AFFIDAMENTO DIRETTO ALLA SOCIETÀ IN HOUSE PASUBIO TECNOLOGIA S.R.L., AI SENSI DELL'ART. 50, COMMA 1, LETT. B) DEL D.LGS. 36/2023, DEI SERVIZI SPECIALISTICI IT DI AFFIANCAMENTO, SERVIZI SOC (SECURITY OPERATIONS CENTER) AS A SERVICE E PROJECT MANAGEMENT OFFICE, PER LA REALIZZAZIONE DEL PROGETTO DENOMINATO "VICENZA (CYBER)SICURA RINFORZIAMO LA DIFESA DIGITALE DELLA NOSTRA CITTÀ" - ID PROGETTO 75_WP9_A8_COMUNE DI VICENZA - CUP B37H24000910006, AVVISO PUBBLICO ACN N. 08/2024, FINANZIATO DALL'UNIONE EUROPEA – NEXT GENERATION UE – PNRR, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY", MEDIANTE TRATTATIVA DIRETTA SUL MEPA

FOGLIO PATTI E CONDIZIONI

CUP B37H24000910006
CPV 72220000-3 Servizi di consulenza in sistemi informatici e assistenza tecnica (prevalente)
CPV 72410000-7 Servizi di provider (secondario)
CPV: 72224000-1 Servizi di consulenza per la gestione di progetti (secondario)

Indice generale

1. Responsabile Unico del Progetto....3
2. Premessa e contesto....3
3. Oggetto dell'appalto e importo....4
4. Durata....5
5. Caratteristiche generali del servizio....5
   - Censimento degli asset....5
   - Campagne di phishing....6
   - Valutazione rischio ed esposizione degli asset, inclusa valutazione reti....6
   - Installazione, configurazione e formazione piattaforma MISP....6
   - Redazione playbook in caso di incidente e aggiornamento post-simulazioni....7
   - Startup SIEM e affiancamento operativo....7
   - Vulnerability assessment mensile....8
   - Consulenza per analisi e hardening Active Directory....8
   - Servizi PMO qualificati....8
6. Cronoprogramma....9
7. Obblighi specifici PNRR....9
8. Rispetto del principio di non arrecare danno significativo all'ambiente (DNSH)....10
9. Prescrizioni generali....10
10. Soggetti ammessi, requisiti di ordine generale e altre cause di esclusione....10

Settore Informatico Comunale
Corso Andrea Palladio 98 - Vicenza
tel. 0444 221349
mail: sistemi_informativi@comune.vicenza.it
pec: vicenza@cert.comune.vicenza.it

11. Modalità di presentazione dell'offerta....11
12. Termine di presentazione dell’offerta....12
13. Riserva di non aggiudicazione....12
14. Direttore dell’esecuzione del contratto....12
15. Avvio dell’esecuzione del contratto....12
16. Divieto di modifiche introdotte dall’esecutore....12
17. Varianti introdotte dalla stazione appaltante....12
18. Variazioni entro il 20 per cento....13
19. Verifica di conformità....13
20. Penali in caso di ritardo....13
21. Risoluzione del contratto....14
22. Recesso....15
23. Pagamenti....16
24. Svincolo della garanzia definitiva....17
25. Cessione del contratto e subappalto....17
26. Garanzia definitiva e stipula del contratto....17
27. Nuove convenzioni Consip....18
28. Estensione degli obblighi di condotta previsti dal codice di comportamento dei dipendenti pubblici....18
29. Protocollo di legalità....18
30. Foro competente....18
31. Informativa ai sensi del D.Lgs. n. 2003/196 e s.m.i. e Regolam. UE n.2016/679 (GDPR)....19
32. Designazione a responsabile trattamento dati personali (art. 28 Reg. UE 2016/67)....19

1. Responsabile Unico del Progetto

Il Responsabile unico del Progetto, ai sensi dell'art. 15 del D.Lgs. 36/2023, è il Direttore del Servizio Informatico Comunale, dr. Lorenzo Beggiato.

(email: sistemi_informativi@comune.vicenza.it tel 0444 221357).

2. Premessa e contesto

Il Next Generation EU, approvato nel 2020, è il fondo europeo creato per sostenere i paesi colpiti dalla pandemia, e, in tale ambito, l'Italia ha sviluppato il Piano Nazionale di Ripresa e Resilienza (PNRR), da attuare mediante "Italia Digitale 2026", il piano strategico finalizzato a migliorare le infrastrutture digitali e modernizzare la Pubblica Amministrazione (PA).

In tale ambito, l'Agenzia per la Cybersicurezza Nazionale (ACN), individuata quale soggetto attuatore dell'investimento dal Dipartimento per la Trasformazione Digitale, ha pubblicato l'Avviso 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 PNRR, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" – M1C1I1.5, finalizzati ad irrobustire le infrastrutture e i servizi digitali del Sistema Paese nonché migliorare le competenze specialistiche necessarie e a garantire adeguati livelli di cyber resilienza.

In particolare, l'Avviso concerne:

- il finanziamento per la realizzazione di un censimento dei livelli di maturità della postura di sicurezza dei servizi e delle infrastrutture digitali delle PA;
- il finanziamento per la realizzazione di un piano programmatico di potenziamento, sia a breve che a medio-lungo termine, delle capacità cyber, volto a supportare il percorso di trasformazione digitale sicura della PA;
- il finanziamento per la realizzazione di interventi di potenziamento cyber a breve-medio termine dei servizi e delle infrastrutture in essere della PA,

con l'obiettivo di dotare i Soggetti attuatori degli interventi dei necessari strumenti e processi per una gestione del rischio cyber in linea con le migliori pratiche nazionali e internazionali.

Per l'attuazione degli interventi di potenziamento delle capacità cyber della PA e il perseguimento dei relativi Target previsti dal PNRR, la strategia adottata dall'Agenzia per la Cybersicurezza Nazionale ha previsto l'individuazione e la selezione di progetti da finanziare mediante procedure ad evidenza pubblica rivolte alle Pubbliche Amministrazioni.

Il Comune di Vicenza ha presentato domanda di partecipazione con il Progetto denominato *"Vicenza (cyber)sicura - rinforziamo la difesa digitale della nostra città"* (nel seguito *Progetto)*- ID 75_WP9_A8_Comune di Vicenza - CUP B37H24000910006, a valere sul PNRR, finanziato dall'Unione Europea – Next Generation UE - Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I.5, che è risultato totalmente finanziato.

Il cronoprogramma del bando prevede che tutte le attività siano completate entro il 31/12/2025.

La proposta progettuale presentata dal Comune di Vicenza, prevede 27 azioni, articolate nei 5 interventi previsti dal bando:

1. Governance e programmazione cyber
2. Gestione del rischio cyber e della continuità operativa
3. Gestione e risposta agli incidenti di sicurezza
4. Gestione delle identità digitali e degli accessi logici
5. Sicurezza delle applicazioni, dei dati e delle reti.

Per ciascun intervento possono essere presentate attività riconducibili a una o più delle seguenti specifiche tipologie di intervento:

A) Analisi della postura di sicurezza e definizione di un piano di potenziamento
B) Miglioramento dei processi e dell'organizzazione
C) Formazione e miglioramento della consapevolezza delle persone
D) Progettazione e sviluppo di nuovi sistemi e tecnologie.

Con la presente procedura, il Comune di Vicenza intende affidare le attività afferenti al Progetto che sono descritte ai paragrafi che seguono.

3. Oggetto dell'appalto e importo

Il presente appalto ha per oggetto l'affidamento diretto, ai sensi dell'art. 50, comma 1, lett. b) del D.Lgs. 36/2023, alla Società in house Pasubio Tecnologia S.r.l., dei servizi specialistici IT di affiancamento, servizi SOC (Security operations center) as a service, e Project Management Office, per la realizzazione del Progetto denominato "Vicenza (cyber)sicura - rinforziamo la difesa digitale della nostra città" - ID 75_WP9_A8_Comune di Vicenza - CUP B37H24000910006, a valere sul PNRR, finanziato dall'Unione Europea – Next Generation UE - Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I.5, come di seguito dettagliato.

Importo dell'appalto:

n.	Descrizione servizi/beni/lavori	CPV	P (principale) S (secondaria)	Importo
1	Servizi specialistici IT di affiancamento	72220000-3	P	€ 82.000,00
2	Servizi SOC (Security operations center) as a service	72410000-7	S	€ 32.800,00
3	Servizi di PMO	72224000-1	S	€ 25.000,00
A) Importo a base di gara				€ 139.800,00
B) Oneri per la sicurezza da interferenze non soggetti a ribasso *[indicare € 0,00 in caso di assenza di rischi]*				€ 0,00
A) + B) Importo complessivo				€ 139.800,00

L’importo è da intendersi comprensivo di tutti i servizi, le provviste, le prestazioni, le spese accessorie e qualsiasi altro onere, espresso e non dal presente foglio patti e condizioni, inerente e conseguente all'esecuzione del servizio di cui trattasi.

Non sono ammesse offerte in aumento o pari all’importo base definito.

Non sono previsti costi per oneri di sicurezza.

Non sono stati riscontrati rischi da interferenze trattandosi di servizi di natura intellettuale.

4. Durata

Il contratto decorre dalla data di stipula e si concluderà il 31/12/2025, salvo proroghe disposte dall’Agenzia per la Cybersicurezza Nazionale (ACN).

5. Caratteristiche generali del servizio

L’affidamento ha per oggetto le attività dettagliate nel seguito, organizzate in *“interventi”* e *“tipologie di interventi”*, come articolato nella scheda di Progetto presentato e che concorrono alla realizzazione del Progetto denominato “Vicenza (cyber)sicura - rinforziamo la difesa digitale della nostra città” - ID 75_WP9_A8_Comune di Vicenza - CUP B37H24000910006, a valere sul PNRR, finanziato dall’Unione Europea – Next Generation UE - Missione 1 - Componente 1 - Investimento 1.5 “Cybersecurity” M1C1I.5.

Le attvità, classificate in base agli interventi e relative tipologie di intervento, oggetto dell’appalto sono nel seguito dettagliate; il fornitore dovrà produrre una proposta progettuale che, per ognuna delle attività di seguito elencate e descritte, definisca nel dettaglio le modalità operative di esecuzione, le figure specialistiche coinvolte e i deliverables previsiti.

Censimento degli asset
Intervento 1. Governance e programmazione cyber
Tipologia di intervento A. Analisi della postura di sicurezza e definizione di un piano di potenziamento

L'attività di censimento degli asset rappresenta un passaggio fondamentale per costruire una solida base informativa sulla quale impostare le successive strategie di sicurezza. Il servizio dovrà essere svolto da figure professionali specialistiche e prevedere l’analisi degli attuali strumenti di censimento, la verifica del loro stato di completezza e aggiornamento anche tramite l'implementazione e la configurazione della piattaforma Zabbix come strumento principale per il discovery e il monitoraggio continuo degli asset, da affiancare all’ottimizzazione dell’attuale software ManageEngine per la componente di gestione e controllo degli endpoint. Il servizio prevede una fase iniziale di configurazione della piattaforma e definizione dei parametri di scansione e discovery più appropriati per l’ecosistema IT del Comune.

Il censimento verrà condotto in modo incrementale, partendo da una mappatura di alto livello dell'infrastruttura per poi scendere progressivamente nel dettaglio. Verranno identificati e catalogati tutti gli asset fisici (server, workstation, dispositivi di rete) e virtuali (macchine virtuali, container, servizi cloud), registrando per ciascuno le informazioni critiche come collocazione, stato operativo, versioni software/firmware e dipendenze con altri sistemi.

Il servizio deve includere supporto specialistico al team di lavoro del comune nelle fasi di analisi dell'architettura e nell'identificazione delle dipendenze tra i sistemi, oltre ad attività di project management per la supervisione dell'intero processo, a garanzia del rispetto delle tempistiche, coordinando le interazioni necessarie con il personale IT del Comune.

Campagne di phishing

Intervento: 1. Governance e programmazione cyber
Tipologia di intervento: C. Formazione e miglioramento della consapevolezza delle persone

L'azione di cui sopra deve prevedere l'individuazione e implementazione di una piattaforma di simulazione a sostegno della campagna di phishing ed una ttività che preveda almeno le seguenti fasi

1. esecuzione di una campagna iniziale di phishing simulato per verificare il livello di consapevolezza del personale comunale:
2. progettazione e erogazione di un intervento formativo mirato, basato sui risultati ottenuti nella campagna di cui al punto precedente che fornisca al personale gli strumenti pratici per riconoscere e gestire correttamente i tentativi di phishing;
3. esecuzione di una seconda campagna di phishing simulato, finalizzata a verificare l'efficacia dell'intervento formativo nella capacità del personale di riconoscere e gestire correttamente i tentativi di phishing.

Valutazione rischio ed esposizione degli asset, inclusa valutazione reti

Intervento: 2. Gestione del rischio cyber e della continuità operativa
Tipologia di intervento: A. Analisi della postura di sicurezza e definizione di un piano di potenziamento

La valutazione del rischio ed esposizione degli asset rappresenta un'attività cruciale per comprendere il livello di sicurezza complessivo dell'infrastruttura comunale e identificare le aree che necessitano di interventi prioritari. Il servizio dovrà prevedere ed integrare un'analisi tecnica delle vulnerabilità con una valutazione dettagliata dell'architettura di rete e delle misure di protezione esistenti.

L'analisi dovrà porevedere un assessment con una mappatura dell'architettura di rete identificando i flussi di traffico, le zone di sicurezza e i punti di interconnessione critici. Particolare attenzione dovrà essere posta sull'analisi della segmentazione di rete e sull'efficacia dei controlli di sicurezza perimetrali. Per ciascun asset censito dovrà essere condotta una valutazione del rischio.

Particolare attenzione dovrà essere posta nella verifica di criticità che possono compromettere i livelli di protezione dei dati personali, con riferimento alle normative di settore applicabili.

Installazione, configurazione e formazione piattaforma MISP

Intervento: 2. Gestione del rischio cyber e della continuità operativa
Tipologia di intervento: C. Formazione e miglioramento della consapevolezza delle persone
Tipologia di intervento: D. Progettazione e sviluppo di nuovi sistemi e tecnologie

L'attività prevede l'implementazione della piattaforma MISP utilizzando la versione open source del

software. Il progetto prevede l'hosting iniziale della piattaforma sulla infrastruttura del fornitore per poi effettuare la migrazione sul datacenter comunale al termine del periodo di implementazione e formazione.

L'attività prevede una fase di progettazione dell'architettura, definendo i requisiti tecnici e di sicurezza per l'implementazione della piattaforma. Il fornitore provvederà all'installazione e configurazione del sistema, in stretto raccordo con il gruppo di lavoro del Comune, implementando le best practice di sicurezza e integrando la piattaforma con le fonti di threat intelligence selezionate.

Il servizio deve prevedere la formazione del personale IT comunale che dovrà gestire la piattaforma. Il programma formativo, strutturato in sessioni teoriche e pratiche, dovrà coprire tutti gli aspetti operativi: dalla gestione quotidiana della piattaforma, all'analisi degli indicatori di compromissione, fino alle procedure di manutenzione e aggiornamento.

Nel periodo di progetto, il fornitore deve garantire un servizio di monitoraggio continuo della piattaforma verificandone il corretto funzionamento e intervenendo tempestivamente in caso di necessità, affiancando e supportando il personale comunale nell'acquisizione delle necessarie competenze per la gestione della piattaforma.

La migrazione finale dell'infrastruttura MISP sul datacenter comunale sarà pianificata e eseguita con particolare attenzione per garantire la continuità del servizio, preservando tutti i dati e le configurazioni implementate.

Redazione playbook in caso di incidente e aggiornamento post-simulazioni

Intervento: 3. Gestione e risposta agli incidenti di sicurezza
Tipologia di intervento: B. Miglioramento dei processi e dell'organizzazione

L'attività consisterà nella redazione della prima versione del playbook, che prevede, mediante l'adozione di un approccio di Cybersecurity di tipo "risk-based", l'adozione di una piattaforma dedicata che, unitamente, ad un sistema avanzato di firewall con analyzer, costituirà un primo nucleo embrionale per un futuro sistema SOAR.

Startup SIEM e affiancamento operativo

Intervento: 3. Gestione e risposta agli incidenti di sicurezza
Tipologia di intervento: C. Formazione e miglioramento della consapevolezza delle persone
Tipologia di intervento: D. Progettazione e sviluppo di nuovi sistemi e tecnologie

L'attività di startup e affiancamento operativo per il SIEM prevede un supporto specialistico durante le fasi di configurazione iniziale e la successiva messa a regime della piattaforma implementata dal Comune sulla propria infrastruttura. L'obiettivo è rendere il personale comunale pienamente autonomo nella gestione del sistema attraverso un percorso strutturato di configurazione, formazione e simulazioni operative.

L'attività di formazione ed addestramento deve essere consentire al personale comunale di acquisire competenze e capacità in relazione alla gestione ordinaria della piattaforma che alla risposta a scenari di incidente e dovrà pertanto prevedere adeguate esercitazioni pratiche di

incident response in cui verranno riprodotti diversi scenari di attacco e compromise detection, permettendo al personale di acquisire familiarità con l'analisi degli alert, la gestione delle evidenze e le procedure di escalation.

Per l'intero periodo del progetto il fornitore dovrà garantire supporto operativo, condividere best practice e affiancare il personale comunale nell'analisi di eventi reali o sospetti.

Vulnerability assessment mensile

Intervento: 5. Sicurezza delle applicazioni, dei dati e delle reti
Tipologia di intervento: A. Analisi della postura di sicurezza e definizione di un piano di potenziamento

L'attività di Vulnerability Assessment prevede l'esecuzione di scansioni mensili sulla base di un piano concordato con l'amministrazione. Il fornitore dovrà definire l'architettura della soluzione e le policy di scansione, assicurando un approccio sistematico e ripetibile alle attività di assessment, si occuperà dell'esecuzione delle scansioni mensili, dell'analisi dei risultati e della produzione della reportistica tecnica. Le attività di VA seguiranno un processo strutturato che include la configurazione iniziale delle policy di scansione, l'esecuzione delle analisi in finestre temporali concordate per minimizzare l'impatto sui sistemi produttivi, l'analisi e validazione dei risultati per eliminare i falsi positivi, e la produzione di report dettagliati con le vulnerabilità riscontrate.

Per ogni sessione di VA dovrà essere prodotta apposita reportistica che include la prioritizzazione delle vulnerabilità secondo standard CVSS, raccomandazioni tecniche per la remediation e trend analysis rispetto alle scansioni precedenti.

Consulenza per analisi e hardening Active Directory

Intervento: 4. Gestione delle identità digitali e degli accessi logici
Tipologia di intervento: A. Analisi della postura di sicurezza e definizione di un piano di potenziamento
Tipologia di intervento: B. Miglioramento dei processi e dell'organizzazione
Tipologia di intervento: D. Progettazione e sviluppo di nuovi sistemi e tecnologie

L'attività di consulenza per l'hardening dell'Active Directory prevede il supporto specialistico al team comunale nell'analisi e ottimizzazione della configurazione AD per la definizione di linee guida, la validazione delle scelte tecniche e la verifica dei risultati.

Servizi PMO qualificati

Intervento: 1. Governance e programmazione cyber
Tipologia di intervento: A. Analisi della postura di sicurezza e definizione di un piano di potenziamento

Il servizio prevede la messa a disposizione di un Project Manager qualificato che coordini la pianificazione e il monitoraggio di tutte le attività garantendo una visione integrata dello stato di avanzamento e facilitando il processo decisionale attraverso la produzione di reportistica direzionale. Le attività includono la gestione del piano di progetto integrato, il coordinamento delle diverse stream progettuali, il monitoraggio dei rischi e delle criticità, la gestione del budget e la produzione della reportistica di governo.

6. Cronoprogramma

Le attività oggetto del presente affidamento dovranno concludersi nei tempi previsti dal cronoprogramma del Progetto denominato “Vicenza (cyber)sicura - rinforziamo la difesa digitale della nostra città” - ID 75_WP9_A8_Comune di Vicenza - CUP B37H24000910006, a valere sul PNRR, finanziato dall’Unione Europea – Next Generation UE - Missione 1 - Componente 1 - Investimento 1.5 “Cybersecurity” M1C1I.5, finanziato e approvato da ACN.

Per ogni singola attività dovrà essere prodotto e sottoscritto apposito verbale di collaudo, con l’ausilio della modulistica fornita dall’Agenzia per la Cybersicurezza Nazionale, con le “Linee guida per i soggetti attuatori individuati tramite Avvisi Pubblici”.

7. Obblighi specifici PNRR

Il servizio affidato è finanziato con fondi PNRR, Finanziato dall’Unione Europea – Next Generation EU, Missione 1, Componente 1 “Investimento 1.5 “Cybersecurity” M1C1I1.5.

Il fornitore, nello svolgimento delle prestazioni e delle attività oggetto dell’appalto, è tenuto al rispetto e all’attuazione dei principi e degli obblighi specifici del PNRR.

Il fornitore è tenuto ad assumere gli obblighi specifici del PNRR, di cui all’art. 8 dell’Avviso Pubblico n. 08/2024 dell’Agenzia per la Cybersicurezza Nazionale (ACN) , e si impegna a rispettare i principi trasversali, quali tra l’altro il principio del contributo all’obiettivo climatico e digitale c.d. Tagging, della parità di genere c.d. Gender Equality, della protezione e valorizzazione dei giovani e del superamento dei divari territoriali, nel rispetto delle specifiche norme in materia.

L’affidatario che occupa oltre cinquanta dipendenti, è tenuto a consegnare, al momento della presentazione dell'offerta, a pena di esclusione, copia dell'ultimo rapporto periodico sulla situazione del personale maschile e femminile redatto ai sensi dell’articolo 46, decreto legislativo n. 198 del 2006, unitamente all’attestazione di conformità a quello già trasmesso alle rappresentanze sindacali aziendali e ai consiglieri regionali di parità ovvero, in mancanza di tale precedente trasmissione, unitamente all’attestazione della sua contestuale trasmissione alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità.

Ai sensi dell'art. 47 comma 3 del decreto-legge 31 maggio 2021, n. 77, convertito nella legge 29 luglio 2021, n. 108, in conformità al comma 6 di detto articolo, l’affidatario che occupi un numero pari o superiore ai 15 dipendenti e inferiore a 50 dipendenti è tenuto alla presentazione di una relazione di genere sulla situazione maschile e femminile entro 6 mesi dalla conclusione (stipula) del contratto e comunque entro la data di fine servizio.

La violazione dell'obbligo di produzione della relazione di genere imposto dal comma 3 dell'art. 47 D.L. 77/2021 come convertito nella L. 108/2021 determina l'impossibilità di partecipare in forma singola ovvero in raggruppamento temporaneo, per un periodo di dodici mesi, ad ulteriori procedure di affidamento afferenti agli investimenti pubblici finanziati con le risorse derivanti da PNRR e PNC.

Ai sensi dell'art. 47 comma 3 bis del decreto-legge 31 maggio 2021, n. 77, convertito nella legge 29 luglio 2021, n. 108, in conformità al comma 6 di detto articolo, l’affidatario che occupi un numero pari o superiore ai 15 dipendenti e inferiore a 50 dipendenti è tenuto alla presentazione di una relazione in merito al rispetto delle norme sul personale disabile entro 6 mesi dalla conclusione

(stipula) del contratto e comunque entro la data di fine servizio.

Ai sensi dell'art. 47 comma 4 del decreto-legge 31 maggio 2021, n. 77, convertito nella legge 29 luglio 2021, n. 108, l'affidatario deve assicurare una quota pari almeno al 30 per cento, delle assunzioni necessarie per l'esecuzione del contratto o per la realizzazione di attività ad esso connesse o strumentali, sia all'occupazione giovanile sia all'occupazione femminile.

8. Rispetto del principio di non arrecare danno significativo all'ambiente (DNSH)

Il fornitore si assume gli obblighi specifici del PNRR relativamente al non arrecare un danno significativo agli obiettivi ambientali c.d. "Do Not Significant Harm" (DNSH), ai sensi dell'articolo 17 del Regolamento (UE) 2020/852 del Parlamento europeo e del Consiglio del 18 giugno 2020 e in conformità alla Guida Operativa per il rispetto del principio di non arrecare danno significativo all'ambiente (cd. DNSH), aggiornata dalla Circolare della Ragioneria dello Stato del 14/05/2024 n. 22, ivi incluso l'impegno a consegnare all'Amministrazione la documentazione a comprova del rispetto dei suddetti requisiti.

9. Prescrizioni generali

In tutta la documentazione dovrà essere indicato che il progetto è finanziato nell'ambito del PNRR, attraverso l'esplicito riferimento al finanziamento da parte dell'Unione Europea e all'iniziativa NextGeneration EU (utilizzando la dicitura "**Finanziato dall'Unione Europea – Next Generation UE – PNRR M1C1 – Investimento 1.5**") e dovrà essere indicato il codice **CUP B37H24000910006.**

10. Soggetti ammessi, requisiti di ordine generale e altre cause di esclusione

Ai sensi della vigente normativa possono presentare offerta i soggetti di cui all'art. 65 del D.Lgs. 36/2023 operanti del settore merceologico oggetto dell'appalto e iscritti nel Mercato Elettronico della P.A. al bando: **SERVIZI - Categoria: "Servizi per l'Information Communication Technology – Sicurezza Informatica - Mepa Servizi" - CPV 72220000-3 Servizi di consulenza in sistemi informatici e assistenza tecnica (Prevalente) - CPV 72410000-7 Servizi di provider (secondario) - CPV 72224000-1 Servizi di consulenza per la gestione di progetti (secondario).**

I concorrenti devono essere in possesso, a pena di esclusione, dei requisiti di ordine generale previsti dal Codice nonché degli ulteriori requisiti indicati nel presente articolo.

La stazione appaltante verifica il possesso dei requisiti di ordine generale accedendo al fascicolo virtuale dell'operatore economico (FVOE).

Le circostanze di cui all'articolo 94 del Codice sono cause di esclusione automatica. La sussistenza delle circostanze di cui all'articolo 95 del Codice è accertata previo contraddittorio con l'operatore economico.

Sono esclusi gli operatori economici che abbiano affidato incarichi in violazione dell'articolo 53, comma 16-ter, del decreto legislativo del 2001 n. 165 a soggetti che hanno esercitato, in qualità di dipendenti, poteri autoritativi o negoziali presso l'amministrazione affidante negli ultimi tre anni.

Sono esclusi gli operatori economici che occupano oltre cinquanta dipendenti, che non consegnano, al momento della presentazione dell'offerta, copia dell'ultimo rapporto periodico

sulla situazione del personale maschile e femminile redatto ai sensi dell'articolo 46, decreto legislativo n. 198 del 2006, unitamente all'attestazione di conformità a quello già trasmesso alle rappresentanze sindacali aziendali e ai consiglieri regionali di parità ovvero, in mancanza di tale precedente trasmissione, unitamente all'attestazione della sua contestuale trasmissione alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità.

Sono esclusi gli operatori economici che occupano un numero di dipendenti pari o superiore a quindici e non superiore a cinquanta, che nei dodici mesi precedenti al termine di presentazione dell'offerta hanno omesso di produrre alla stazione appaltante di un precedente contratto d'appalto finanziato in tutto o in parte con i fondi del PNRR o del PNC o di un precedente contratto riservato ai sensi dell'articolo 61 del codice, la relazione di cui all'articolo 47, comma 3 del decreto legge n. 77 del 2021.

11. Modalità di presentazione dell'offerta

La trattativa avviene sul Me.Pa., Mercato Elettronico della Pubblica Amministrazione gestito da Consip Spa, come previsto dall'art. 1 del DL. 95/2012 convertito dalla L. 135/2012.

All'offerta dovrà essere allegata la documentazione prescritta.

Tutti gli elementi utili per la formulazione dell'offerta sono contenuti nel presente Foglio patti e condizioni e negli eventuali allegati richiesti e nelle risposte ad eventuali chiarimenti che potranno essere formulati tramite piattaforma Me.Pa.

L'offerta deve essere composta dai seguenti documenti:

*a) **Documentazione amministrativa***

La documentazione amministrativa si compone di:

- Il **presente documento** controfirmato digitalmente per accettazione
- **DGUE**
- **dichiarazione integrativa al DGUE**
- **dichiarazione sulla titolarità effettiva**
- **check-list** DNSH scheda 6 - Servizi informatici di hosting e cloud e scheda 8 – Datacenter
- (solo per operatori economici che occupano più di 50 dipendenti) **RAPPORTO SULLA SITUAZIONE DEL PERSONALE** di cui all'art. 46 del D.Lgs. 11 aprile 2006 n. 198, con attestazione della sua conformità a quello eventualmente già trasmesso alla rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di pari opportunità ovvero in caso di inosservanza dei termini previsti dall'art. 46 comma 1, con attestazione della sua contestuale trasmissione alle rappresentanze sindacali aziendali e alla consigliera e al consigliere regionale di parità, come disposto dall'art. 47 comma 2 del Decreto-Legge 31 maggio 2021, n. 77, convertito nella Legge 29 luglio 2021, n. 108.

*b) **Documentazione tecnica***

- Offerta tecnica

*c) **Offerta economica***

- Offerta economica proposta dal sistema Mepa
- Allegato A – Offerta economica con prezzi offerti in dettaglio.

12. Termine di presentazione dell'offerta

L'offerta ed i documenti di cui sopra dovranno essere presentati tramite piattaforma Me.Pa. **entro il termine previsto nella Trattativa diretta.**

13. Riserva di non aggiudicazione

La Stazione Appaltante si riserva di non procedere all'aggiudicazione se nessuna offerta risulti conveniente o idonea in relazione all'oggetto del contratto.

Tale facoltà è qui espressamente indicata ai sensi dell'art. 108 comma 10 del D.Lgs. 36/2023 e potrà essere esercitata non oltre il termine di trenta giorni dalla conclusione delle valutazioni delle offerte.

14. Direttore dell'esecuzione del contratto

L'amministrazione prima dell'esecuzione del contratto provvederà a nominare un direttore dell'esecuzione del contratto, con il compito di monitorare il regolare andamento dell'esecuzione del contratto.

Il nominativo del direttore dell'esecuzione del contratto verrà comunicato tempestivamente all'impresa aggiudicataria.

15. Avvio dell'esecuzione del contratto

L'esecutore è tenuto a seguire le istruzioni e le direttive fornite dalla stazione appaltante per l'avvio dell'esecuzione del contratto. Qualora l'esecutore non adempia, la stazione appaltante ha facoltà di procedere alla risoluzione del contratto.

16. Divieto di modifiche introdotte dall'esecutore

Nessuna variazione o modifica al contratto può essere introdotta dall'esecutore, se non è disposta dal direttore dell'esecuzione del contratto e preventivamente approvata dalla stazione appaltante.

Le modifiche non previamente autorizzate non danno titolo a pagamenti o rimborsi di sorta e, ove il direttore dell'esecuzione lo giudichi opportuno, comportano la rimessa in pristino, a carico dell'esecutore, della situazione originaria preesistente, secondo le disposizioni del direttore dell'esecuzione.

17. Varianti introdotte dalla stazione appaltante

La stazione appaltante può introdurre variazioni al contratto, oltre che nelle ipotesi previste dall'art. 120 del codice dei contratti, nei seguenti casi:

a) per esigenze derivanti da sopravvenute disposizioni legislative e regolamentari;
b) per cause impreviste e imprevedibili, accertate dal responsabile del progetto o per

l'intervenuta possibilità di utilizzare materiali, componenti e tecnologie non esistenti al momento in cui ha avuto inizio la procedura di selezione del contraente, che possono determinare, senza aumento di costo, significativi miglioramenti nella qualità delle prestazioni eseguite;

c) per la presenza di eventi inerenti alla natura e alla specificità dei beni o dei luoghi sui quali si interviene, verificatisi nel corso di esecuzione del contratto;
d) nell'esclusivo interesse della stazione appaltante, le varianti, in aumento o in diminuzione, finalizzate al miglioramento o alla migliore funzionalità delle prestazioni oggetto del contratto.

Inoltre, l'esecutore ha l'obbligo di eseguire tutte quelle variazioni di carattere non sostanziale, non comportanti maggiori oneri per l'esecutore e che siano ritenute opportune dalla stazione appaltante.

18. Variazioni entro il 20 per cento

La stazione appaltante, qualora in corso di esecuzione si renda necessario un aumento o una diminuzione delle prestazioni fino a concorrenza del quinto dell'importo del contratto, si riserva di imporre all'appaltatore l'esecuzione alle stesse condizioni previste nel contratto originario. In tal caso l'appaltatore non potrà far valere il diritto alla risoluzione del contratto.

19. Verifica di conformità

L'esecuzione dell'appalto è soggetta a verifica di conformità al fine di accertarne la regolare esecuzione, rispetto alle condizioni ed ai termini stabiliti nel contratto.

Il responsabile unico del progetto controlla l'esecuzione del contratto congiuntamente al direttore dell'esecuzione del contratto per i servizi.

Le operazioni saranno svolte in contraddittorio e sarà redatto processo verbale che sarà sottoscritto da tutte le parti intervenute.

20. Penali in caso di ritardo

Per ogni violazione degli obblighi derivanti dal presente foglio patti e condizioni e per ogni caso di carente o incompleta esecuzione della servizio sono previste le seguenti penali:

- nel caso di avvio del servizio oltre i termini previsti dal cronoprogramma di cui all'art. 6, salvo cause di forza maggiore o proroghe che possono essere concesse dall'Amministrazione per giustificati motivi, verrà applicata una penalità giornaliera pari all'1 per mille dell'ammontare netto contrattuale (Art. 50, comma 4 DL 77/2021);
- nel caso di ritardi per ogni attività, rispetto al cronoprogramma di cui all'art. 6, in capo alla ditta affidataria prevista dall'art. 5 del presente Foglio Patti e Condizioni, salvo cause di forza maggiore o proroghe che possono essere concesse dall'Amministrazione per giustificati motivi, verrà applicata una penalità giornaliera pari all'1 per mille dell'ammontare netto contrattuale (Art. 50, comma 4 DL 77/2021);
- Nel caso in cui la gestione del servizio non venga effettuata con le modalità di cui all'art. 5

del presente Foglio Patti e Condizioni, una penalità giornaliera di Euro 500,00.= per ogni difformità;

- in caso di esito negativo della verifica di conformità, una penalità giornaliera di Euro 300,00.=;
- nel caso di mancata redazione della relazione di genere sulla situazione del personale maschile e femminile, se dovuta, una penalità giornaliera nella misura dell'1 per mille dell'ammontare netto contrattuale;
- nel caso di mancata produzione della dichiarazione relativa al rispetto delle norme sulla disabilità, se dovuta, una penalità giornaliera nella misura dell'1 per mille dell'ammontare netto contrattuale;
- per non aver rispettato la quota del 30% delle assunzioni di giovani con meno di 36 anni e donne, se dovuto, una penalità giornaliera nella misura dell'1 per mille dell'ammontare netto contrattuale.

In caso di inadempimento contrattuale, l'Amministrazione sarà legittimata ad applicare le penali di cui sopra, fino alla soglia massima del 10% dell'importo netto del contratto.

L'eventuale applicazione delle penali non esime la ditta appaltatrice dalle eventuali responsabilità per danni a cose o persone dovuta a cattiva qualità dei prodotti forniti. Il responsabile del progetto o il direttore dell'esecuzione, con nota indirizzata al dirigente, propone l'applicazione delle suddette penali specificandone l'importo. L'applicazione delle penali sarà preceduta da regolare contestazione scritta dell'inadempienza, a firma del dirigente, avverso la quale la ditta avrà facoltà di presentare le sue controdeduzioni entro 3 (tre) giorni dal ricevimento della contestazione stessa.

Resta, in ogni caso, ferma la facoltà della stazione appaltante, in caso di gravi violazioni, di sospendere immediatamente il servizio alla ditta appaltatrice e di affidarlo anche provvisoriamente ad altra ditta, con costi a carico della parte inadempiente ed immediata escussione della garanzia definitiva.

Il pagamento della penale dovrà essere effettuato entro 15 (quindici) giorni dalla notifica o dalla ricezione della comunicazione di applicazione. Decorso tale termine la stazione appaltante si rivarrà trattenendo la penale sul corrispettivo della prima fattura utile ovvero sulla garanzia definitiva. In tale ultimo caso la ditta è tenuta a ripristinare il deposito cauzionale entro 10 (dieci) giorni dalla comunicazione del suo utilizzo pena la risoluzione del contratto.

21. Risoluzione del contratto

La stazione appaltante può risolvere il contratto, oltre che nei casi contemplati dall'art. 122 del d.lgs. n. 36/2023, anche nelle ipotesi di seguito elencate.

In tutti i casi di risoluzione del contratto l'appaltatore ha diritto soltanto al pagamento delle prestazioni relative ai servizi e alle forniture regolarmente eseguiti.

Nelle ipotesi successivamente elencate, ogni inadempienza agli obblighi contrattuali sarà specificamente contestata a mezzo di comunicazione scritta, inoltrata via PEC al domicilio eletto dall'aggiudicatario. Nella contestazione sarà prefissato un termine non inferiore a 5 giorni lavorativi

per la presentazione di eventuali osservazioni; decorso il suddetto termine, l'amministrazione, qualora non ritenga valide le giustificazioni addotte, ha facoltà di risolvere il contratto nei seguenti casi:

a) frode nella esecuzione dell'appalto;
b) mancato inizio dell'esecuzione dell'appalto nei termini stabiliti dal presente Foglio patti e condizioni;
c) manifesta incapacità nell'esecuzione del servizio appaltato;
d) inadempienza accertata alle norme di legge sulla prevenzione degli infortuni e la sicurezza sul lavoro;
e) interruzione totale del servizio verificatasi, senza giustificati motivi, per 5 giorni anche non consecutivi nel corso dell'anno di durata del contratto;
f) reiterate e gravi violazioni delle norme di legge e/o delle clausole contrattuali, tali da compromettere la regolarità e la continuità dell'appalto;
g) cessione del contratto, al di fuori delle ipotesi previste;
h) utilizzo del personale non adeguato alla peculiarità dell'appalto;
i) concordato preventivo, fallimento, stato di moratoria e conseguenti atti di sequestro o di pignoramento a carico dell'aggiudicatario;
j) inottemperanza agli obblighi di tracciabilità dei flussi finanziari di cui alla legge 13 agosto 2010, n. 136;
k) ogni altro inadempimento che renda impossibile la prosecuzione dell'appalto, ai sensi dell'art. 1453 del codice civile.

Il contratto si intenderà risolto, altresì, qualora la Società in house Pasubio Tecnologia S.r.l., in relazione al presente affidamento, non risulti qualificata secondo la normativa vigente, per tutta la durata contrattuale, ai sensi del Regolamento unico per le infrastrutture e i servizi cloud per la PA, adottato dall'Agenzia per la Cybersicurezza Nazionale, ACN, con Decreto Direttoriale n. 21007/24 del 27 giugno 2024.

Ove si verifichino deficienze e inadempienze tali da incidere sulla regolarità e continuità del servizio, l'amministrazione potrà provvedere d'ufficio ad assicurare direttamente, a spese dell'aggiudicatario, il regolare funzionamento del servizio. Qualora si addivenga alla risoluzione del contratto, per le motivazioni sopra riportate, l'aggiudicatario, oltre alla immediata perdita della cauzione, sarà tenuto al risarcimento di tutti i danni, diretti ed indiretti, ed alla corresponsione delle maggiori spese che l'amministrazione dovrà sostenere per il rimanente periodo contrattuale.

Costituisce causa di risoluzione del presente contratto la violazione dell'obbligo di cui all'art. 53 comma 16-ter del D.Lgs. 165/2001**.**

L'affidatario che per suo ritardo dovesse compromettere il rispetto delle tempistiche e delle scadenze indicate all'art. 8 del presente Foglio patti e condizioni, sarà chiamato a rispondere del danno subito dall'Ente in caso di parziale o mancata corresponsione del contributo PNRR.

22. Recesso

L'amministrazione si riserva la facoltà, in caso di sopravvenute esigenze d'interesse pubblico, di recedere in ogni momento dal contratto, con preavviso di almeno 20 (venti) giorni solari da

notificarsi all'aggiudicatario tramite PEC. In caso di recesso l'aggiudicatario ha diritto al pagamento da parte dell'amministrazione delle sole prestazioni eseguite, oltre al decimo delle prestazioni non eseguite, secondo quanto previsto dall'art. 123 del d.lgs. n. 36/2023 e del relativo allegato II.14.

23. Pagamenti

I pagamenti saranno effettuati entro 30 (trenta) giorni dalla data di ricevimento di regolare fattura elettronica, tramite piattaforma SDI, trasmessa al seguente codice univoco ufficio: **RJ45YI**, previa verifica della corretta esecuzione delle prestazioni.

In ogni caso, qualora le fatture pervengano anteriormente al citato accertamento, il termine di cui sopra decorrerà solo dopo il completamento del menzionato accertamento.

Il pagamento avverrà previo accertamento della regolarità previdenziale della ditta.

Il termine di pagamento potrà essere sospeso dall'amministrazione qualora difficoltà tecniche, attribuibili alla piattaforma informatica degli enti previdenziali e non attribuibili all'amministrazione medesima, impediscano l'acquisizione del DURC.

I pagamenti saranno effettuati tramite bonifico bancario o postale su un conto corrente dedicato, anche non in via esclusiva, acceso presso banche o Poste Italiane S.p.A. A questo proposito, l'appaltatore deve comunicare alla stazione appaltante entro sette giorni dall'accensione gli estremi identificativi del conto corrente di cui sopra nonché, nello stesso termine, le generalità ed il codice fiscale delle persone delegate ad operare sullo stesso.

L'appaltatore deve impegnarsi a garantire la tracciabilità dei flussi finanziari in relazione al presente appalto.

Il **codice C.I.G.** relativo al servizio di cui trattasi, i cui estremi saranno comunicati dalla stazione appaltante, dovrà essere riportato obbligatoriamente in tutte le fatture emesse dal fornitore in relazione al presente appalto.

Qualora l'appaltatore non assolva agli obblighi previsti dall'art. 3 della legge n. 136/2010 per la tracciabilità dei flussi finanziari relativi all'appalto, il contratto si risolverà di diritto ai sensi del comma 8 del medesimo art. 3.

Tutte le fatture devono riportare obbligatoriamente:

- CUP: **B37H24000910006**

- CIG: i cui estremi saranno comunicati dalla stazione appaltante

- estremi della **determina di affidamento** i cui estremi saranno comunicati dalla stazione appaltante

- il nome e codice del Progetto: **"Vicenza (cyber)sicura - rinforziamo la difesa digitale della nostra città" - ID 75_WP9_A8_Comune di Vicenza**

- la dicitura: **"Finanziato dall'Unione Europea – Next Generation UE – PNRR M1C1 - Investimento 1.5".**

24. Svincolo della garanzia definitiva

La garanzia definitiva è progressivamente svincolata in funzione dell'avanzamento dell'esecuzione del contratto, nel limite massimo dell'80 per cento dell'importo garantito.

L'ammontare residuo del 20% è svincolato a conclusione del contratto, previo accertamento degli adempimenti, sulla base del certificato di verifica di conformità.

25. Cessione del contratto e subappalto

È vietata sotto qualsiasi forma la cessione del contratto.

Il concorrente può dichiarare, nella documentazione di gara, le parti di servizio che intende eventualmente subappaltare.

Il contraente principale e il subappaltatore sono responsabili in solido nei confronti della stazione appaltante in relazione alle prestazioni oggetto del contratto di subappalto.

26. Garanzia definitiva e stipula del contratto

Prima della stipula del contratto, l'aggiudicatario è tenuto a costituire apposita garanzia definitiva, a norma dell'art. 53 del d.lgs. n. 36/2023. La garanzia può essere costituita mediante cauzione, come precisato nell'art. 106 del codice dei contratti, al quale si formula espresso rinvio, o con garanzia fideiussoria, anche in questo caso, con le modalità specificate dal citato articolo 106, purché contenga la rinuncia all'eccezione di cui all'art. 1957, comma 2 del codice civile, preveda espressamente la rinuncia al beneficio della preventiva escussione del debitore principale, preveda l'operatività entro 15 giorni, a semplice richiesta della stazione appaltante.

Non verrà accettata altra forma di costituzione della garanzia definitiva.

il contratto sarà stipulato mediante corrispondenza secondo l'uso commerciale, consistente in apposito scambio di lettere, anche tramite posta elettronica certificata o sistemi elettronici di recapito certificato qualificato ai sensi del regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014., come previsto dall'art. 23 del Regolamento Comunale per la disciplina dei Contratti, approvato con deliberazione del Consiglio Comunale n. 23 del 23 aprile 2024;

Sono a carico dell'appaltatore tutte le spese, tasse, imposte inerenti e conseguenti al contratto nonché ogni altro onere che per legge non sia inderogabilmente posto a carico del Comune.

L'imposta di bollo relativa alla stipula del contratto, determinata sulla base della tabella "A", annessa all'All. I.4 del D.Lgs. 36/2023, viene assolta ai sensi del provvedimento del direttore dell'Agenzia delle entrate n. 240013 del 28 giugno 2023 e della successiva Circolare dell'Agenzia delle entrate n. 22/E del 28 luglio 2023.

La corresponsione dell'imposta dovrà avvenire secondo le modalità che verranno rese note.

27. Nuove convenzioni Consip

In conformità a quanto disposto dall'art. 1, comma 7 del d.l. n. 95/2012, convertito in l. n. 135/2012, la stazione appaltante si riserva di recedere in qualsiasi tempo dal contratto qualora l'impresa affidataria del contratto non sia disposta ad una revisione del prezzo d'appalto, allineandolo con quanto previsto da nuove convenzioni Consip rese disponibili durante lo svolgimento del rapporto contrattuale. L'amministrazione eserciterà il diritto di recesso solo dopo aver inviato preventiva comunicazione, e fissando un preavviso non inferiore ai 15 giorni.

In caso di recesso l'amministrazione provvederà a corrispondere all'appaltatore il corrispettivo per le prestazioni già eseguite ed il 10 pe cento di quelle ancora da eseguire.

28. Estensione degli obblighi di condotta previsti dal codice di comportamento dei dipendenti pubblici

Ai sensi del combinato disposto dell'art. 2, comma 3, del D.P.R. n. 62/2013 "Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165" e dell'art. 1 del Codice di comportamento del Comune di Vicenza, adottato con deliberazione della Giunta Comunale n. 16 del 28/01/2014, l'appaltatore e, per suo tramite, i suoi dipendenti e/o collaboratori a qualsiasi titolo si impegnano, pena la risoluzione del contratto, al rispetto degli obblighi di condotta previsti dai sopracitati codici, per quanto compatibili, codici che – pur non venendo materialmente allegati al presente contratto – sono pubblicati e consultabili sul sito internet del Comune di Vicenza ai seguenti link: https://servizi2.comune.vicenza.it/utilita/documento.php/100685

29. Protocollo di legalità

L'Appaltatore si impegna a rispettare tutte le clausole pattizie di cui al Protocollo di legalità sottoscritto dalla Regione del Veneto in data 17 settembre 2019, approvato con delibera della Giunta comunale n. 170 del 6 novembre 2019, ai fini della prevenzione dei tentativi d'infiltrazione della criminalità organizzata nel settore dei contratti pubblici di lavori, servizi e forniture (consultabile al link: https://www.regione.veneto.it/web/lavori-pubblici/protocollo-di-legalita), applicabili in via transitoria, nelle more del suo rinnovo e conseguente recepimento, compatibili con la tipologia del presente contratto, consultabili sul sito del Comune di Vicenza al link: https://servizi2.comune.vicenza.it/utilita/documento.php/369058 e di accettarne incondizionatamente il contenuto e gli effetti.

30. Foro competente

Ai fini dell'esecuzione del contratto e per la notifica di eventuali atti giudiziari, la ditta aggiudicataria dovrà comunicare espressamente il proprio domicilio ovvero elegge domicilio presso la Sede Comunale. Per le controversie che dovessero insorgere tra le parti, relativamente all'interpretazione, applicazione ed esecuzione del contratto, sarà competente il foro di Vicenza.

E' esclusa, in ogni, caso la clausola arbitrale.

31. Informativa ai sensi del D.Lgs. n. 2003/196 e s.m.i. e Regolam. UE n.2016/679 (GDPR)

Il Comune di Vicenza (in seguito "Comune"), nella persona del titolare (in seguito, "Titolare"), informa ai sensi dell'art. 13 D.Lgs. 30.6.2003 n. 196 e ss.mm.ii. (in seguito, "Codice Privacy") e dell'art. 13 Regolamento UE n. 2016/679 (in seguito, "GDPR") che:

1. Titolarità del trattamento – Responsabile della Protezione dei dati - Delegato al trattamento

Il Titolare del Trattamento è il Sindaco pro tempore del Comune di Vicenza con sede in Corso A. Palladio 98, 36100 Vicenza.

2. Finalità del trattamento e durata del trattamento

I dati personali sono utilizzati dal Comune nell'ambito del procedimento di cui trattasi e saranno conservati a norma di legge.

I dati saranno trattati con l'utilizzo di procedure anche informatizzate, nei modi e nei limiti necessari per perseguire le predette finalità, anche in caso di eventuale comunicazione a terzi. Il conferimento di tali dati è necessario per la stipula del contratto.

3. Modalità del trattamento

I dati saranno trattati con strumenti cartacei e/o informatici, nel rispetto dei principi del D.Lgs. 196/2003 e s.m.i. e del Regolamento UE 2016/679 e con l'adozione di misure di sicurezza idonee a ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito o non conforme alle finalità del trattamento stesso in server ubicati all'interno dell'Unione Europea del Titolare e/o di società terze incaricate e debitamente nominate quali Responsabili del trattamento. I dati non saranno oggetto di trasferimento al di fuori dell'Unione Europea.

4. Ambito di comunicazione

I dati potranno essere comunicati a Organismi di vigilanza, Autorità giudiziarie nonché a tutti gli altri soggetti ai quali la comunicazione sia obbligatoria per legge per l'espletamento delle finalità inerenti e conseguenti al procedimento al quale si riferiscono. I dati saranno diffusi esclusivamente per quanto previsto dalla normativa in tema di trasparenza (D. Lgs. 14 marzo 2013, n. 33 "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni", e ss.mm.ii).

5. Modalità di esercizio dei diritti dell'interessato

All'interessato è riconosciuto il diritto di accesso ai propri dati personali, di chiederne la rettifica, l'aggiornamento e la cancellazione, se incompleti, erronei o raccolti in violazione della legge, nonché di opporsi al loro trattamento per motivi legittimi rivolgendo le richieste al Servizio Informatico Comunale del Comune di Vicenza (Corso Palladio, 98 - 36100 Vicenza).

6. Dati di contatto del Responsabile della Protezione dei Dati

dpo@comune.vicenza.it

32. Designazione a responsabile trattamento dati personali (art. 28 Reg. UE 2016/67)

La stazione appaltante, titolare del trattamento dei dati personali, si avvarrà dell'appaltatore in qualità di responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679, in relazione ai dati personali che saranno da esso trattati per l'espletamento del servizio.

L'appaltatore è tenuto a conoscere e rispettare tutti gli obblighi previsti dalla vigente normativa a carico del responsabile del trattamento, impegnandosi a vigilare sull'operato dei soggetti da esso autorizzati al trattamento e di eventuali propri sub-responsabili del trattamento.

E' fatto divieto all'appaltatore ed al personale da esso impiegato di utilizzare le informazioni

assunte nell'espletamento della attività per fini diversi da quelli inerenti l'attività stessa. Il trattamento dei dati personali dovrà avvenire nel rispetto delle norme vigenti ed in particolare del Regolamento UE 2016/679 e del D.Lgs. 196/2003.
Il trattamento dei dati da parte dell'appaltatore in qualità di responsabile del trattamento rappresenta condizione imprescindibile per l'espletamento del contratto. In caso di mancata accettazione la stazione appaltante, constata l'impossibilità di affidare il servizio all'operatore selezionato, procederà ad affidare l'appalto al soggetto nella successiva posizione nella graduatoria di aggiudicazione.

IL DIRETTORE
Settore Informatico Comunale
dr. Lorenzo Beggiato
(firmato digitalmente ai sensi del d.lgs.7 marzo 2005, n. 82 e s.m.i.)