provvedimenti, comunicati ufficiali, autorizzazioni generali, pronunce in genere emessi dall'Autorità Garante per la protezione dei dati personali.
In particolare, si impegna ad eseguire i soli trattamenti funzionali, necessari e pertinenti all'esecuzione delle prestazioni contrattuali e, in ogni modo, non compatibili con le finalità per cui i dati sono stati raccolti.

L'aggiudicatario si impegna ad adottare le misure di sicurezza di natura fisica, logica, tecnico ed organizzativa adeguate a garantire un livello di sicurezza adeguato al rischio, ivi compresa quelle specificate nel contratto, unitamente ai suoi allegati; si impegna, altresì ad osservare le vigenti disposizioni in materia di sicurezza e privacy e a farle osservare ai relativi dipendenti e collaboratori, opportunamente autorizzati al trattamento dei Dati personali. L'aggiudicatario prende atto che l'ente potrà operare verifiche periodiche, ispezioni ed audit, anche tramite soggetti terzi autorizzati dallo stesso, volti a riscontrare l'applicazione e l'adeguatezza delle misure di sicurezza dei dati personali applicate.

18. ART. 26 – CODICE DI COMPORTAMENTO.

Ai sensi dell'art. 2, comma 3, del D.P.R. 62/2013 (Regolamento recante codice di comportamento dei dipendenti pubblici a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165), la Società, tramite i propri operatori, è tenuta al rispetto degli obblighi di condotta previsti nel Codice di comportamento dei dipendenti pubblici, nonché del Codice di comportamento integrativo del Comune di Olbia approvato con deliberazione di Giunta Comunale n° 132 del 23/04/2024 e pubblicato in "Amministrazione Trasparente" nel sito istituzionale al seguente link: https://servizi.comune.olbia.ot.it/L190/?idSezione=15201&id=&sort=&activePage=&search=

19. RISERVATEZZA

a. Il Fornitore ha l'obbligo di mantenere riservati i dati e le informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e comunque, a conoscenza, di non divulgarli in alcun modo e in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione del contratto e comunque per i cinque anni successivi alla cessazione di efficacia del rapporto contrattuale.
b. L'obbligo di cui al precedente comma sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione del contratto; tale obbligo non concerne i dati che siano o divengano di pubblico dominio.
c. Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché dei propri eventuali subappaltatori e dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di segretezza anzidetti.
d. In caso di inosservanza degli obblighi di riservatezza, l'Amministrazione ha la facoltà di dichiarare risolto di diritto il contratto, fermo restando che il Fornitore sarà tenuto a risarcire tutti i danni che dovessero derivare all'Amministrazione.
e. Il Fornitore potrà citare i contenuti essenziali del contratto, nei casi in cui ciò fosse condizione necessaria per la partecipazione del Fornitore medesimo a gare e appalti.
f. Il Fornitore si impegna, altresì, a rispettare quanto previsto dalla normativa sul trattamento dei dati personali (Regolamento UE n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) e ulteriori provvedimenti in materia.

Via Dante, 1 – 07026 OLBIA (OT) Tel. 0789/52220

20. CONTROVERSIE

Qualsiasi controversia dovesse sorgere in merito all'interpretazione, esecuzione, validità o efficacia del contratto sarà di competenza esclusiva del **Foro di Tempio Pausania**.

21. NORME APPLICABILI

Per quanto non espressamente previsto nelle condizioni contenute nel presente documento, trovano applicazione le norme di Legge vigenti in materia di affidamento di contratti pubblici, con particolare riferimento al D.Lgs. 36/2023, nonché quelle proprie del Codice civile e le condizioni generali di contratto del bando "MEPA Beni - Licenze software".

Olbia, **25/06/2026**

Il RUP
Dott. Sebastiano Bellu

SEBASTIANO BELLU
30.06.2026 13:38:16
GMT+02:00

Via Dante, 1 – 07026 OLBIA (OT) Tel. 0789/52220