

CAPITOLATO PER LA FORNITURA DEL SERVIZIO DI ASSISTENZA SISTEMISTICA SUL FIREWALL CHECK POINT PER 12 MESI E DI ATTIVITA' DI PROGETTAZIONE E SUPPORTO SPECIALISTICO PER TECH REFRESH HW CHECK POINT

Art. 1 Oggetto e importo contrattuale

La presente trattativa ha per oggetto la fornitura del servizio di assistenza sistemistica per Firewall Check Point per la durata di 12 mesi e di attività di progettazione tecnica e supporto specialistico (tech refresh HW Check Point) con migrazione nel DC Lepida, nelle modalità specificate al successivo articolo 2

L'importo complessivo a base della trattativa è pari a **€. 14.0000,00 (iva esclusa)**, così suddiviso: **€ 11.000,00 (iva esclusa)** per il servizio di assistenza sistemistica (**art. 2 lett. A**) - **€. 3.000,00 (iva esclusa)** per le attività di progettazione e supporto specialistico (**art. 2 lett. B**)

Art. 2 Descrizione e durata

La descrizione dettagliata e la durata dei servizi oggetto della presente trattativa sono riportati di seguito.

Let. A - Servizio di assistenza sistemistica al sistema Firewall Check Point in uso presso l'Ente

Attualmente la soluzione Firewall Check Point utilizzata dall'Ente è così composta:

- N.1 Virtual Appliance Security Management Server Check Point
- N.2 Gateway Check Point con bundle NGTX, su piattaforma Open Certified Server con licenza 8 core.
- N.1 appliance SandBlast TE250X con licenza NGTX

- licenze Mobile unlimited per l'accesso VPN

La Security Management è installata su macchina virtuale VMWare mentre il cluster di firewall Check Point lavora su una coppia di Server HP DL360p Gen9 ognuno con le seguenti caratteristiche:

- Processore Intel E5-2630V3 con 8 core
- Memoria, 16GB
- Dischi, 3 x 300GB 12G SAS in configurazione Raid 1 + spare
- Network Interface, 6 porte Gigabit Ethernet 1000 Base Tx e 2 porte 10Gb
- Alimentazione singolo 500W

Il bundle installato include le seguenti blade:

- Firewall
- VPN
- Advanced Networking & Clustering



Area Risorse Servizio Gestione e Sviluppo delle Tecnologie e dei Sistemi informativi

P.zza Scapinelli, 2 - 42121 Reggio Emilia

- Identity Awareness
- Application Control (*)
- URL Filtering (*)
- Anti-Virus (*)
- Intrusion Prevention System (*)
- Antibot (*)
- Antispam (*)

(*) Service Blade coperte da un canone di servizio attivo fino al 31/08/2023

E' inoltre attivo il Supporto hardware/software di tipo Collaborative Enterprise Standard Edition comprensivo del rinnovo dei servizi a canone, valido fino al 31/08/2023 sia per i bundle NGTX che per l'appliance TE250X (HW e SW)

I server HP sono coperti da un servizio di manutenzione HW erogato direttamente da HP con modalità on-site NBD

Nessuno dei software o sistemi operativi coinvolti nel servizio è stato dichiarato in end-of-support dal vendor e l'infrastruttura è stata installata rispettando i requisiti (minimi, tabelle di compatibilità, ecc.) dichiarati dal vendor.

Caratteristiche del servizio richiesto

I referenti informatici del Servizio Gestione Tecnologie sono in grado di operare in autonomia su attività ordinarie di modifica della configurazione e/o di analisi degli eventi e del traffico dell'infrastruttura firewall Check Point installata presso l'ente.

E' però necessario attivare un servizio esterno di assistenza sistemistica per la gestione di problematiche ed attività per cui siano richieste competenze maggiori e/o l'escalation verso il vendor.

Il servizio di assistenza sistemistica richiesto dovrà pertanto operare in stretta sinergia con il personale dell'Ente, avrà come perimetro di azione il firewall Check Point nella configurazione descritta precedentemente e riguarderà le seguenti attività:

- gestione eventi anomali
- esecuzione di operazioni di riconfigurazione
- supporto sistemistico ai referenti informatici dell'ente

Il fornitore dovrà mettere a disposizione una propria struttura interna che sarà il "punto di contatto" per l'ente (POC) e che avrà la responsabilità della gestione del servizio di assistenza sistemistica oggetto della fornitura con le modalità di seguito descritte.

I tecnici del POC dovranno avere ottime conoscenze sistemistiche della piattaforma firewall Check Point nonché della configurazione attivata presso l'ente (vedi start-up del servizio).

P.zza Scapinelli, 2 - 42121 Reggio Emilia

Non rientrano nel servizio richiesto attività inerenti problematiche hw sui server fisici, interventi sistemistici relativi all'infrastruttura Vmware, la copertura delle parti di ricambio, contratti di manutenzione hardware e software.

Gestione eventi anomali

Rientra in questa categoria ogni evento non pianificato o comportamento anomalo che non è parte dell'operatività standard del firewall e che causa o può causare un'interruzione, o una riduzione, della qualità del servizio o dell'operatività degli utenti.

Le attività che verranno messe in atto per la risoluzione dell'evento anomalo possono coinvolgere oltre al fornitore del servizio di assistenza sistemistica anche il personale dell'Ente o eventuali Terze Parti e verranno svolte con l'obiettivo di ripristinare il funzionamento normale nel più breve tempo possibile e minimizzando gli impatti negativi sull'operatività. L'ente può richiedere che il POC si interfacci direttamente con eventuali terze parti coinvolte nella soluzione.

Se necessario saranno messe in atto anche soluzioni temporanee (workaround), nell'ottica di assicurare il mantenimento del miglior livello di operatività possibile.

Il servizio dovrà prevedere da parte del fornitore un supporto di Primo Livello e di Secondo Livello

Supporto di Primo Livello.

Il supporto di I livello include assistenza sistemistica basata su procedure pre-concordate le quali non richiedono autorizzazioni specifiche per essere eseguite e che non costituiscono modifiche tecnologiche.

Qualora il problema permanga il POC dovrà passare il caso al secondo livello che può essere:

- il supporto specialistico del fornitore stesso
- il supporto sistemistico di Check Point
- una Terza Parte

Supporto di secondo livello

Il supporto di II livello include l'assistenza sistemistica specialistica.

In questo ambito gli operatori del POC metteranno in campo le specializzazioni e le competenze in loro possesso per assicurare che l'operatività normale sia ripristinata nel più breve tempo possibile e che l'impatto negativo sull'ente sia minimizzato, anche tramite l'impiego di workaround.

Qualora sia necessario coinvolgere il supporto sistemistico di Check Point, il POC effettuerà la gestione del processo di escalation, utilizzando la partnership esistente. Nel caso di escalation saranno applicati i livelli di servizio previsti dal contratto con Check Point e sarà cura del POC assicurarsi che vengano rispettati e informare l'ente di eventuali inadempienze da parte del vendor.

Classificazione degli eventi anomali

I livelli di servizio si basano sulla priorità attribuita all'evento anomalo.

Sono stati definiti tre livelli di priorità:

- Priorità 1 (P1): livello più alto di importanza

- Priorità 2 (P2): livello di media importanza
- Priorità 3 (P3): livello di bassa importanza

Questi livelli sono determinati da Criticità e Impatto. Gli impatti riguardano il numero di utenti coinvolti mentre la Criticità misura l'importanza del problema

Tabella 1: Classificazione degli impatti causati da un evento anomalo

Impatto	Definizione
Enterprise	<ul style="list-style-type: none"> • Impossibilità di operare per tutti gli utenti o per la maggioranza degli stessi • Perdita totale di uno o più servizi fondamentali per l'ente • Incapacità di eseguire i servizi strategici per l'ente
Dipartimento, Sito, Gruppo di Utenti	<ul style="list-style-type: none"> • Evidente effetto sulla capacità di erogare un servizio importante per l'ente • Coinvolge un gruppo di utenti o un intero servizio dell'ente
Singolo Utente	<ul style="list-style-type: none"> • Nessun impatto sui servizi critici, ed impatta un solo utente

Tabella 2: Livelli di criticità associati ad un evento anomalo

Criticità/Urgenza	Definizione
1 (Critica)	Perdita di servizio immediata, senza un workaround disponibile
2 (Alta)	Perdita di servizio imminente, oppure immediata, ma riducibile tramite workaround
3 (Media)	Perdita di servizio NON critico da uno a più utenti impattati
4 (Bassa)	Nessuna perdita di servizio, gli utenti continuano a lavorare seppure con qualche disagio

Tabella 3: Classificazione delle Priorità di un evento anomalo

Priorità	Criticità	Impatto		
		Enterprise	Dipartimento, Sito, Gruppo di Utenti	Singolo Utente
	1	P1	P1	P2
	2	P1	P2	P2
	3	P2	P2	P3
	4	P2	P3	P3

La classificazione della priorità dell'evento anomalo viene proposta dai referenti tecnici dell'ente e può essere modificata dal personale tecnico del POC durante il periodo di presa in carico della chiamata, in quanto solo avendo tutte le informazioni a disposizione è possibile stabilirlo.

Esecuzione di operazioni di riconfigurazione

P.zza Scapinelli, 2 - 42121 Reggio Emilia

Rientrano in questo tipo di attività operazioni di riconfigurazione dovute ad esigenze **legate alla normale operatività**, e non attività di riorganizzazione della configurazione, modifiche sostanziali della topologia logica o fisica dell'architettura firewall che si configureranno invece come progetti veri e propri e pertanto esclusi dal presente contratto.

E' onere del fornitore la **valutazione preventiva** del rischio e dell'impatto dell'operazione di riconfigurazione richiesta, tenendo conto sia della probabilità che l'attività abbia esiti negativi che vadano ad influire sui livelli di servizio o, in generale, sui servizi erogati, sia dei rischi connessi alla mancata riconfigurazione.

Il fornitore dovrà pertanto tenere conto di:

1. dipendenze esterne (disponibilità di sistemi, risorse, fornitori, esecuzione contemporanea di altre riconfigurazioni);
2. possibilità di effettuare un test prima dell'implementazione;
3. esistenza di un piano di roll-back (un piano che permetta di ripristinare il servizio alla situazione preesistente).

Le operazioni di riconfigurazione sono le seguenti:

- Attività ricorrenti o di ordinaria amministrazione caratterizzate da basso rischio e basso impatto e con impegno non superiore alle 2 ore di attività da remoto. Sono richieste dai referenti del Servizio Gestione e Sviluppo delle tecnologie e possono essere svolte durante il normale orario lavorativo, eventualmente previo avviso agli utenti. Dovranno essere comunque concordate con i referenti dell'ente soprattutto quando modificano le politiche di sicurezza o potrebbero causare disservizi.
- Attività di patching e/o di aggiornamento di minor release che dovranno comunque essere pianificate in accordo con i referenti dell'ente. Sono incluse le attività di aggiornamento dell'infrastruttura Check Point a R81.20, che introduce importanti nuove funzionalità e un supporto prolungato (Novembre 2026). Viene prevista anche l'attività per gestire upgrade software, più attivazione e configurazione nuove funzionalità e revisione policy threat prevention

Supporto sistemistico ai referenti informatici dell'ente

Il servizio di supporto sistemistico include attività di "How-to" verso i referenti informatici dell'ente. Non rientrano attività di formazione strutturata o training on-the-job, ma semplicemente:

- supporto specialistico puntuale su modalità operative necessarie ad attivare una determinata configurazione che possa poi essere resa operativa dal personale dell'ente in autonomia
- possibili soluzioni adottabili per rispondere ad una data esigenza

E' responsabilità del fornitore far presente eventuali rischi od impatti relativi alla configurazione richiesta

Livelli di servizio

I livelli di servizio prevedono un **tempo di richiamata** ed un **tempo di intervento**: entro il primo il POC è tenuto a raccogliere tutte le informazioni utili per la presa in carico e la soluzione della richiesta, entro il secondo il POC deve garantire l'erogazione dell'intervento da remoto.

Il tempo di richiamata viene calcolato a partire dall'orario della richiesta mentre il tempo di intervento decorre dal termine del tempo di richiamata; entrambi vengono calcolati sulla base della copertura oraria richiesta per il servizio.



Area Risorse Servizio Gestione e Sviluppo delle Tecnologie e dei Sistemi informativi

P.zza Scapinelli, 2 - 42121 Reggio Emilia

	Tempo richiamata	di	Tempo intervento remoto	di	Tempo intervento onsite garantito	di	Copertura Oraria
Eventi anomali (P1)	Max 1 ora		Max 4 ore		N/A		Lunedì-venerdì (festivi esclusi) 8:30-12:30, 14:00-18:00
Eventi anomali (P2, P3)	Max 2 ore		Max 6 ore		N/A		Lunedì-venerdì (festivi esclusi) 8:30-12:30, 14:00-18:00
Operazioni di riconfigurazione / attività di supporto	Max 2 ore		Max 6 ore		N/A		Lunedì-venerdì (festivi esclusi) 8:30-12:30, 14:00-18:00

Il servizio viene erogato principalmente da remoto tramite collegamento VPN ma è prevista la possibilità di interventi on-site senza costi aggiuntivi per l'ente, qualora questi si riferiscano ad eventi di particolare gravità (priorità P1) o attività particolarmente critiche.

Modalità di erogazione

Il fornitore deve mettere a disposizione dell'ente diverse modalità di accesso al servizio:

- via web
- tramite e-mail, telefono o fax

Per ciascuna richiesta il POC deve aprire un caso a cui è assegnato un codice identificativo univoco che viene comunicato via email ai referenti dell'ente. Deve essere possibile consultare il portale web per ottenere informazioni su chi ha in carico la propria richiesta e sullo stato in cui si trova il relativo processo di elaborazione.

L'accesso al servizio sarà effettuato solo dai referenti dell'ente individuati durante il processo di avvio del servizio.

Le richieste di riconfigurazione saranno effettuate solamente via web o via email.

Per l'erogazione del servizio l'Ente mette a disposizione un accesso da remoto ai gateway Check Point e alla Management con privilegi di amministratore.

Durata del servizio

Il servizio decorre dal 1/4/2023 fino al **31/03/2024**.

Il servizio include ticket illimitati

Requisiti di partecipazione e modalità di aggiudicazione

Considerata l'alta criticità dei dispositivi oggetto dell'attività è necessario il possesso dei seguenti requisiti di capacità tecniche:

- Livello certificazione partner: Gold 5 stelle
- Certificazioni professionali: almeno 2 CCSM Elite

Lett. B) - Attività di progettazione tecnica e supporto specialistico (tech refresh HW CP)

Il Comune di Reggio Emilia intende rinnovare, sia tecnologicamente che dal punto di vista topologico, il sistema Firewall attualmente in uso. Al fine di individuare la migliore soluzione disponibile sul mercato, in un'ottica di piena compatibilità con l'infrastruttura e l'organizzazione tecnologica, e di conformità alle linee guida del Dipartimento per la Trasformazione Digitale della Misura 1.2 del PNRR, l'Ente ha la necessità di affidare, con la presente trattativa, la realizzazione delle attività di seguito dettagliate:

- Analisi dei fabbisogni per refresh tecnologico Hardware Check Point e migrazione in Datacenter Lepida;
- analisi configurazione attuale e proposta nuove soluzioni adeguate all'esigenza dell'Ente post migrazione risorse in DC di Lepida
- progettazione di nuova infrastruttura di firewalling in datacenter di Lepida e nuova infrastruttura di firewalling presso Comune di Reggio per gestione dei servizi non migrati verso il datacenter
- definizione risorse necessarie per realizzazione progetto (Hardware, software, tempistiche per realizzazione, configurazione e collaudo)

Nel documento finale di progetto che il fornitore dovrà produrre, devono essere rispettati i requisiti di conformità tecnica previsti dalle linee guida del Dipartimento per la Trasformazione Digitale per il cloud, finanziabile tramite investimenti del PNRR (Avviso Misura 1.2 – “Abilitazione al Cloud per le PA Locali”)

Le tempistiche di realizzazione e conclusione delle suddette attività devono essere concordate con il referente tecnico dell'Ente e comunque **dovranno concludersi entro e non oltre il 30/09/2023**. Tale scadenza potrà essere posticipata, solo per sopravvenute esigenze da parte dell'Ente

Art. 3 Documentazione amministrativa da presentare

La ditta deve presentare, mediante la piattaforma MEPA, i seguenti documenti:

- **dichiarazione da rendere ex artt. 46 e 47 del DPR 445/2000 attestante il possesso dei requisiti per l'ammissione**, debitamente **firmata digitalmente** dal Legale Rappresentante;
- **originali digitali ovvero scansione PassOE** rilasciato dall'Autorità Nazionale Anticorruzione a seguito di accreditamento al seguente indirizzo internet: <https://ww2.anticorruzione.it/idp-sig/> e successivo inserimento dei dati identificativi del procedimento in oggetto; non è necessario che i PassOE siano firmati dalla ditta.

Art. 4 Corrispettivi e obblighi relativi alla tracciabilità dei flussi finanziari

I corrispettivi sono quelli risultanti dalla stipula della trattativa diretta e la fatturazione dovrà avvenire:

- per il servizio di assistenza sistemistica al sistema Firewall Check, di cui all'art. 2 lett. A, in due tranche anticipate di pari importo;
- per le attività di progettazione tecnica e supporto specialistico, di cui all'art. 2 lett. B, in un'unica soluzione dopo consegna del progetto.

P.zza Scapinelli, 2 - 42121 Reggio Emilia

Il pagamento delle fatture sarà effettuato dal Comune a 30 giorni data di ricevimento fattura, previo controllo e verifica in ordine alla regolarità e rispondenza formale e fiscale e ottemperando a quanto disposto dall'art.25 del D.L. 66/2014 relativamente all'obbligo della fatturazione elettronica.

La ditta affidataria assume l'obbligo di tracciabilità dei flussi finanziari relativi al presente contratto secondo la disciplina contenuta nella Legge 136 del 2010 e successive modifiche.

L'inadempienza di tale obbligo comporta la risoluzione di pieno diritto del presente contratto ai sensi dell'articolo 1456 del codice civile.

Art. 5 Costi della sicurezza

Ai sensi del combinato disposto degli art. 86, comma 3bis e 3ter, del D.Lgs. n. 50 del 18.04.2016 e dell'art. 26, comma 3, del D.Lgs. n. 81/2008, ed in considerazione di quanto indicato con determina dall'Autorità di Vigilanza sui contratti pubblici di lavori, servizi e forniture del 5 marzo 2008 "Sicurezza nell'esecuzione degli appalti relativi a servizi e forniture", si ritiene che i costi della sicurezza derivanti da "interferenze" siano pari a zero.

Con riferimento a possibili rischi dati da interferenze, si precisa che non è stato pertanto predisposto il D.U.V.R.I., in quanto viste le attività oggetto dell'appalto non si ravvisano interferenze per le quali intraprendere misure di prevenzione e protezione atte a eliminare e/o ridurre i rischi trattandosi di attività di natura intellettuale; gli oneri relativi risultano quindi essere pari a zero in quanto non sussistono rischi interferenti da valutare, fermi restando gli obblighi a carico dell'impresa in ordine alla sicurezza sul lavoro.

Resta fermo che il concorrente dovrà indicare, nella Dichiarazione di Offerta Economica i costi relativi alla sicurezza afferenti all'esercizio dell'attività svolta dal concorrente medesimo.

Art. 6 Subappalto

L'amministrazione non autorizza il subappalto in conformità all'art. 105 del D.Lgs. n. 50/2016.

Art. 7 Risoluzione del contratto

In caso di inadempimento accertato dall'Amministrazione, nel concorso delle circostanze previste dagli articoli 1453 e seguenti del Codice Civile, si darà luogo alla risoluzione del contratto, previa diffida del Dirigente del Servizio ad adempiere nelle forme stabilite dalla legge, senza pregiudizio della rifusione dei danni e delle spese.

Nel caso di inosservanza, da parte dell'aggiudicatario, delle modalità e dei parametri di esecuzione delle attività previste e dettagliate nei documenti della trattativa, l'Amministrazione ha facoltà di risolvere il contratto, con particolare riferimento ai seguenti casi:

- gravi violazioni degli obblighi sottoscritti, anche a seguito di diffide ad adempiere per ripetute inadempienze contrattuali regolarmente contestate, per almeno cinque volte;
- subappalto non autorizzato;
- nel caso in cui le transazioni finanziarie siano eseguite con strumenti che non consentano la piena tracciabilità delle stesse, così come previsto dall'art. 3 comma 8 della Legge 13.08.2010 n. 136;

P.zza Scapinelli, 2 - 42121 Reggio Emilia

- in presenza di Durc Negativo per due volte consecutive, ai sensi dell'art. 6 comma 8 del D.P.R. 207/2010;

Qualora l'aggiudicatario dovesse cessare l'attività o trasferirla ad altro titolare, sarà pure facoltà dell'Amministrazione comunale, di recedere dal contratto in vigore o di continuarlo col nuovo titolare, fatta salva la responsabilità dell'aggiudicatario e del nuovo titolare per le obbligazioni anteriori al trasferimento.

In caso di fallimento dell'affidatario sarà facoltà dell'Ente di ritenere sciolto il contratto salvi gli effetti previsti dalla normativa vigente.

Art. 8 Recesso dal contratto

Per sopravvenuti motivi d'interesse pubblico l'Amministrazione si riserva la facoltà di recedere dal contratto, ai sensi dell'art. 1671 del c.c., fino al termine della validità contrattuale.

Tale facoltà è esercitata per iscritto mediante invio di apposita comunicazione a mezzo di raccomandata A.R. o PEC.

Ai sensi del Decreto Legge n. 95/2012, convertito nella Legge 7 agosto 2012 n. 135, art. 1 commi 7 e 13, il contratto potrà essere recesso nell'immediato senza che la ditta possa vantare alcuna rivalsa nei confronti dell'Amministrazione Comunale nel caso di intervenuta disponibilità di convenzioni Consip e/o delle centrali di committenza regionali che prevedano condizioni di maggior vantaggio economico.

Art. 9 Passaggio di funzionari pubblici a ditte private

Ai sensi dell'articolo 53, comma 16-ter, del Decreto Legislativo n. 165 del 2001 si evidenzia che "i dipendenti pubblici che, negli ultimi tre anni di servizio, hanno esercitato poteri autoritativi o negoziali per conto delle pubbliche amministrazioni di cui all'articolo 1, comma 2, non possono svolgere, nei tre anni successivi alla cessazione del rapporto di pubblico impiego, attività lavorativa o professionale presso i soggetti privati destinatari dell'attività della pubblica amministrazione svolta attraverso i medesimi poteri.

Pertanto "i contratti conclusi e gli incarichi conferiti in violazione di quanto previsto dal presente comma sono nulli ed è fatto divieto ai soggetti privati che li hanno conclusi o conferiti di contrattare con le pubbliche amministrazioni per i successivi tre anni con obbligo di restituzione dei compensi eventualmente percepiti e accertati ad essi riferiti.

Inoltre, ai fini applicativi della suddetta norma, l'articolo 21 del Decreto Legislativo n. 39 del 2013 precisa che "...sono considerati dipendenti delle pubbliche amministrazioni anche i soggetti titolari di uno degli incarichi di cui al presente decreto, ivi compresi i soggetti esterni con i quali l'amministrazione, l'ente pubblico o l'ente di diritto privato in controllo pubblico stabilisce un rapporto di lavoro, subordinato o autonomo. Tali divieti si applicano a far data dalla cessazione dell'incarico."

Art. 10 Variazioni della ragione sociale

La/e ditta/e aggiudicataria/e dovrà/nno comunicare all'Amministrazione qualsiasi variazione intervenuta nella denominazione o ragione sociale dell'impresa indicando il motivo della variazione (cessione dell'azienda, fusione, trasformazione ecc..).

L'Amministrazione non si assume alcuna responsabilità per il ritardo nei pagamenti dovuto a ritardo della comunicazione stessa.

Art. 11 Trattamento dei dati

1. Premessa

Ai sensi dell'art. 13 del Regolamento europeo n. 679/2016, Il Comune di Reggio Emilia, in qualità di Titolare del trattamento dei dati personali, è tenuto a fornirle informazioni in merito all'utilizzo dei suoi dati personali.

2. Titolare del trattamento dei dati personali

Il Titolare del trattamento dei dati personali di cui alla presente informativa è il Comune di Reggio Emilia, con sede a Reggio Emilia, Piazza Prampolini n°1, cap 42121, Tel. 0522/456111, indirizzo mail: **privacy@comune.re.it**, indirizzo pec: **comune.reggioemilia@pec.municipio.re.it**.

3. Responsabile della protezione dei dati personali

Il Responsabile della protezione dei dati personali del Comune di Reggio Emilia ha sede a Reggio Emilia, Piazza Prampolini n°1, cap 42121, Tel. 0522/456111, indirizzo mail: **dpo@comune.re.it**.

4. Responsabili del trattamento

Il Comune di Reggio Emilia può avvalersi di soggetti terzi per l'espletamento di attività e relativi trattamenti di dati personali di cui è Titolare nominandoli Responsabili del trattamento. Conformemente a quanto stabilito dall'art. 28 del Regolamento europeo 679/2016 con tali soggetti il Comune sottoscrive contratti che vincolano il Responsabile al Titolare per le attività inerenti il trattamento dei dati personali. Per il trattamento in oggetto il Comune di Reggio Emilia non ha nominato Responsabili del trattamento.

5. Soggetti autorizzati al trattamento

I Suoi dati personali sono trattati da personale del Comune di Reggio Emilia previamente autorizzato e designato quale incaricato del trattamento, a cui sono impartite idonee istruzioni in ordine alle finalità e alle modalità di trattamento dei dati in base alla vigente normativa in materia di protezione dei dati personali.

6. Finalità del trattamento

I Suoi dati personali sono trattati per le finalità di affidamento di contratti pubblici di forniture, servizi, lavori e concessioni ai sensi del D.Lgs. 50/2016 e s.m. e i. e per la tracciabilità dei flussi finanziari ai sensi dell'art. 3 co. 5 della L. 136/2010 e s.m. e i.

7. Base giuridica del trattamento

Il trattamento dei Suoi dati personali viene effettuato dal Comune di Reggio Emilia per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, pertanto, ai sensi dell'art. 6 comma 1 lett. e) del Regolamento europeo 679/2016 non necessita del Suo consenso.

I Suoi dati personali sono trattati dal Comune di Reggio Emilia esclusivamente per le finalità che rientrano nei compiti istituzionali dell'Amministrazione e per adempiere ad eventuali obblighi di legge, regolamentari o contrattuali.

Il trattamento dei Suoi dati personali avviene ai sensi del D.Lgs. 50/2016 e s.m. e i. e della L. 136/2010 art. 3 co. 5 e s.m. e i.

8. Destinatari dei dati personali

I suoi dati personali non sono oggetto di diffusione.

9. Trasferimento dei dati personali a Paesi extra UE

I suoi dati personali non sono trasferiti al di fuori dell'Unione europea, salvo i casi previsti da specifici obblighi normativi.

10. Periodo di conservazione

I suoi dati sono conservati per un periodo non superiore a quello necessario per il perseguimento delle finalità sopra menzionate. A tal fine, anche mediante controlli periodici, viene verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati

P.zza Scapinelli, 2 - 42121 Reggio Emilia

rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che Lei fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili, vengono cancellati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

11. I suoi diritti

Nella sua qualità di interessato, Lei ha diritto:

- di accesso ai dati personali;
- di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano;
- di opporsi al trattamento;
- di proporre reclamo al Garante per la protezione dei dati personali

Per l'esercizio dei diritti di cui sopra l'interessato può contattare:

- **Il Titolare del trattamento** dei dati Comune di Reggio Emilia, con sede a Reggio Emilia, Piazza Prampolini n°1, cap 42121, Tel. 0522/456111, mail: privacy@comune.re.it , pec: comune.reggioemilia@pec.municipio.re.it

- **Il Responsabile della protezione dei dati personali del Comune di Reggio Emilia** con sede a Reggio Emilia, Piazza Prampolini n°1, cap 42121, indirizzo mail: dpo@comune.re.it

12. Conferimento dei dati

Il conferimento dei Suoi dati è facoltativo, ma necessario per le finalità indicate al punto 6. Il mancato conferimento comporterà l'impossibilità di affidamento di forniture, servizi, lavori e concessioni .

Art. 12 Sicurezza e riservatezza

4. Il fornitore ha l'obbligo di mantenere riservati i dati e le informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione dati, di cui venga in possesso e comunque a conoscenza, anche tramite l'esecuzione del contratto, di non divulgarli in alcun modo e in qualsiasi forma, di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione del Contratto e di non farne oggetto di comunicazione o trasmissione senza l'espressa autorizzazione dell'Amministrazione.
5. L'obbligo di cui al precedente comma sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione del Contratto.
6. L'obbligo di cui ai commi 1 e 2 non concerne i dati che siano o divengano di pubblico dominio.
7. Il fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti, consulenti e collaboratori, nonché di subappaltatori e dei dipendenti, consulenti e collaboratori di questi ultimi, degli obblighi di segretezza di cui ai punti 1, 2 e 3 e risponde nei confronti della Committente per eventuali violazioni dell'obbligo di riservatezza commesse dai suddetti soggetti.
8. Il fornitore può utilizzare servizi di cloud pubblici ove memorizzare i dati e le informazioni trattate nell'espletamento dell'incarico affidato, solo previa autorizzazione dell'Ente.
9. In caso di inosservanza degli obblighi descritti nei punti da 1 a 5, l'Amministrazione ha facoltà di dichiarare risolto di diritto il Contratto, fermo restando che il fornitore/incaricato/contraente sarà tenuto a risarcire tutti i danni che ne dovessero derivare.
10. Il fornitore potrà citare i termini essenziali del Contratto nei casi in cui fosse condizione necessaria per la partecipazione del fornitore stesso a gare e appalti, previa comunicazione alla Amministrazione delle modalità e dei contenuti di detta citazione.

P.zza Scapinelli, 2 - 42121 Reggio Emilia

11. Sarà possibile ogni operazione di auditing da parte della Amministrazione attinente le procedure adottate dal fornitore/incaricato/contraente in materia di riservatezza e degli altri obblighi assunti dal presente contratto.
12. Il fornitore non potrà conservare copia di dati e programmi della Amministrazione, né alcuna documentazione inerente ad essi dopo la scadenza del Contratto e dovrà, su richiesta, ritrasmetterli all'Amministrazione.
13. Le parti prestano il proprio reciproco consenso al trattamento dei propri dati personali all'esclusivo fine della gestione amministrativa e contabile del presente contratto con facoltà, solo ove necessario per tali adempimenti, di fornirli anche a terzi e comunque in ottemperanza degli obblighi previsti dal Regolamento UE 2016/679.

Art. 13 Wistleblowing dipendenti/appaltatori/concessionari/gestori di servizio

Dal dicembre 2018 il Comune di Reggio Emilia ha attivato la piattaforma informatica dedicata al "whistleblowing" che permette ai dipendenti, agli appaltatori, ai concessionari di segnalare, con garanzia di riservatezza, illeciti, abusi, illegalità o irregolarità lesivi dell'interesse pubblico.

L'Appaltatore/Il Concessionario/Il Gestore di Servizio, partecipando alla trattativa indetta dal Comune di Reggio Emilia, prende atto dell'attivazione da parte dell'Ente del sistema suddetto, comunicando ai propri dipendenti/collaboratori interessati, tramite e-mail dedicata, la possibilità di accesso al sistema di whistleblowing del Comune di Reggio Emilia, ai fini della segnalazione di condotte illecite di cui siano venuti a conoscenza in ragione del rapporto di lavoro (art. 54 bis del D. Lgs. n. 165/2001, commi 1 e 2).

Detta e-mail è inoltrata per conoscenza al Comune di Reggio Emilia.

L'Appaltatore/Il Concessionario/Il Gestore di Servizio si impegna solennemente a non adottare misure ritorsive nei confronti dei segnalanti.

Il software è conforme alla legge n. 179/2017 nonché alle LINEE GUIDA ANAC, Determinazione n. 6 del 2015 e al Comunicato del Presidente ANAC del 5 settembre 2018. Il software, infatti, con modalità strettamente aderenti alla norma, separa la segnalazione dall'identità del segnalante. L'accesso all'identità del segnalante è concessa esclusivamente al Responsabile della Prevenzione della Corruzione tramite stringente procedura di sicurezza, che registra l'accesso all'identità, con richiesta della specifica motivazione. Dal punto di vista informatico è garantita l'assoluta inviolabilità dei sistemi e la massima riservatezza. Il Responsabile Anticorruzione è l'unico utente in grado di ricevere le segnalazioni attraverso la console di amministrazione del software, mantenendole riservate nel rispetto del quadro normativo.

Di seguito il percorso per accedere alla piattaforma attivata dal Comune di Reggio Emilia, messo a disposizione anche dei dipendenti delle imprese fornitrici.

www.comune.re.it - Il Comune > Amministrazione trasparente > Altri contenuti > Prevenzione della corruzione > Piano triennale di prevenzione della corruzione > whistleblowing.

Nella medesima sezione sono disponibili il manuale operativo per le modalità di segnalazione e i relativi moduli.

Art. 14 Controversie

Per la definizione di tutte le controversie tra l'Amministrazione Comunale e la/e ditta/e aggiudicataria/e che possono insorgere in relazione al presente rapporto contrattuale,



Area Risorse
Servizio Gestione e Sviluppo delle Tecnologie e dei
Sistemi informativi

P.zza Scapinelli, 2 - 42121 Reggio Emilia

comprese quelle inerenti la validità del medesimo, la sua interpretazione, esecuzione e risoluzione, sarà competente il Foro di Reggio Emilia.

Art. 15 Rinvio

Per quanto non espressamente previsto dalla presente convenzione, si intendono applicate le disposizioni legislative e regolamentari in vigore al momento dell'affidamento del servizio.

Art. 16 Responsabile del procedimento

Ai sensi dell'art. 31 del D.Lgs 50/2016, il responsabile del procedimento è individuato nella persona del Dirigente Ing. Andrea Bertani.

Il responsabile del procedimento potrà avvalersi di suoi collaboratori per effettuare, in particolare, controlli sulla qualità, sul rispetto di tutta la normativa vigente, ed in particolare, seguire l'esecuzione del servizio, verificando il rispetto delle disposizioni e modalità contrattuali, evidenziare e verbalizzare le disfunzioni, i ritardi e tutte le altre eventuali inadempienze.

IL DIRIGENTE

(Ing. Andrea Bertani)