Capitolato speciale d’appalto per la realizzazione di un Security Assessment del Comune di Trieste e la redazione di un Piano di Sicurezza Informatica

Indice generale

Art.1 PREMESSA

La sicurezza informatica è un tema che si fa sempre più pressante all’interno della Pubblica Amministrazione, dove, grazie anche al grande impulso alla digitalizzazione offerto dalle misure del PNNR, la quantità di dati e informazioni raccolte sta crescendo e richiede un livello di protezione sempre più elevato,

Anche il Piano Triennale dell’Informatica della Pubblica Amministrazione 2024-2026, redatto da Agid, dedica un intero capitolo a questo argomento dove viene evidenziato come la minaccia cibernetica cresce in quantità e qualità, crescita determinata anche dall’evoluzione delle tecniche di ingegneria sociale volte a ingannare gli utenti finali dei servizi digitali sia interni alla PA che esterni.

L’esigenza di contrastare tali minacce diventa fondamentale in quanto garanzia non solo della disponibilità, l’integrità e riservatezza delle informazioni proprie del Sistema informativo della Pubblica Amministrazione, ma presupposto per la

protezione del dato che ha come conseguenza diretta l'aumento della fiducia nei servizi digitali erogati dalla PA.

Tutto ciò premesso risulta quindi fondamentale adottare una serie di misure che consentano di proteggere il patrimonio informativo siano, questi interventi tecnologici oppure l'adozione di opportune regole comportamentali, da imporsi a tutti coloro che utilizzino l'infrastruttura.

Per minimizzare il verificarsi di attacchi informatici e soprattutto per cercare di contenerne i danni, e di conseguenza i disservizi, è ormai noto che occorra prima di tutto conoscere il profilo di rischio della propria infrastruttura e mettere in campo le azioni più idonee, se del caso anche differenziate, a proteggere adeguatamente le parti più esposte.

Art.2 OGGETTO DEL CONTRATTO

Il presente Capitolato ha lo scopo di realizzare un Security Assessment per identificare e mettere in luce le vulnerabilità presenti nel sistema informatico del Comune di Trieste, effettuare una valutazione del rischio e realizzare la stesura di un Piano di Sicurezza in grado di eliminare o mitigare i rischi individuati con l'obiettivo non solo di rispondere a minacce conosciute, ma anche di anticipare e prevenire potenziali rischi futuri.

La documentazione prodotta potrà far parte della documentazione di gara per la successiva fase di implementazione delle misure di mitigazione del rischio e di miglioramento delle difese informatiche aziendali.

Art.3 VALORE E DURATA DEL CONTRATTO

La base d'asta è pari a euro 50.000,00 (cinquantamila) oltre IVA dovuta nelle misure di legge per un totale complessivo di Euro 61,000,00 (sessantunomila) IVA inclusa.

Il contratto avrà una durata di 120 giorni naturali e consecutivi a decorrere dalla stipula dello stesso.

Art.4 RISCHI DA INTERFERENZA

Gli accertamenti effettuati in materia di interferenze nello svolgimento delle attività riguardanti l'appalto non hanno evidenziato rischi da interferenza ai sensi dell'art. 26, comma 3-bis del D.lgs 81/2008 e conseguentemente non è stato prodotto il DUVRI.

Art.5 PROCEDURA

Per l'affidamento del presente appalto si procederà mediante affidamento diretto ai sensi dell'art. 50 comma1, lettera b) D. Lgs. 36/2023. A tal fine si precisa che, secondo

quanto previsto dall’art. 3, comma 1 dell’allegato I.1 del codice dei contratti per “Affidamento diretto” si intende l’affidamento del contratto senza una procedura di gara, nel quale, anche nel caso di previo interpello di più operatori economici, la scelta è operata **discrezionalmente** dalla stazione appaltante, nel rispetto dei criteri qualitativi e quantitativi di cui all’articolo 50 comma 1 lettere a) e b) del codice e dei requisiti generali o speciali previsti dal medesimo codice.

Per la scelta del contraente verrà richiesto un elaborato tecnico progettuale ed un preventivo di spesa che saranno oggetto di valutazione da parte della stazione appaltante che terrà conto della documentazione e delle soluzioni proposte secondo quanto meglio precisato all'art. 8.

Individuato il contraente secondo quanto indicato nel precedente capoverso del presente articolo, il contratto verrà stipulato mediante lo strumento della Trattativa Diretta sulla piattaforma certificata del MEPA.

Art.6 MODALITÀ DI SVOLGIMENTO DELLE PRESTAZIONI

L’obiettivo del Comune di Trieste è quello di creare un ambiente digitale più sicuro e resiliente rispetto alla situazione attuale, in grado di resistere a potenziali attacchi esterni e di proteggere le informazioni detenute dell’Ente.

Le prestazioni analizzeranno 5 aspetti specifici della sicurezza informatica dell’Ente e non si richiede che vengano svolte in modo sequenziale.

L’appaltatore sarà tenuto ad eseguire le prestazioni contrattuali, da svolgersi sia in presenza, presso il Comune di Trieste, che da remoto partecipando o organizzando tavoli di coordinamento periodici in base allo stato di avanzamento dei lavori.

L’appaltatore si obbliga a collaborare e condividere le informazioni tra i diversi attori coinvolti (sia interni che esterni all’Ente).

1: Analisi degli hash delle password

L’appaltatore eseguirà un’analisi offline degli hash delle password degli utenti comunali (l’elenco degli hash, la cui funzione verrà concordata con l’aggiudicatario, verrà fornito in sede di affidamento) per valutarne il livello di robustezza.

Questo processo serve a rilevare ed evidenziare eventuali criticità legate alle scelte degli utenti comunali e a proteggersi da attacchi di tipo “credential stuffing”.

Output richiesto (numero massimo di 50 pagine A4):

1. elenco degli hash associati a password identificate come deboli e facilmente individuabili (senza indicare esplicitamente l’hash, ma riferendosi al

progressivo identificativo dell'hash);
2. analisi statistiche comprensive di valutazioni fatte in raffronto ad elenchi pubblici di password compromesse
3. documento che descriva le raccomandazioni e suggerimenti per migliorare la sicurezza delle password per renderle più forti, nella forma di un insieme di linee guida da veicolare agli utenti;
4. piano di azione su come coinvolgere gli utenti per stimolarli all'utilizzo di password con criteri di sicurezza migliori

2: Campagna di phishing

In questa attività l'appaltatore dovrà organizzare una sessione formativa ed informativa, sui rischi del phishing, ad un gruppo di 50 dipendenti del Comune.

Seguirà poi una campagna di phishing indirizzata ad un gruppo di dipendenti più ampio del precedente, circa 100, con l'obiettivo di valutare la capacità degli utenti di riconoscere e rispondere adeguatamente alle minacce di questo tipo, evidenziare eventuali comportamenti anomali, insicuri o pericolosi e valutare l'efficacia del processo formativo.

Output richiesto (numero massimo di 30 pagine A4): un report dettagliato che include:

1. i risultati della campagna di phishing come ad esempio: il numero di accessi a link di phishing,il numero informazioni sensibili fornite;
2. un'analisi del comportamento degli utenti durante la campagna di phishing, evidenziando eventuali comportamenti anomali o critici;
3. una valutazione dell'efficacia della formazione, quanto e se la formazione ha aiutato a migliorare la consapevolezza dei dipendenti sui rischi del phishing;
4. dei suggerimenti su come migliorare le future campagne di phishing e la formazione sulla sicurezza;
5. un piano di azione su come affrontare le debolezze identificate durante la campagna di phishing e migliorare la consapevolezza della sicurezza tra i dipendenti, nella forma di un insieme di linee guida da veicolare agli utenti.

3: Analisi delle vulnerabilità

Questa attività ha l'obiettivo di individuare le vulnerabilità del sistema, che possono derivare ad esempio da configurazioni di sicurezza inadeguate, lacune nei livelli di protezione attualmente in uso, software obsoleti o dispositivi non appartenenti al sistema che potrebbero essere sfruttati da potenziali attaccanti esterni.

L'analisi delle vulnerabilità consiste nell'effettuare una valutazione delle:

- vulnerabilità interne effettuando una disamina dei dispositivi connessi alla rete interna del comune ad esempio: postazioni di lavoro, stampanti e server e fare una valutazione dei livelli di protezione (anche in relazione alle politiche di backup attualmente implementate) e dello stato di aggiornamento dei software.
- vulnerabilità esterne, riguardano servizi e applicazioni web visibili dall'esterno. L'appaltatore dovrà analizzare gli IP pubblici dell'Ente (89.96.138.0/26), l'infrastruttura deputata all'effettuazione dei Consigli Comunali (struttura a sè stante esposta su internet) e cinque siti web individuati dal Comune e non ospitati sugli IP pubblici sopraindicati (l'elenco degli IP e l'url dei siti web verrà fornito in sede di esecuzione) per identificarne le vulnerabilità e i relativi rischi per la sicurezza.

L'analisi dovrà essere effettuata utilizzando strumenti aggiornati e tener conto delle informazioni relative alle vulnerabilità e minacce più recenti.

Output richiesto (numero massimo di 50 pagine A4):

Report di Assessment: questo documento dovrà fornire una panoramica dettagliata, completa e comprensibile dei risultati dell'assessment. Dovrà include una descrizione del contesto, la metodologia utilizzata per l'assessment, i risultati delle misurazioni, una classificazione in base al livello di rischio per il Comune e delle opportune valutazioni per la risoluzione o mitigazione delle vulnerabilità. La relazione non dovrà superare il numero di 50 pagine A4.

4: Esecuzione di un penetration test

Il Penetration Test sarà eseguito sull'infrastruttura deputata all'effettuazione dei Consigli Comunali e sui 5 siti web di cui al punto 3 più le eventuali vulnerabilità rilevate nella scansione dei nostri IP pubblici.

Prima dell'esecuzione del Penetration Test, si dovrà fornire all'Ente un piano delle attività che dettagli l'ambito, il target di riferimento, le tempistiche e le metodologie utilizzate: se tali attività possono causare interruzioni o danni, il Servizio Trasformazione Digitale Comunale deciderà se autorizzare o meno la prosecuzione, pianificando eventualmente un'interruzione o un disservizio programmato.

Output richiesto (numero massimo di 30 pagine A4):
un report dettagliato dei risultati con indicati i dettagli delle vulnerabilità riscontrati, una classificazione in base al livello di rischio, le possibili implementazioni e raccomandazioni su come risolvere o mitigare le vulnerabilità identificate.

5: Redazione di un Piano di Sicurezza Informatica

I risultati e le informazioni ottenute dall'implementazione delle fasi precedenti dovranno essere rielaborati nella forma di un Piano di Sicurezza Informatica (numero massimo di 50 pagine A4).

Eventualmente arricchito da quanto offerto come proposte migliorative nel documento di risposta all'offerta tecnica.

Art.7 CRONOPROGRAMMA

L'impresa appaltatrice dovrà presentare, in sede di confronto di preventivi, un cronoprogramma contenente le tempistiche di esecuzione dell'appalto i cui dettagli potranno essere concordati con la stazione appaltante in caso di affidamento.

Art.8 PROCEDURA E CRITERI DI VALUTAZIONE

Il contratto verrà stipulato mediante l'utilizzo dello strumento della Trattativa diretta del MePA.

Nella valutazione delle proposte ricevute saranno considerati premianti i criteri di seguito indicati che costituiranno il fondamento delle ragioni della scelta del contraente ai sensi dell'art. 17, comma 2 del D.Lgs. 36/2023:

a. Le tempistiche indicate nel cronoprogramma per lo svolgimento delle attività programmate. Verrà valutato il minor tempo di realizzazione delle prestazioni oggetto dell'appalto rispetto ai 120 giorni massimo indicati nel presente capitolato;

b. curriculum del personale che troverà impiego nell'esecuzione dell'appalto;

c. le certificazioni inerenti alle tematiche di sicurezza possedute dall'impresa e/o dal personale impiegato;

d. l'eventuale possesso da parte dell'offerente della "Cybersecurity Made in Europe Label";

e. le documentate esperienze pregresse idonee all'esecuzione dell'appalto in termini di complessità, di soggetti verso i quali sono state eseguite le prestazioni, in termini economici e temporali, eseguiti nei confronti di soggetti pubblici o privati. La valutazione verrà effettuata sulla base di una relazione di max 4 pagine A4 presentata dall'offerente;

f. la proposta progettuale di come effettuare un'analisi offline degli hash delle password degli utenti comunali, in particolare sulla scelta della funzione di hashing, sulla modalità pratica di effettuazione dell'analisi offline e sull'eventuale messa a disposizione degli strumenti software necessari (e delle

istruzioni) per effettuare autonomamente lo stesso tipo di analisi in un successivo momento, in totale autonomia (punto 1). La valutazione verrà effettuata sulla base di una relazione di max 4 pagine A4 presentata dall'offerente;

g. la proposta progettuale di come organizzare ed effettuare la formazione e la campagna di phishing (punto 2), in termini di minor impatto nei confronti degli utenti e del personale sistemistico dell'Ente. La valutazione verrà effettuata sulla base di una relazione di max 4 pagine A4 presentata dall'offerente;

h. la proposta progettuale di come condurre le analisi delle vulnerabilità (punto 3), in termini di minor impatto nei confronti degli utenti e del personale sistemistico dell'Ente ed utilizzo di soluzioni tecniche innovative. La valutazione verrà effettuata sulla base di una relazione di max 4 pagine A4 presentata dall'offerente;

i. la proposta progettuale di come effettuare il penetration test (punto 4), in termini di minor impatto nei confronti degli utenti e del personale sistemistico dell'Ente ed utilizzo di soluzioni tecniche innovative. La valutazione verrà effettuata sulla base di una relazione di max 4 pagine A4 presentata dall'offerente;

j. i contenuti del Piano di Sicurezza Informatica valutando positivamente un ampliamento ed approfondimento degli esiti relativi agli aspetti della sicurezza informatica oggetto di analisi e che includa una sezione aggiuntiva relativa ad un "Piano di Risposta agli Incidenti informatici". La valutazione verrà effettuata sulla base di una relazione di max 4 pagine A4 presentata dall'offerente;

k. eventuale modalità, tipologia e durata di eventuale supporto tecnico offerto per coprire un periodo successivo alla scadenza naturale del contratto.

La stazione appaltante si riserva di convocare un incontro di approfondimento con i partecipanti alla procedura per chiarire alcuni aspetti inerenti all'offerta presentata.

Art.9 RESPONSABILE DEL PROCEDIMENTO E DEL PROGETTO

Responsabile unico del procedimento (RUP ai sensi della legge n. 241/90) nonché il Responsabile di Progetto e responsabile per le fasi di programmazione, progettazione, affidamento ed esecuzione (ai sensi dell'art. 15, D.Lgs. 36/2023) è il Direttore del Servizio Trasformazione Digitale, dott.ssa Giannina Ceschin che svolge tutti i compiti relativi all'affidamento e all'esecuzione del presente appalto che non siano specificatamente attribuiti ad altri soggetti.

Art.10 DIRETTORE DELL'ESECUZIONE DEL CONTRATTO

L’amministrazione prima dell’esecuzione del contratto provvederà a nominare un Direttore dell’esecuzione, 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.

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

Art.11 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.

Art.12 MODIFICHE DEI CONTRATTI IN CORSO DI ESECUZIONE

Sono ammesse, ai sensi dell’art. 120 del d.lgs. n. 36/2023, le modifiche del contratto rese necessarie al perseguimento degli obiettivi dell’intervento.

Qualora in corso di esecuzione si renda necessario un aumento o una diminuzione delle prestazioni fino a concorrenza del quinto dell'importo del contratto, la stazione appaltante potrà imporre all'appaltatore l'esecuzione alle condizioni originariamente previste. In tal caso l'appaltatore non può fare valere il diritto alla risoluzione del contratto.

Qualora disponibili potranno essere utilizzate anche le economie di spesa derivanti dai ribassi verificatisi in sede di offerta.

Art.13 PENALI

Per ogni violazione degli obblighi derivanti dal presente capitolato nonché per ogni caso di carente, tardiva o incompleta esecuzione del servizio, la stazione appaltante, fatto salvo ogni risarcimento di maggiori ed ulteriori danni, potrà applicare alla ditta appaltatrice penali per il ritardo nell’esecuzione delle prestazioni contrattuali da parte dell’appaltatore commisurate ai giorni di ritardo e proporzionali rispetto all’importo del contratto o alle prestazioni del contratto rispetto al cronoprogramma pattuito.

Le penali dovute per il ritardato adempimento e in ogni caso di carente, tardiva o incompleta esecuzione del servizio sono calcolate in misura giornaliera compresa tra

lo 0,3 per mille e l’1 per mille dell’ammontare netto contrattuale da determinare in relazione all‘ entità delle conseguenze legate al ritardo, e non possono comunque superare, complessivamente, il 10 per cento di detto ammontare netto contrattuale.

Laddove l'importo delle penali erogate superasse il 10% dell'ammontare contrattuale, la Stazione appaltante potrà procedere alla risoluzione del contratto e all'escussione della garanzia fidejussoria, fatta salva ogni azione per il risarcimento di ulteriori danni.

L’eventuale applicazione delle penali non esime la ditta appaltatrice dalle eventuali responsabilità per danni a cose o persone dovuta a cattiva qualità dei servizi 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 affidarla 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.

Art.14 GARANZIA E BOLLO

L'impresa aggiudicataria è tenuta alla costituzione di una garanzia definitiva per l’esecuzione del contratto pari al 5 per cento dell’importo contrattuale ai sensi dell’art. 53, comma 4, del D.Lgs. 36/2023.

L’operatore economico aggiudicatario è altresì tenuto alla trasmissione di una dichiarazione sostitutiva di notorietà ex DPR 445/2000 dell'avvenuto assolvimento dell'imposta di Bollo secondo quanto previsto dall’art. 18, comma 10 e dall’Allegato I.4 del D.Lgs. 36/2023“Codice dei contratti pubblici.

Art.15 FATTURAZIONE

L’appaltatore potrà emettere fattura, previa autorizzazione del comune di Trieste al raggiungimento del 50% del valore delle prestazioni. Il pagamento avverrà entro 30 giorni dalla data di ricezione della fattura, previo accertamento della prestazione da parte del direttore dell'esecuzione del contratto.

Sull'importo netto progressivo delle prestazioni sarà effettuata una ritenuta dello 0,50%, che potrà essere svincolata soltanto in sede di liquidazione finale, ai sensi dell'art 6, comma 11 del d.lgs. 36/2023.

Con specifico riferimento alle fatture che dovranno essere presentate per la liquidazione delle spese, verranno date precise istruzioni per la compilazione.

Secondo quanto previsto dal Decreto Ministeriale n. 55 del 3 aprile 2013 [1], **il Comune di Trieste** dal 31 marzo 2015[2] **non può più accettare fatture che non siano trasmesse in formato elettronico**, secondo le specifiche tecniche indicate nell'allegato A "Formato della fattura elettronica" del citato D.M. 55/2013.

Per le finalità di cui sopra, l'Amministrazione ha ottenuto dall'Indice delle Pubbliche Amministrazioni (IPA) il Codice Univoco Ufficio, un'informazione obbligatoria della fattura elettronica che consente al Sistema di Interscambio (SdI) dell'Agenzia delle Entrate di recapitare correttamente il documento all'Ente.[3]

Il **"Codice Univoco Ufficio"** al quale dovranno essere indirizzate le fatture elettroniche intestate al **Comune di Trieste** e che dovrà essere inserito obbligatoriamente nell'elemento del tracciato della fattura elettronica denominato <Codice Destinatario>, è il seguente:

B87H10

Nel corpo della fattura elettronica vanno, altresì, indicati:

- il Codice Identificativo Gara[4] (**CIG**), da inserire nell'elemento del tracciato fattura elettronica <CodiceCIG>
- tutti gli elementi riconducibili al contratto e/o all'ordine di acquisto, compresi i dati del provvedimento di impegno di spesa
- una puntuale e comprensibile descrizione del bene o servizio
- se si tratta di nota di accredito, la fattura che con essa viene stornata in tutto o in parte
- la corretta natura dell'operazione in caso di non applicazione dell'IVA (esente, non soggetta, non imponibile, esclusa ...)

[1]Il DM 55/2013 entrato in vigore il 6 giugno 2013 ha disciplinato l'obbligo di utilizzo della fatturazione elettronica nei rapporti economici con la Pubblica Amministrazione, in attuazione delle disposizioni della Legge n. 244/2007, art. 1, commi da 209 a 214

[2]La decorrenza dell'obbligo è stata anticipata ai sensi dell'art. 25 comma 1 del D.L. n. 66/2014 convertito in legge n. 89/2014

[3]A titolo informativo e a completamento del quadro regolamentare, si segnala che l'allegato B "Regole Tecniche" al citato DM 55/2013 contiene le modalità di emissione e trasmissione della fattura elettronica alla Pubblica Amministrazione per mezzo dello SdI, mentre l'allegato C "Linee Guida" del medesimo decreto riguarda le operazioni per la gestione dell'intero processo di fatturazione.
Si invita a consultare, per quanto di proprio interesse, il sito www.fatturapa.gov.it nel quale sono disponibili ulteriori informazioni in merito alle modalità di predisposizione e trasmissione della fattura elettronica oltre al sito www.indicepa.gov.it in merito all'identificazione degli uffici destinatari della fattura elettronica.

[4]Tranne i casi di esclusione dall'obbligo di tracciabilità di cui alla Legge n. 136 del 13/8/2010

Si comunica inoltre che il Comune di Trieste è soggetto, ai sensi dell'art. 17 ter comma 1 DPR 633/1972 al meccanismo della **scissione dei pagamenti** che comporta l'obbligo per il Comune di **pagare al fornitore SOLO il valore imponibile fatturato**, mentre l'IVA regolarmente esposta in fattura va versata all'Erario. Conseguentemente nel campo <EsigibilitaIVA> del tracciato xml della fattura elettronica andrà inserita la lettera “S” che individua il meccanismo della scissione; qualora ricorrano i presupposti di legge per il non assoggettamento al meccanismo citato, resta a carico del fornitore indicare nel campo apposito i relativi **riferimenti normativi** (quali, a mero titolo di esempio, i regimi speciali c.d. monofase dell'art 74 DPR 633/72, o del margine di cui all'art. 36 DL 41/1995, o di cui alla Legge 398/91 per le associazioni culturali).

Merita ricordare che, nel caso di compilazione di campi non obbligatori, questi devono essere corretti; in particolare, l'importo da inserire nel campo <ImportoTotale> nei Dati Generali del Documento deve corrispondere alla sommatoria di imponibile, imposta ed eventuali somme fuori campo IVA, mentre nel caso di applicazione del meccanismo della scissione dei pagamenti l'importo da indicare nel campo <Importo> nei Dati del Pagamento non deve includere la relativa imposta.

Per agevolare la distribuzione delle numerose fatture elettroniche tra le Aree, Servizi ed Uffici in cui è suddiviso il Comune di Trieste, si richiede infine la Vostra collaborazione invitandoVi a compilare anche il campo del tracciato della fattura elettronica <Causale> presente nei DatiGeneraliDocumento anteponendo alla descrizione della causale vera e propria e separato da questa con il carattere speciale Pipe: | il seguente codice SISIN

Tale indicazione, - pur non obbligatoria – è vivamente consigliata poiché serve ad identificare l'unità operativa del Comune di Trieste che segue il rapporto giuridico instaurato con il singolo fornitore, oltre ad impegnare ed ordinare la spesa e a curarne il relativo pagamento, risultando quindi di fondamentale importanza per lo svolgimento dell'iter di liquidazione della fattura elettronica.

Art.16 PRIVACY

Ai sensi dell’art. 13 del D. Lgs. 196/2003 (di seguito “Codice Privacy”), e successive modifiche e integrazioni, e degli art. 13 e 14 del Regolamento UE n. 2016/679 (GDPR 2016/679), recante disposizioni a tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, si informa che i dati personali forniti dagli Operatori economici ai fini della partecipazione alla presente procedura saranno raccolti e trattati nell’ambito del medesimo procedimento e dell’eventuale, successiva stipula e gestione del contratto secondo le modalità e finalità di cui alla normativa sopra indicata.

I diritti spettanti all’interessato sono quelli di cui al succitato agli artt. 15 e seguenti del GDPR n. 679/2016 al quale si fa espresso rinvio per tutto quanto non previsto dal presente paragrafo.

L'Impresa è tenuta al segreto d'ufficio ed è vietata la divulgazione a terzi di ogni dato relativo al presente contratto, ivi inclusi i risultati finali, fatto salvo un eventuale specifica autorizzazione, data dal Comune di Trieste, alla divulgazione.

Al termine dell'esecuzione del contratto, l'Impresa si impegna a distruggere tutti i dati raccolti per le necessità di elaborazione e produzione di quanto richiesto nelle varie fasi.

Art.17 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. Per le controversie che dovessero insorgere tra le parti, relativamente all'interpretazione, applicazione ed esecuzione del contratto, sarà competente il foro di Trieste.

Art.18 NORME DI RIFERIMENTO

Per quanto non espressamente previsto nel presente documento si rinvia alle disposizioni previste dalla Legge, dal codice dei contratti pubblici di cui al d.lgs. 36/2023 e s.m.i., e, ove espressamente non derogato, alle regole del sistema di e-Procurement della P.A.