

## COMUNE DI TRIESTE

Dipartimento Innovazione e Servizi al Cittadino

Servizio Trasformazione Digitale

# CAPITOLATO TECNICO

## Servizio SOC e SIEM

# Sommario

1 Introduzione ..... 4
1.1 Premessa ..... 4
1.2 Obiettivi dell'affidamento ..... 4
2 Norme di carattere generale ..... 4
2.1 Oggetto e perimetro ..... 4
2.2 Durata e corrispettivo ..... 5
2.3 Modalità generali di erogazione ..... 5
2.4 Disponibilità dei dati e documentazione ..... 5
2.5 Riferimenti normativi e sicurezza ..... 5
3 Fasi dell'affidamento e attivazione dei servizi ..... 6
3.1 Cronoprogramma ..... 6
3.2 Fase 1 – Setup ..... 7
3.3 Fase 2 – Esercizio a regime ..... 8
3.4 Fase 3 – Uscita e trasferimento ..... 8
4 Servizi inclusi nel corrispettivo ..... 9
4.1 Servizio SOC ..... 9
4.1.1 Operatività del SOC ..... 9
4.1.2 Monitoraggio, triage e gestione incidenti ..... 9
4.1.3 Escalation e notifiche ..... 10
4.2 Servizio SIEM ..... 10
4.2.1 Piattaforma e raccolta ..... 10
4.3 Dashboard ..... 11
4.4 Reportistica e formazione ..... 11
4.5 Requisiti tecnici minimi ..... 12

5 Modalità di erogazione del servizio ..... 13
5.1 Requisiti operativi e governance ..... 13
5.2 Orari, strumenti e canali ..... 13
6 Personale e requisiti professionali ..... 13
6.1 Composizione e competenze ..... 13
6.2 Formazione e riservatezza ..... 14
7 Livelli di servizio (SLA) ..... 14
7.1 Regole di misurazione ..... 14
7.2 Livelli di servizio minimi ..... 14
8 Modalità di partecipazione, requisiti e criteri di affidamento ..... 16
8.1 Elementi di valutazione del preventivo economico e del piano operativo ..... 17
9 Disposizioni ..... 18
9.1 Verifiche di conformità ..... 18
9.2 Corrispettivo e inadempimenti ..... 18
9.3 Modifiche contrattuali ..... 19
10 Sicurezza informatica ..... 19
11 Uso dell'intelligenza artificiale ..... 22
12 Fatturazione ..... 24
13 Penali ..... 25
13.1 Disposizioni generali ..... 25
13.2 Ritardo nel completamento della fase di setup ..... 25
13.3 Ritardo nel rispetto degli SLA e degli altri termini contrattuali ..... 25
13.4 Mancato rispetto degli indicatori percentuali ..... 26
13.5 Cumulo e limiti ..... 27
13.6 Contestazione e applicazione ..... 27
13.7 Recupero delle somme e ulteriori rimedi ..... 27
14 Protezione dei dati personali e nomina a responsabile del trattamento ..... 28

# 1 Introduzione

## 1.1 Premessa

Il presente capitolato definisce i requisiti per l'affidamento del servizio di Security Operations Center (SOC) e di Security Information and Event Management (SIEM), finalizzato a migliorare la postura di sicurezza informatica del Comune di Trieste, identificato quale "soggetto importante" nell'ambito del D.Lgs. 138/2024 (recepimento Direttiva NIS2).

## 1.2 Obiettivi dell'affidamento

Il servizio garantisce raccolta, analisi e correlazione dei log, presidio umano continuativo, generazione ed analisi degli alert, comunicazione tempestiva ai referenti indicati dal Comune, supporto tecnico alla risposta agli incidenti.

# 2 Norme di carattere generale

## 2.1 Oggetto e perimetro

Il servizio, a corrispettivo complessivo a corpo e omnicomprensivo, comprende avvio e configurazione del SIEM, integrazione e mantenimento delle fonti, conduzione della piattaforma SIEM e del SOC H24/7, threat intelligence mediante aggiornamento degli IOC, incident response, reportistica, accesso alle dashboard, formazione iniziale e trasferimento finale di dati e configurazioni. Sono comprese nel corrispettivo tutte le attività ordinarie di configurazione, manutenzione, troubleshooting, tuning e adeguamento di connettori, parser, regole e dashboard necessarie a mantenere efficace il servizio sul perimetro preso in carico. Il perimetro tecnico e l'elenco iniziale delle fonti sono concordati in avvio sulla base della documentazione resa disponibile dal Comune; sostituzioni, aggiornamenti ed evoluzioni ordinarie delle fonti già comprese nel perimetro restano incluse, purché non comportino il superamento delle capacità o delle licenze. La capacità minima richiesta è precisata al paragrafo 4.5 Requisiti tecnici minimi.

## 2.2 Durata e corrispettivo

La durata complessiva del contratto è di 13 mesi dalla data di stipula: i primi 12 mesi comprendono il setup, da completare entro 60 giorni solari dalla stipula, e l'esercizio dei servizi SOC e SIEM; l'ultimo mese è destinato al completamento delle attività di uscita e trasferimento. Tutte le attività, comprese quelle dell'ultimo mese, sono incluse nel corrispettivo complessivo.

L'importo massimo previsto per l'affidamento è pari a euro 139.000,00, IVA esclusa; il prezzo si intende omnicomprensivo per tutte le attività necessarie all'erogazione e al mantenimento dell'efficacia dei servizi sul perimetro contrattuale e non sono previsti servizi a consumo o opzioni di servizio.

## 2.3 Modalità generali di erogazione

L' appaltatore assicura continuità del presidio, tracciabilità delle attività e un referente unico per il coordinamento con la stazione appaltante. Le comunicazioni con il Comune, i ticket e i report sono in lingua italiana. Il centro operativo SOC è ubicato nell'Unione europea. Gli interventi sui sistemi comunali sono eseguiti con accessi nominali, limitati alle funzioni necessarie per l'esecuzione delle attività.

## 2.4 Disponibilità dei dati e documentazione

Log, eventi, ticket, analisi, report, configurazioni e regole sviluppati nell'esecuzione del contratto restano nella disponibilità del Comune. L'appaltatore ne consente l'esportazione, senza costi aggiuntivi, in formati elettronici aperti o di uso comune. Qualora specifiche configurazioni o regole non siano tecnicamente esportabili in forma direttamente riutilizzabile, l'appaltatore consegna comunque la relativa logica, i parametri, le dipendenze e la documentazione necessaria a consentirne la ricostruzione o migrazione verso altra piattaforma. La documentazione tecnica del Comune è usata esclusivamente per il servizio e trattata come riservata e non divulgabile.

## 2.5 Riferimenti normativi e sicurezza

Durante tutta la durata del Contratto, l'appaltatore è tenuto a garantire che l'erogazione dei servizi sia conforme e costantemente allineata alla normativa vigente applicabile, nonché alle linee guida, raccomandazioni e disposizioni emanate

dalle autorità competenti, incluse l'Agenzia per la Cybersicurezza Nazionale (ACN) e l'European Union Agency for Cybersecurity (ENISA).

A titolo esemplificativo e non esaustivo, l'Aggiudicatario dovrà conformarsi almeno:

- D. Lgs. 4 settembre 2024, n. 138
- Legge 28 giugno 2024, n. 90
- Al Regolamento (UE) 2016/679 (GDPR) e alla normativa nazionale in materia di protezione dei dati personali
- Al Regolamento UE 2024/1689 (c.d. "AI Act") e agli eventuali ulteriori riferimenti regolatori applicabili all'utilizzo di sistemi di intelligenza artificiale
- Alle linee guida, raccomandazioni e determinazioni emanate da ACN, ENISA e dalle ulteriori Autorità competenti, ove pertinenti al perimetro del servizio.

# 3 Fasi dell'affidamento e attivazione dei servizi

## 3.1 Cronoprogramma

| Fase | Termine | Risultato verificabile |
|---|---|---|
| 1 – Setup | Dalla stipula, entro 60 giorni solari | Piano di avvio; censimento delle fonti e delle informazioni disponibili; integrazione iniziale; piattaforme SIEM e SOC H24/7 operative; procedure di escalation stabilite; formazione iniziale.<br>Completamento delle integrazioni concordate, tuning delle regole, verifica della qualità dei log, report iniziale e consolidamento delle procedure. |
| 2 – Esercizio a regime | Dalla conclusione positiva del setup fino alla scadenza del dodicesimo mese dalla stipula. | Servizi continuativi H24/7, reportistica e riesame trimestrale del perimetro. |
| 3 – Uscita | Avvio del passaggio di consegne | Consegna dei dati e delle configurazioni esportabili, documentazione aggiornata, |

| | | |
|---|---|---|
| | nell'ultimo mese di esercizio e completamento entro la scadenza del tredicesimo mese dalla stipula. | assistenza alla conclusione del passaggio di consegne verso nuovo subentrante. |

## 3.2 Fase 1 – Setup

L'appaltatore prende in carico la documentazione disponibile e verifica, per quanto ragionevolmente rilevabile nell'ambito delle attività contrattuali, eventuali lacune della documentazione, della telemetria, delle configurazioni di logging. Le carenze rilevate vengono analizzate in termini di impatto sulla capacità di detection e vengono proposte delle azioni correttive.

L'appaltatore definisce in dettaglio e concorda con il Comune l'architettura, le fonti, le priorità, i risultati attesi ("use case"), i destinatari delle notifiche e i canali di contatto, tenendo conto degli IoC minimi pubblicati da ACN.

L'appaltatore configura raccolta, normalizzazione, correlazione e dashboard, documenta policy, regole e procedure di gestione delle emergenze. Per ciascuna fonte verifica che i dati effettivamente acquisiti, il parsing, i campi, i timestamp e le configurazioni di logging disponibili siano adeguati; ove le configurazioni della fonte non consentano una telemetria sufficiente, l'appaltatore indica al Comune le modifiche o integrazioni necessarie e ne supporta l'attivazione.

Il Comune mette a disposizione una macchina virtuale con funzione di "log collector; il dimensionamento preliminare previsto è pari a 16 vCore, 16 GB di RAM e 300 GB di disco, da validare dall'appaltatore in relazione ai flussi effettivi, ai picchi, alla conservazione temporanea e al buffering necessario in caso di indisponibilità della destinazione.

L'appaltatore definisce le modalità di inoltro sicuro dei log e le misure atte ad evitare perdita di eventi in caso di indisponibilità temporanea.

L'appaltatore esegue il tuning iniziale delle regole, elimina o documenta le anomalie di raccolta, verifica la reperibilità dei referenti e completa la documentazione. Il tuning comprende almeno l'analisi dei falsi positivi ricorrenti, la verifica degli use

case rispetto alla telemetria disponibile e l'adeguamento delle soglie o delle logiche senza ridurre ingiustificatamente la capacità di detection.

La conclusione della fase è attestata da verbale di verifica con esito positivo che contiene un prospetto delle integrazioni classificate come operative, operative con limitazioni o non operative.

## 3.3 Fase 2 – Esercizio a regime

A partire dalla conclusione positiva della fase 1, il SOC opera senza interruzione e vengono continuamente monitorati gli SLA.

L'appaltatore eroga tutte le prestazioni previste, verifica continuativamente lo stato dei flussi e periodicamente la loro completezza e qualità, mantenendo aggiornati configurazioni, IOC, connettori, parser, regole, use case e documentazione. Il tuning e l'adeguamento costituiscono attività continuative e sono effettuati quando necessari, in particolare a seguito di falsi positivi ricorrenti, evidenza di falsi negativi o incidenti non adeguatamente rilevati, modifiche significative delle fonti o variazioni rilevanti del contesto di minaccia. Il riesame del perimetro, dei gap e del rispetto degli SLA è almeno trimestrale. Le attività ordinarie di tuning e manutenzione sono eseguite e tracciate dall'appaltatore; le modifiche che comportano riduzione significativa della copertura, disattivazione di use case rilevanti o variazioni sostanziali del perimetro sono preventivamente concordate con il Comune.

## 3.4 Fase 3 – Uscita e trasferimento

Durante il tredicesimo mese non è richiesta la prosecuzione del monitoraggio SOC/SIEM; l'appaltatore garantisce la conservazione e l'accessibilità dei dati necessari al completamento del trasferimento.

Entro la scadenza del tredicesimo mese dalla stipula, l'appaltatore completa le attività di uscita e trasferimento e consegna i log ancora soggetti a conservazione, i ticket, i report, lo schema dell'architettura, le configurazioni, le regole di correlazione e la documentazione degli use case, nonché un riepilogo delle attività ancora aperte. Assiste il Comune nel completamento del passaggio di consegne. La cancellazione definitiva delle copie residue presso l'appaltatore avviene dopo la consegna e la verifica da parte del Comune della completezza e leggibilità dei dati e della documentazione trasferiti; l'appaltatore ne attesta per iscritto l'avvenuta esecuzione.

# 4 Servizi inclusi nel corrispettivo

## 4.1 Servizio SOC

### 4.1.1 Operatività del SOC

Il SOC garantisce presidio umano H24, sette giorni su sette per l'analisi degli alert prodotti dal SIEM, l'early warning e il controllo dello stato della telemetria. Nell'ambito degli incidenti, degli IOC e delle informazioni di minaccia pertinenti al perimetro, il servizio comprende anche attività mirate di ricerca retrospettiva e approfondimento sui dati disponibili, senza che ciò configuri un servizio separato di threat hunting continuativo.

La prima attività svolta è sempre la categorizzazione dell'evento in base alla seguente tabella:

| **Livello** | **Impatto** |
|---|---|
| P1 - Critical | Diffusa compromissione dei sistemi informativi o perdita di controllo sull'infrastruttura<br>Esfiltrazione di dati personali o particolari su larga scala<br>Blocco o degrado grave dei servizi pubblici per periodi prolungati<br>Potenziale impatto sulla sicurezza pubblica o sull'integrità di servizi essenziali |
| P2 - High | Interruzione o compromissione di un servizio pubblico essenziale<br>Accesso non autorizzato, alterazione o perdita di dati personali, particolari o tecnici |
| P3 – Medium | Impatto su più utenti o su un servizio/sistema non critico<br>Possibile rischio per dati personali o tecnici<br>Possibile degrado temporaneo delle prestazioni di un servizio |
| P4 - Low | Impatto limitato a un singolo utente o servizio/sistema non critico<br>Nessun coinvolgimento di dati personali o tecnici<br>Nessuna interruzione o degrado percepibile dei servizi |

Il servizio distingue triage iniziale, approfondimento tecnico e supporto specialistico agli incidenti, con escalation interna tracciata.

### 4.1.2 Monitoraggio, triage e gestione incidenti

Per ogni evento rilevante, il SOC verifica la pertinenza, attribuisce la severità, registra tempi e motivazioni nel ticket, individua asset e possibili impatti e avvisa i destinatari designati.

Per gli incidenti esegue analisi e supporta contenimento, mitigazione, risoluzione e ripristino. Le azioni che modificano i sistemi del Comune richiedono autorizzazione esplicita. L'appaltatore conserva le evidenze tecniche disponibili, mantenendo ove possibile il dato originale, la sorgente, i timestamp e la tracciabilità delle acquisizioni/esportazioni; per le evidenze esportate garantisce l'integrità mediante hash o meccanismo equivalente. Redige inoltre un rapporto tecnico di incidente secondo le tempistiche stabilite.

### 4.1.3 Escalation e notifiche

Il piano operativo identifica referenti primari e sostituti del Comune, canali ordinari e urgenti. L'appaltatore supporta il Comune nell'analisi e nella predisposizione degli elementi tecnici per gli eventuali adempimenti verso ACN/CSIRT e segnala tempestivamente gli eventi che, sulla base delle informazioni disponibili, risultino anche solo potenzialmente riconducibili alle fattispecie soggette a notifica, senza attendere la qualificazione definitiva. La qualificazione finale dell'obbligo e l'invio istituzionale restano in capo al Comune.

## 4.2 Servizio SIEM

### 4.2.1 Piattaforma e raccolta

La piattaforma messa a disposizione e condotta dall'appaltatore riceve i log dalla componente di raccolta e dalle fonti concordate ("log collector" ospitato su infrastruttura comunale), li normalizza e correla in tempo reale.

L'appaltatore gestisce connettori, parser, regole, controlli sulla continuità e sulla latenza dei flussi, aggiornamenti del software e degli IOC tramite feed istituzionali, open source e/o commerciali e la manutenzione correttiva. Deve inoltre rilevare l'assenza anomala di eventi o il degrado delle fonti in relazione al comportamento atteso della sorgente; per le fonti critiche, i tempi di silenzio o ritardo che determinano alert o ticket sono definiti durante il setup e riesaminati durante il servizio. Dashboard e report programmati o a richiesta sono esportabili in formati standard.

L'appaltatore verifica la qualità dei dati, non limitandosi alla mera presenza del flusso, ma considerando almeno correttezza del parsing, disponibilità dei campi e dei timestamp necessari, coerenza dei dati e adeguatezza rispetto agli use case applicabili. Esegue tuning continuativo, mantiene aggiornate le configurazioni e

registra le modifiche significative, le motivazioni e gli effetti attesi sulla capacità di detection.

Il servizio deve essere in grado di generare alert anche in base a logiche comportamentali. Qualora siano disponibili sistemi EDR sui server o sui client dell'Ente, l'appaltatore ne verifica la possibilità di integrazione e, ove tecnicamente possibile, acquisisce e correla nel SIEM i relativi dati e alert. L'attività è compresa nel corrispettivo.

## 4.3 Dashboard

L'appaltatore rende disponibile una interfaccia web con profili di accesso adeguati a consultare stato del servizio, eventi, classificazioni, ticket, indicatori SLA e regole di correlazione attive.
La dashboard fornisce informazioni direttamente o mediante report di immediata consultazione, come ad esempio lo stato di salute delle fonti e dell'ingestion (acquisizione), evidenziando almeno fonti silenti, degradate o in errore e anomalie rilevanti di raccolta.
Sono richiesti privilegi granulari, tracciatura completa degli accessi e delle attività, cifratura in transito e a riposo, resilienza e procedure di ripristino in caso di errore.

## 4.4 Reportistica e formazione

L'appaltatore produce report trimestrali con perlomeno i seguenti dati e con evidenza delle variazioni rispetto al trimestre precedente; il report include inoltre lo stato delle fonti degradate o intermittenti, i gap aperti e chiusi, gli use case aggiunti, modificati o disattivati e le principali attività di tuning effettuate:

- Fonti di log attive.
- Elenco degli eventi occorsi con descrizione sintetica, classificazione, trattamento.
- Elenco dei ticket aperti dal Comune di Trieste, con descrizione sintetica e trattamento.
- Analisi del rispetto di tutti gli SLA contrattualizzati, vedasi paragrafo 7.2 Livelli di servizio minimi.

Per gli incidenti "critical" o "high" fornisce anche rapporti tecnici su evidenze, cronologia, attività e misure suggerite.

La formazione iniziale all'uso delle dashboard e della reportistica dura almeno quattro ore effettuabili anche da remoto; materiali e registrazione dell'attività sono consegnati al Comune.

## 4.5 Requisiti tecnici minimi

| Requisito | Valore minimo o prestazione |
|---|---|
| Fonti di log | Collegamento ad almeno 120 server linux, 100 stack switch Cisco (fino a 300 dispositivi singoli), 20 server Windows, 2 cluster Fortigate (HA cluster). È incluso il supporto alla personalizzazione delle integrazioni e al loro mantenimento. |
| Capacità | Almeno 2.000 eventi al secondo (EPS) sostenuti, senza perdita, campionamento o soppressione degli eventi dovuti a limiti di capacità o licenza. La soluzione deve gestire picchi temporanei mediante capacità adeguata e/o accodamento e buffering, preservando gli eventi fino al ripristino della normale capacità di ingestion.<br>- Volume log medio stimato su 30gg: 20 GB/giorno<br>- Volume log massimo stimato su 30gg: 30GB/giorno |
| Trattamento | Acquisizione, normalizzazione e correlazione in tempo reale;<br>IOC aggiornati periodicamente. |
| Conservazione | Log conservati e interrogabili secondo una politica rolling: almeno 90 giorni di disponibilità operativa immediata, con log completi direttamente e liberamente interrogabili; almeno 12 mesi complessivi decorrenti dal timestamp del singolo evento per analisi forense, threat hunting, indagini post-incidente e analisi storiche. Alla cessazione del contratto, i dati ancora soggetti a conservazione sono consegnati al Comune secondo quanto previsto dal paragrafo 4. |
| Ubicazione | Conservazione e trattamento in infrastrutture ubicate nell'Unione europea. |

# 5 Modalità di erogazione del servizio

## 5.1 Requisiti operativi e governance

L'appaltatore nomina un responsabile del servizio e un referente tecnico e mantiene almeno: un registro aggiornato delle fonti, un registro degli use case. Il registro degli use case riporta, ove applicabile, le fonti necessarie, finalità, severità, stato, principali dipendenze, data dell'ultimo tuning e dell'ultima verifica.

L'appaltatore collabora con il Comune all'analisi dei report trimestrali.

Le attività ordinarie di tuning, manutenzione e adeguamento sono documentate e possono essere eseguite autonomamente dall'appaltatore; devono essere preventivamente concordate le modifiche che riducono significativamente la copertura, disattivano use case rilevanti o comportano variazioni sostanziali del perimetro.

Il Comune indica i propri referenti e le modalità di ingaggio.

## 5.2 Orari, strumenti e canali

Il presidio e i canali urgenti sono attivi H24/7. Il sistema di ticketing registra apertura, presa in carico, classificazione, escalation, comunicazioni e chiusura con data e ora. Le comunicazioni avvengono secondo i canali che verranno identificati.

# 6 Personale e requisiti professionali

## 6.1 Composizione e competenze

Il gruppo di lavoro dell'appaltatore comprende analisti per il triage continuativo, figure esperte per l'analisi degli incidenti e la conduzione SIEM e un responsabile per il coordinamento e gli SLA. Il gruppo deve disporre, nel suo complesso, di competenze adeguate alle principali tecnologie effettivamente integrate nel perimetro del servizio, senza vincolo a specifiche certificazioni salvo quanto eventualmente previsto negli atti di gara. Eventuali sostituzioni devono assicurare

continuità e pari competenza ed essere tempestivamente comunicate alla stazione appaltante.

## 6.2 Formazione e riservatezza

Il personale riceve istruzioni sulle procedure concordate con il Comune e sugli obblighi di riservatezza. Gli accessi sono personali, proporzionati al ruolo e revocati tempestivamente alla cessazione delle esigenze operative. L'allegato "Norme di comportamento terze parti" va considerato parte integrante del presente capitolato.

# 7 Livelli di servizio (SLA)

## 7.1 Regole di misurazione

I termini in minuti e ore sono da considerarsi continuativi H24/7 e misurati singolarmente per ogni caso; la misurazione decorre dalla generazione dell'alert nel SIEM o dalla segnalazione registrata nel sistema di ticketing, se precedente. La presa in carico richiede l'avvio documentato del triage da parte di un operatore e non si considera soddisfatta dalla sola modifica dello stato del ticket: deve risultare almeno l'assegnazione a un operatore e una prima valutazione tecnica dell'evento, anche preliminare.

Le indisponibilità delle fonti o della connettività vengono documentate e conteggiate negli SLA solo se imputabili all'appaltatore.

## 7.2 Livelli di servizio minimi

| Indicatore | Livello richiesto | Misura |
|---|---|---|
| Disponibilità del servizio SIEM/SOC (*) | Almeno 99% di disponibilità; | Mensile, sul tempo complessivo; escluse sole interruzioni concordate e documentate o imputabili alla infrastruttura comunale. |

| | | |
|---|---|---|
| Presa in carico Critical | Entro 30 minuti | Per evento rilevato dal SIEM. |
| Presa in carico High | Entro 60 minuti | Per evento rilevato dal SIEM. |
| Presa in carico Medium | Entro 240 minuti | Per evento rilevato dal SIEM. |
| Presa in carico Low | Entro 480 minuti | Per evento rilevato dal SIEM. |
| Percentuale di falsi positivi a regime dopo 4 mesi dalla stipula | < 20% a trimestre | KPI misurato sulla base degli alert chiusi e classificati come falso positivo o attacco; |
| Falsi positivi reiterati | Tuning entro 8 ore dalla conferma di prima categorizzazione di falso positivo | Per evento riportato dal SOC. |
| Report trimestrale | Entro 10 giorni lavorativi dalla scadenza del trimestre | Per report; consegna elettronica. |
| Eventi soggetti a notifica: avviso (**) | Entro 8 ore | Per evento; consegna elettronica. |
| Eventi soggetti a notifica: analisi preliminare (**) | Entro 24 ore | Per evento; consegna elettronica. |
| Eventi soggetti a notifica: analisi completa (**) | Entro 20 giorni | Per evento; consegna elettronica. |

(*) La soglia indicata per la disponibilità del servizio corrisponde alla disponibilità della piattaforma e dei canali operativi contrattuali; sono escluse dal conteggio le ore di indisponibilità imputabili al Comune di Trieste.

(**) Per eventi potenzialmente soggetti a notifica riconducibili all'Allegato 3 della Determinazione ACN n. 379907 del 19 dicembre 2025, come successivamente modificata, integrata o sostituita, l'appaltatore applica i seguenti SLA contrattuali di supporto al Comune (tali SLA non sostituiscono né modificano i termini di legge applicabili al soggetto notificante):

- avvisa il Comune entro 8 ore dalla decorrenza individuata al paragrafo 7.1
- trasmette un'analisi tecnica preliminare a supporto della comunicazione di cui all'art. 25, comma 5, lettera b), D.Lgs. 138/2024 entro 24 ore,
- trasmette un'analisi tecnica completa a supporto della comunicazione di cui all'art. 25, comma 5, lettera d) entro 480 ore (20 giorni solari).
- L'appaltatore aggiorna progressivamente l'analisi quando emergono nuove evidenze.

# 8 Modalità di partecipazione, requisiti e criteri di affidamento

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 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.

L'operatore economico che intenda partecipare alla presente procedura in forma individuale, non può manifestare interesse come componente di altro operatore economico con idoneità plurisoggettiva.

L'amministrazione non opera alcuna limitazione in ordine al numero di operatori economici che intendano partecipare alla presente procedura.

Le imprese interessate sono tenute a inoltrare il documento "Istanza_manifestazione_interesse_SOC_SIEM" e il documento "Piano_operativo_SOC_SIEM" compilati in ogni loro parte.

L'amministrazione, in esito all'istruttoria di valutazione di cui al punto 8.1, procederà all'individuazione del contraente esecutore ai sensi dell'art. 50, comma 1, lettera b) mediante Trattativa Diretta Mepa.

## 8.1 Elementi di valutazione del preventivo economico e del piano operativo

Il RUP esamina i preventivi acquisiti e individua la soluzione maggiormente rispondente alle esigenze dell'Amministrazione, tenendo conto degli elementi tecnici, organizzativi ed economici di seguito indicati.

Saranno valutati i seguenti elementi:

- Per i tempi di presa in carico è valutata la riduzione dei termini massimi previsti per gli eventi Critical, High, Medium e Low, considerando l'entità del miglioramento e la sua sostenibilità;
- Tempistiche e cronoprogramma: sono valutate la chiarezza e la sostenibilità del piano di attivazione, con indicazione delle fasi, dei tempi e delle priorità di integrazione delle fonti, delle dipendenze tecniche e delle verifiche previste prima dell'avvio a regime. Sono considerate favorevolmente le soluzioni che consentono di anticipare l'operatività sulle fonti più rilevanti e ridurre l'impegno del personale tecnico comunale, attraverso l'autonomia esecutiva dell'appaltatore e le misure descritte nel Piano operativo per minimizzare l'impatto sul reparto tecnico comunale
- Qualità della soluzione offerta: sono valutate l'adeguatezza e l'integrazione dei software e dei componenti proposti per l'erogazione del servizio SOC/SIEM, con indicazione delle relative funzioni, delle licenze incluse e degli eventuali limiti d'uso. Sono considerate la copertura degli scenari di attacco pertinenti al perimetro comunale, descritti mediante casi d'uso e relative fonti necessarie, la capacità di correlare eventi provenienti da sistemi diversi, inclusi, ove disponibili e tecnicamente integrabili, i sistemi EDR, e le modalità di verifica e aggiornamento delle regole di rilevamento. Sono inoltre valutate l'efficacia delle procedure di controllo della qualità dei log e di riduzione dei falsi positivi, nonché la chiarezza e l'utilità operativa delle dashboard e delle informazioni rese disponibili al Comune.
- Per la capacità del SIEM è valutata la capacità sostenuta offerta oltre il minimo di 2.000 EPS, riferita all'intera catena di raccolta, normalizzazione e correlazione. Sono considerate l'adeguatezza del dimensionamento e la capacità di gestire picchi e incrementi dei flussi senza perdita;

- Per le figure chiave e i gruppi assegnati al servizio sono valutate la pertinenza delle esperienze significative e l'adeguatezza dei ruoli e delle attività proposti, sulla base delle informazioni riportate alla sezione "FIGURE PROFESSIONALI E ORGANIZZAZIONE DEL GRUPPO DI LAVORO" dichiarate nell'istanza di manifestazione;
- Le migliorie devono essere descritte in modo preciso e verificabile nel Piano operativo, essere comprese nel prezzo e, in caso di affidamento, costituiscono obblighi contrattuali. La scelta del contraente dà conto dei vantaggi tecnici e organizzativi della soluzione proposta;
- Il prezzo complessivo è valutato sotto il profilo della convenienza, della congruità e della sostenibilità rispetto alle prestazioni e ai miglioramenti offerti, entro l'importo massimo previsto e con carattere omnicomprensivo.

# 9 Disposizioni

## 9.1 Verifiche di conformità

Il Comune verifica la corretta conclusione della fase iniziale mediante accesso alle dashboard, ticket di prova, verifica delle procedure concordate e verifica, su un campione rappresentativo di fonti e use case concordato con l'appaltatore, della catena di raccolta, normalizzazione, correlazione, generazione dell'alert ed escalation. Ove tecnicamente e operativamente possibile, la verifica utilizza eventi controllati o simulati. L'esito, le eventuali limitazioni e i gap residui vengono verbalizzati.

Il Comune di Trieste durante l'esercizio verifica trimestralmente i report; le carenze sono contestate all'appaltatore con richiesta di correzione e nuova verifica.

La chiusura del servizio richiede la consegna prevista al paragrafo 3.4 Fase 3 – Uscita e trasferimento.

## 9.2 Corrispettivo e inadempimenti

Il corrispettivo copre tutte le attività e le risorse necessarie al rispetto del presente capitolato. Le condizioni di fatturazione, la disciplina delle penali e gli ulteriori rimedi contrattuali sono regolati dagli altri atti di gara e dal contratto; il presente capitolato fornisce le evidenze tecniche per accertare le prestazioni.

## 9.3 Modifiche contrattuali

L'amministrazione, fermo restando la disponibilità finanziaria e nei limiti massimi di spesa complessiva di Euro 139.999,99 potrà disporre, ai sensi dell'art. 120, comma 9, del D.Lgs. 36/2023, la diminuzione o l'estensione delle prestazioni affidate nei limiti del 20% dell'importo contrattuale.

# 10 Sicurezza informatica

L'appaltatore dichiara che il servizio offerto mediante tecnologia "cloud" o "SaaS" è presente nel "Catalogo delle Infrastrutture digitali e dei Servizi cloud" dell'ACN. L'appaltatore comunica senza ritardo al Comune di Trieste ogni sospensione, revoca o altra variazione rilevante dello stato di qualificazione.

L'appaltatore, al momento della sottoscrizione del contratto, è tenuto a comunicare il nominativo del proprio referente per la sicurezza informatica, completo di recapiti telefonici ed e-mail. Ogni variazione deve essere comunicata entro 48 ore solari al RUP e alla casella cyber@comune.trieste.it. Il referente deve possedere competenze adeguate in materia di sicurezza informatica e garantire la continuità del contatto con l'Ente.

L'appaltatore è tenuto a collaborare e a fornire, su richiesta, report di conformità, attestazioni di audit di terza parte, o altra documentazione idonea a dimostrare il rispetto dei requisiti di sicurezza dichiarati. Il Comune di Trieste si riserva la facoltà di effettuare audit, ispezioni e verifiche documentali in qualsiasi momento della durata contrattuale.

L'appaltatore accetta l'esecuzione di test di sicurezza (penetration test) promossi dal Comune o da soggetti terzi da esso incaricati. In alternativa, l'appaltatore può fornire la documentazione rilasciata da enti indipendenti qualificati che attesti l'avvenuta esecuzione dei test e la risoluzione di eventuali vulnerabilità riscontrate.

L'appaltatore si impegna al pieno rispetto delle disposizioni contenute nel documento allegato "Norme di comportamento Terze Parti", che costituisce parte integrante e sostanziale del contratto.

L'appaltatore deve garantire la tempestiva applicazione delle patch di sicurezza e degli aggiornamenti software rilasciati dai produttori, assicurando che i sistemi

impiegati per l'esecuzione del contratto non presentino vulnerabilità note. Ogni aggiornamento critico deve essere tracciato e, su richiesta, documentato all'Ente.

L'appaltatore deve predisporre, mantenere aggiornato e testare periodicamente un piano di continuità operativa e di disaster recovery, in grado di garantire la ripresa dei servizi e la tutela dei dati in caso di incidente, nel rispetto degli SLA contrattuali. L'appaltatore si impegna ad effettuare le verifiche periodiche presenti nei due piani citati mettendone a disposizione del Comune gli esiti. L'appaltatore si impegna a partecipare a test di continuità operativa promossi dal Comune.

L'appaltatore è tenuto ad adottare misure adeguate di sicurezza fisica nei locali e nei data center che ospitano i sistemi o i dati dell'Ente, garantendo il controllo degli accessi, la protezione contro intrusioni e danneggiamenti, nonché la tracciabilità degli ingressi. I registri di accesso devono essere disponibili su richiesta per eventuali verifiche.

L'appaltatore garantisce che il personale coinvolto nelle attività oggetto del contratto riceva un'adeguata formazione in materia di cybersicurezza e protezione dei dati, con aggiornamenti periodici (almeno annuali) finalizzati al mantenimento di un livello adeguato di consapevolezza dei rischi informatici.

L'appaltatore deve assicurare che tutti i dati trattati nell'ambito del servizio siano cifrati sia a riposo sia in transito, mediante algoritmi conformi alle "linee guida funzioni crittografiche" di ACN. Le comunicazioni devono avvenire esclusivamente tramite protocolli sicuri e reti protette da adeguati sistemi di difesa.

L'appaltatore deve garantire il monitoraggio dei propri sistemi e la registrazione dei log di accesso e delle attività svolte per tutta la durata contrattuale, conservandoli per almeno sei mesi successivi alla cessazione del contratto. Tali log devono essere messi a disposizione dell'Ente in caso di audit, ispezioni o indagini.

L'appaltatore è tenuto a comunicare immediatamente dall'avvenuta conoscenza qualsiasi incidente di sicurezza informatica che possa compromettere dati o servizi dell'Ente, inviando una notifica alle caselle cyber@comune.trieste.it e dpo.privacy@comune.trieste.it contenente almeno data e ora, sistemi coinvolti, impatto presunto, misure immediate adottate, ulteriori azioni raccomandate. Restano ferme le ulteriori valutazioni e notifiche di legge in materia di NIS2 e protezione dei dati personali. L'appaltatore è tenuto a collaborare con l'Ente nella gestione dell'incidente e nell'attuazione delle misure di mitigazione e correttive.

L’appaltatore garantisce che ogni software fornito o sviluppato rispetti i principi di “security by design” e “security by default”, adottando pratiche di sviluppo sicuro, revisione del codice e aggiornamento continuo per la correzione di vulnerabilità o bug di sicurezza.

L’appaltatore garantisce che il software abbia la funzionalità per estrarre l’elenco completo degli utenti che hanno accesso al sistema, distinguendoli in base al ruolo, in particolare nel caso degli amministratori. Il report dovrà obbligatoriamente contenere l’informazione relativa all’ultima data di accesso.

Alla cessazione del contratto, l’appaltatore deve restituire tutti i dati e i documenti dell’Ente o prodotti per conto dell'Ente nei formati previsti contrattualmente e comunque aperti e interoperabili, cancellare in modo definitivo le copie residue, revocare gli accessi e fornire attestazione scritta delle operazioni eseguite. Eventuali strumenti concessi in uso devono essere restituiti contestualmente.

Ogni subfornitore, nel caso in cui effettui attività con potenziale impatto sui sistemi informativi e di rete dell’ente, deve sottostare alle medesime clausole di sicurezza dell’appaltatore.

L’autenticazione ai sistemi informatici deve avvenire tramite identità digitale multifattore (SPID, CIE o altre modalità conformi all’art. 64 del D.Lgs. 82/2005). Qualora la conformità al D.Lgs 82/2005 art. 64 non fosse tecnicamente possibile, comunque deve essere adottata un'autenticazione a più fattori (MFA).

L’appaltatore deve garantire che le abilitazioni concesse a terze parti siano limitate ai soli privilegi strettamente necessari per l’esecuzione delle attività contrattuali. L’insieme delle autorizzazioni deve essere oggetto di revisione periodica e aggiornamento tempestivo in caso di variazioni di ruolo o cessazione di rapporti di lavoro.

L’appaltatore è tenuto a fornire e mantenere costantemente aggiornato l'elenco del proprio personale dotato di credenziali di accesso ai sistemi dell’Ente, trasmettendo ogni variazione al RUP.

Nel caso in cui, per esigenze operative correlate alla corretta erogazione del servizio, si renda necessario il collegamento alla rete comunale di dispositivi di proprietà dell’appaltatore, questi devono:

- essere censiti in un elenco mantenuto aggiornato;

- qualora tecnicamente possibile, essere dotati almeno di antivirus aggiornato, Firewall attivo e sistema operativo supportato (non EOL) e costantemente aggiornato fornendo la relativa politica di aggiornamento;

- essere aggiornati senza ritardo a meno di giustificate ed approvate motivazioni tecniche."

L'appaltatore deve fornire ad inizio contratto e/o a ogni richiesta del Comune un elenco aggiornato di indirizzi IP pubblici e nomi di domino utilizzati a qualsiasi titolo per fornire il servizio. Ogni variazione deve essere comunicata preventivamente alla casella cyber@comune.trieste.it.

L'appaltatore deve produrre un'autodichiarazione circa l'assenza dei prodotti e dei servizi di cui al paragrafo B) della Circolare 14 novembre 2025 dell'ACN (Attuazione dell'art. 29, c. 3, del D.L. 21 marzo 2022 n. 21 – Diversificazione di prodotti e servizi tecnologici di sicurezza informatica [G.U. 22 novembre 2025 n. 272]).

L'appaltatore si impegna a manutenere i componenti software e la documentazione di supporto adattandoli ai requisiti di cybersicurezza previsti dalle normative tempo per tempo vigenti.

L'inosservanza delle clausole contrattuali legate alla sicurezza informatica viene considerata violazione contrattuale e come tale può comportare la risoluzione del contratto.

# 11 Uso dell'intelligenza artificiale

L'Aggiudicatario, nell'ambito dell'erogazione dei servizi oggetto del presente affidamento, è tenuto a garantire che l'eventuale utilizzo di sistemi di Intelligenza Artificiale (IA), inclusi modelli di machine learning, sistemi di generative AI e strumenti di automazione avanzata, avvenga nel rispetto della normativa applicabile, con particolare riferimento al Regolamento (UE) 2016/679 e al Regolamento europeo sull'Intelligenza Artificiale (AI Act).

A tal fine è richiesto che:

- le componenti IA debbano poter essere disabilitate su richiesta del Comune, senza perdita o degrado di funzionalità previste a capitolato;
- l'operatore economico indichi nell'offerta tutte le funzionalità della soluzione che utilizzano o incorporano sistemi o modelli di intelligenza artificiale,

specificandone finalità, modalità di impiego, modello o componente utilizzato, versione ove disponibile, soggetto fornitore e ruolo dei soggetti coinvolti ai sensi del Regolamento (UE) 2024/1689. Sono altresì indicate le funzionalità IA opzionali, disattivabili o attivabili successivamente;

- l'appaltatore comunichi i principali sistemi, modelli, componenti e soggetti terzi dai quali dipende l'erogazione delle funzionalità IA. Ogni modifica rilevante della funzionalità IA, del modello, del fornitore del modello, delle finalità, delle modalità di trattamento dei dati o delle condizioni di sicurezza è comunicata preventivamente al Comune, con indicazione degli effetti attesi. Il Comune può subordinare l'uso della versione modificata all'esito di una nuova verifica;
- l'appaltatore assicuri, per quanto di propria competenza e in relazione al ruolo rivestito, la conformità della soluzione alla normativa applicabile, incluso il Regolamento (UE) 2024/1689, e metta a disposizione del Comune le informazioni e la documentazione necessarie a consentire all'Ente di adempiere agli obblighi derivanti dal proprio ruolo. L'appaltatore comunica la classificazione della soluzione ai sensi dell'AI Act, le relative motivazioni e ogni variazione rilevante;
- la soluzione debba consentire un'effettiva supervisione umana secondo il caso d'uso definito dal Comune e non debba impedire all'utente autorizzato di verificare, correggere, non utilizzare o sostituire gli output prodotti. L'appaltatore rende disponibili informazioni sufficienti a comprendere finalità, capacità, limiti, condizioni d'uso e corrette modalità di supervisione della funzionalità IA;
- l'appaltatore non attivi autonomamente nuove funzionalità IA né modifichi le impostazioni IA disabilitate dal Comune. Le nuove funzionalità sono rese disponibili, ove tecnicamente possibile, in modalità non attiva e possono essere abilitate soltanto a seguito di decisione del Comune secondo le proprie procedure interne. Il Comune può chiedere di disabilitarle in qualunque momento;
- l'appaltatore informi senza indebito ritardo il Comune di incidenti, vulnerabilità, malfunzionamenti, degradi significativi delle prestazioni o altri eventi relativi alla componente IA che possano incidere sulla sicurezza, sui dati, sui diritti delle persone, sulla conformità normativa o sulla corretta erogazione del servizio. L'appaltatore fornisce le informazioni necessarie alla gestione

dell'evento e coopera nelle attività di contenimento, analisi, ripristino e adempimento;

- sia fatto espresso divieto di inserire, trasferire o comunque trattare dati, log, eventi di sicurezza o altre informazioni riconducibili al perimetro ICT del Committente, anche in forma parziale o pseudonimizzata, all'interno di servizi di IA pubblici o condivisi (quali, a titolo esemplificativo, ChatGPT, Microsoft Copilot o analoghi), anche mediante prompt, query o altri meccanismi di interazione;
- l'utilizzo di sistemi di IA avvenga esclusivamente in ambienti segregati e controllati (on-premise o tenant dedicati), idonei a garantire la separazione dei dati del Committente da quelli di altri clienti e da dataset utilizzati per l'addestramento o il miglioramento dei modelli;
- i dati del Committente non siano in alcun caso utilizzati per finalità di addestramento, riaddestramento, fine-tuning o miglioramento di modelli di IA;
- i dati del Committente non siano riutilizzati per finalità ulteriori rispetto all'erogazione del servizio né trasferiti a terzi, inclusi fornitori di tecnologie IA, salvo quanto strettamente necessario all'esecuzione del servizio e nel rispetto delle misure di sicurezza applicabili;
- siano adottate misure tecniche e organizzative adeguate a garantire la sicurezza, l'integrità e la riservatezza dei dati trattati, nonché la tracciabilità delle operazioni effettuate tramite sistemi di IA.

Resta ferma la piena responsabilità dell'Aggiudicatario per qualsiasi utilizzo non conforme dei sistemi di Intelligenza Artificiale e l'obbligo di manlevare e tenere indenne il Committente da ogni conseguenza pregiudizievole derivante da tale utilizzo.

# 12 Fatturazione

La fatturazione avviene con periodicità trimestrale posticipata. Il pagamento è subordinato alla verifica della regolare esecuzione delle prestazioni relative al periodo, anche sulla base del report trimestrale e il saldo finale è subordinato alla verifica del completamento delle attività di uscita e trasferimento previste al paragrafo 3.4.

# 13 Penali

## 13.1 Disposizioni generali

Le penali previste dal presente articolo si applicano agli inadempimenti imputabili all'Appaltatore, nel rispetto dell'articolo 126 del D.Lgs. 36/2023 e secondo il procedimento di contestazione disciplinato di seguito.
Ai fini del calcolo delle penali, per «importo netto contrattuale» si intende il corrispettivo complessivo risultante dall'affidamento, al netto dell'IVA.
L'Appaltatore risponde anche degli inadempimenti dei propri dipendenti, collaboratori, subappaltatori, subfornitori e degli altri soggetti dei quali si avvale per l'esecuzione del contratto.
Non sono applicate penali per ritardi o disservizi imputabili al Comune o derivanti da cause non imputabili all'Appaltatore. Quest'ultimo è tenuto a segnalare tempestivamente tali circostanze, documentandone la causa, la durata, gli effetti sulle prestazioni e le misure adottate per limitarne le conseguenze. L'eventuale esclusione dal computo è riconosciuta dal Comune sulla base delle evidenze disponibili.

## 13.2 Ritardo nel completamento della fase di setup

In caso di mancato completamento delle prestazioni della fase di setup di cui al paragrafo 3.2 entro il termine contrattualmente previsto, si applica una penale pari all'1‰ dell'importo netto contrattuale per ogni giorno solare di ritardo.
Il ritardo decorre dalla scadenza del termine previsto fino alla data di effettivo completamento delle prestazioni dovute, accertata dal Comune.
Non sono conteggiati i tempi impiegati dal Comune per le verifiche successive al completamento delle prestazioni, salvo che tali verifiche evidenzino carenze imputabili all'Appaltatore che impediscano l'accettazione della fase.

## 13.3 Ritardo nel rispetto degli SLA e degli altri termini contrattuali

Per il superamento dei termini previsti al paragrafo 7.2 relativamente alla presa in carico degli eventi, al tuning dei falsi positivi reiterati, alla consegna dei report e alla trasmissione degli avvisi e delle analisi degli incidenti, si applica una penale pari

all'1‰ dell'importo netto contrattuale per ogni giorno di ritardo, riferita a ciascun adempimento.
La stessa penale si applica al ritardo nella consegna dei dati e della documentazione e nel completamento delle attività di uscita e trasferimento di cui al paragrafo 3.4.
Quando il ritardo è inferiore a un giorno, la penale è calcolata proporzionalmente alla sua durata effettiva, assumendo un giorno pari a ventiquattro ore e considerando anche le frazioni di ora.
La decorrenza dei termini e le eventuali esclusioni sono determinate secondo le disposizioni del capitolato applicabili alla prestazione interessata. Quando il termine di adempimento è espresso in giorni lavorativi, il ritardo decorre dalla scadenza di tale termine ed è successivamente computato in tempo solare continuativo.
Qualora siano stati accettati nell'affidamento termini migliorativi rispetto a quelli minimi del capitolato, le penali sono applicate rispetto ai termini migliorativi divenuti obbligazioni contrattuali.

## 13.4 Mancato rispetto degli indicatori percentuali

Per il mancato rispetto dell'indicatore di disponibilità del servizio previsto al paragrafo 7.2, si applica, per ciascun mese di riferimento, una penale pari all'1‰ dell'importo netto contrattuale per ogni punto percentuale di disponibilità inferiore alla soglia contrattuale. Per le frazioni di punto percentuale il calcolo è proporzionale.
Per il mancato rispetto dell'indicatore relativo alla percentuale di falsi positivi, si applica, per ciascun trimestre nel quale l'indicatore è contrattualmente operativo, una penale pari all'1‰ dell'importo netto contrattuale per ogni punto percentuale di superamento del valore del 20%, con calcolo proporzionale per le frazioni di punto percentuale e con una penale minima pari all'1‰ dell'importo netto contrattuale.
Poiché il capitolato richiede una percentuale di falsi positivi inferiore al 20%, la penale minima si applica anche quando il valore rilevato è esattamente pari al 20%.
Gli indicatori sono determinati secondo le regole di misurazione del capitolato, sulla base delle registrazioni e delle evidenze verificabili. La sola mancanza di dati sufficienti non consente di presumere il raggiungimento o il mancato raggiungimento del livello richiesto; resta fermo l'obbligo dell'Appaltatore di produrre la documentazione dovuta.

## 13.5 Cumulo e limiti

Le penali possono essere applicate congiuntamente quando riguardano obbligazioni distinte e inadempimenti autonomi.
Quando il medesimo fatto integra esclusivamente diverse qualificazioni dello stesso inadempimento, si applica la sola penale di importo maggiore. Resta possibile il cumulo quando siano accertate violazioni ulteriori e autonome, dandone espressa motivazione.
L'importo complessivo delle penali per ritardo riferibili alla medesima giornata non può superare l'1,5‰ dell'importo netto contrattuale. In caso di superamento, gli importi sono ricondotti a tale limite.
L'ammontare complessivo di tutte le penali applicate durante l'esecuzione del contratto non può superare il 10% dell'importo netto contrattuale.

## 13.6 Contestazione e applicazione

Il Comune contesta per iscritto all'Appaltatore l'inadempimento rilevato, indicando la prestazione interessata, i fatti accertati, il periodo di riferimento, le evidenze disponibili e il calcolo della penale proposta.
L'Appaltatore può presentare controdeduzioni e documentazione giustificativa entro dieci giorni naturali e consecutivi dal ricevimento della contestazione.
Esaminate le controdeduzioni, oppure decorso il termine senza riscontro, il Comune comunica la propria determinazione motivata, disponendo l'archiviazione, la riduzione o l'applicazione della penale.
L'accertamento dell'inadempimento e il calcolo della penale sono effettuati dal Comune. Le registrazioni dei sistemi e i report dell'appaltatore costituiscono elementi istruttori e non determinano automaticamente l'addebito.
Il procedimento di contestazione non sospende gli obblighi di esecuzione, intervento e ripristino a carico dell'Appaltatore.

## 13.7 Recupero delle somme e ulteriori rimedi

Le penali definitivamente applicate sono recuperate mediante detrazione dai corrispettivi dovuti, nei limiti consentiti dalla legge, oppure mediante richiesta di

pagamento all'Appaltatore. In caso di mancato pagamento, il Comune può rivalersi sulla garanzia definitiva secondo la relativa disciplina.
L'applicazione delle penali non esonera l'Appaltatore dall'esatto adempimento delle obbligazioni contrattuali.
Resta salvo il diritto del Comune al risarcimento dell'eventuale maggior danno, evitando duplicazioni risarcitorie.
In presenza di inadempimenti gravi o reiterati, oppure qualora le penali maturate raggiungano il limite complessivo previsto, il Comune valuta l'attivazione dei rimedi contrattuali, compresa la risoluzione, nel rispetto dell'articolo 122 del D.Lgs. 36/2023 e delle altre disposizioni applicabili. Il raggiungimento del limite non costituisce autorizzazione a proseguire l'esecuzione in modo difforme dagli obblighi contrattuali.

# 14 Protezione dei dati personali e nomina a responsabile del trattamento

Il Comune di Trieste opera quale titolare del trattamento dei dati personali trattati nell'ambito del servizio. Per le attività di trattamento svolte per conto del Comune, l'Appaltatore è designato responsabile del trattamento ai sensi dell'articolo 28 del Regolamento (UE) 2016/679.
L'Appaltatore è tenuto a fornire le informazioni necessarie alla predisposizione dell'atto di nomina e a sottoscriverlo secondo il modello adottato dal Comune. L'atto è perfezionato contestualmente alla stipula del contratto e, in ogni caso, prima di qualsiasi accesso o trattamento di dati personali per conto del Comune, comprese le attività di setup.
L'atto di nomina e i relativi allegati costituiscono parte integrante della disciplina contrattuale e individuano le attività affidate, la durata, la natura e le finalità del trattamento, le categorie di dati personali e di interessati, le istruzioni del titolare e gli obblighi del responsabile.
L'Appaltatore tratta i dati esclusivamente per l'esecuzione del servizio e secondo le istruzioni documentate del Comune. Il ricorso a ulteriori responsabili del trattamento è subordinato all'autorizzazione del Comune e alle condizioni stabilite nell'atto di nomina, nel rispetto dell'articolo 28, paragrafi 2 e 4, del Regolamento.

Alla cessazione del servizio, la restituzione dei dati e la cancellazione delle copie sono effettuate secondo le istruzioni del Comune, l'atto di nomina e le disposizioni contrattuali sul trasferimento finale, assicurando il coordinamento con le verifiche di completezza e leggibilità dei dati consegnati. Restano salvi gli obblighi di conservazione previsti dalla legge.
Gli adempimenti derivanti dalla nomina sono compresi nel corrispettivo contrattuale. La mancata sottoscrizione dell'atto per causa imputabile all'Appaltatore impedisce l'avvio dei trattamenti e costituisce inadempimento contrattuale, ferme le ulteriori conseguenze previste dal contratto e dalla legge.