SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Bologna

Istituto delle Scienze Neurologiche
Istituto di Ricovero e Cura a Carattere Scientifico

Servizio acquisti area vasta
Il Direttore

Acquisizione servizi SAP Analytics Cloud (SAC) finalizzata alla prosecuzione del tenant cloud relativo ai servizi di business intelligence in ambito SAP, per le esigenze dell'Azienda Ospedaliero Universitaria di Ferrara – lotto unico

Capitolato Speciale

DA RESTITUIRE FIRMATO

Sommario

1. Premessa e obiettivi

L'Azienda Ospedaliero Universitaria di Ferrara ha acquisito a suo tempo e in altro contratto il sistema software in licenza d'uso SAP, pertanto con il presente capitolato l'Azienda Sanitaria si pone l'obiettivo di acquisire i servizi SAP Analytics Cloud (SAC) finalizzati alla prosecuzione del tenant cloud relativo ai servizi di business intelligence in ambito SAP.

2. Oggetto

Il presente Capitolato Speciale disciplina il contratto per l'acquisizione di servizi SAP Analytics Cloud (SAC) per l'Azienda Ospedaliero-Universitaria di Ferrara per la prosecuzione del tenant cloud relativo ai servizi di business intelligence in ambito SAP e pertanto sono richiesti i seguenti servizi, con le metriche minime indicate a fianco di ciascuno

Servizio Cloud Di SAP	MetriCa di Utilizzo	Limitazione MetriCa Di Utilizzo
SAP HANA Cloud	1 CapaCity UnitS	19.000
SAP AnalytCloud teSt ten publiC CF	1 USer	50
SAP BuSineSS AppliCation Studio	1 USer	50
SAP AnalytCloud BI publiC CF	1 USer	50

3. Manutenzione e assistenza tecnica e sistemistica

La Ditta dovrà assicurare il corretto funzionamento del sistema nel suo complesso. In caso di malfunzionamenti la Ditta è tenuta al ripristino delle funzionalità rispettando le condizioni e i tempi di intervento previsti e concordati con l'Azienda Sanitaria.

Il fornitore risponde della professionalità dei tecnici incaricati.

Poiché nell'esercizio dei servizi oggetto del presente capitolato il personale del fornitore potrà interagire sia con il personale dell'Azienda Sanitaria ed eventualmente con altre ditte o servizi, tale interazione dovrà essere orientata alla totale efficienza nella risoluzione dei problemi. È richiesta, pertanto, una fattiva e piena collaborazione secondo questo orientamento.
Va ricordato e sottolineato come i destinatari principali dell'erogazione del servizio richiesto siano gli operatori aziendali. Qualsiasi eventuale intervento di assistenza telefonica e/o on-site, pertanto, deve avere in ogni caso l'obiettivo della soluzione completa del problema. Il tecnico della manutenzione, a tal fine, deve sempre accettare la richiesta e attivare il corretto percorso di risoluzione.
Tutti gli interventi di manutenzione programmata e di assistenza per guasti dovranno essere

opportunamente dettagliati con report tecnici sulle attività svolte.

Il servizio di assistenza deve includere tutte le attività di supporto agli operatori, tecnici, sistemisti e utenti aziendali per qualsiasi attività inerente il presente capitolato.

Più in generale, la Ditta dovrà assicurare il corretto funzionamento di quanto fornito nel suo complesso.

Requisiti minimi di erogazione dei servizi

1. Back up almeno giornaliero dell'ambiente
2. Back up completo mensile con tempo di conservazione non inferiore a 2 mesi
3. Servizio di risposta a fronte di incidenti garantito 24 ore al giorno 7 giorni su 7
4. Tempo di risposta entro 2 ore (consecutive) dalla segnalazione per incidenti a priorità alta; entro 4 ore (consecutive) per incidenti a priorità media; entro il giorno lavorativo successivo per incidenti a priorità bassa. (per priorità alta si intende la totale compromissione dell'ambiente; per priorità media si intende un incidente con notevole impatto sui processi aziendali; per priorità bassa si intende un incidente con minimo impatto sull'organizzazione aziendale)
5. Tempo di disponibilità di sistema non inferiore al 95% su base annua
6. Fornitura al cliente di apposita reportistica mensile (in lingua italiana) e di evidenza dei livelli di servizio richiesti

~~(~~Si precisa che i dati e i back up dell'ambiente informatico, devono essere obbligatoriamente conservati presso stati soggetti al GDPR europeo~~)~~.

4. Monitoraggio, gestione del contratto controlli di qualità

Il fornitore, in accordo con le U.O. utilizzatrici del software e/o la Direzione dell'U.O. ICT dell'Azienda Sanitaria, dovrà garantire la sistematica e corretta gestione di tutti gli aspetti contrattuali, anche attraverso la costituzione di un gruppo di progetto misto fornitore/Azienda Sanitaria per evitare/prevenire l'inadempimento contrattuale e monitorare le diverse fasi della fornitura del servizio, con particolare riferimento a:

1. pianificazione delle attività con la stesura di piani di lavoro concordati tra le parti;
2. gestione degli stati di avanzamento delle attività tramite produzione di reportistica con cadenza temporale concordata, soprattutto in relazione alle giornate erogate suddivise per commessa;
3. monitoraggio dei tempi di rilascio delle applicazioni, dei ritardi e degli imprevisti;
4. corretta ed adeguata gestione dei gruppi di lavoro in relazione ed in accordo alle esigenze dell'Azienda Sanitaria.

Al fine di consentire la corretta esecuzione dei controlli di qualità, previsti dai protocolli dell'U.O. ICT dell'Azienda Sanitaria, dovranno essere forniti e resi accessibili alle Direzioni stesse tutti i programmi di elaborazione e le procedure per il controllo delle prestazioni dei sistemi.

5. Referenti e verifiche

L'Azienda Sanitaria, prima dell'inizio del contratto di servizio, comunicherà alla Società il referente aziendale (process owner) per la fornitura del servizio oggetto del presente contratto. La Società dovrà, a sua volta, prima dell'inizio del contratto, comunicare il proprio referente (process owner) nei rapporti contrattuali con l'Azienda Sanitaria.

La Società pertanto:

- si obbliga a consentire all'Azienda Sanitaria, per quanto di propria competenza, di procedere, in qualsiasi momento e anche senza preavviso, alle verifiche della piena e corretta

esecuzione delle prestazioni oggetto del presente contratto, nonché a prestare la propria collaborazione per consentire lo svolgimento di tali verifiche;

- si obbliga a dare immediata comunicazione al responsabile del processo, per quanto di propria competenza, di ogni circostanza che abbia influenza sull'esecuzione delle attività previste dal presente contratto;
- è obbligata, nell'adempimento delle proprie prestazioni ed obbligazioni, ad osservare tutte le indicazioni operative, di indirizzo e di controllo che a tale scopo saranno predisposte e comunicate dall'Azienda Sanitaria, per quanto di competenza;
- è obbligata, nell'adempimento delle proprie prestazioni ed obbligazioni, a comunicare tempestivamente all'Azienda Sanitaria le eventuali variazioni della propria struttura organizzativa coinvolta nell'esecuzione del contratto, indicando analiticamente le variazioni intervenute ed il nominativo del nuovo responsabile di processi. I servizi pertanto dovranno corrispondere a quanto pattuito contrattualmente e con quanto autorizzato e riscontrato dalla Direzione dell'U.O. ICT dell'Azienda Sanitaria; eventuali prestazioni non autorizzate non verranno riconosciute e di conseguenza non saranno pagate.

6. Inadempienze contrattuali e penalità

Ai sensi dell'art. 126 comma 1 del D.lgs 36/2023 e s.m.i., l'entità delle penali legate al ritardo dell'esecuzione delle prestazioni contrattuali sono calcolate in misura giornaliera compresa tra lo 0,5 per mille e l'1,5 per mille dell'ammontare netto contrattuale, da determinare in relazione all'entità delle conseguenze legate al ritardo e non può comunque superare, complessivamente, il 10 per cento del valore del contratto.

Fermo restando quanto previsto dall'articolo 15, la fornitura derivante dal presente Capitolato Speciale sarà monitorata per tutta la sua durata. La ditta aggiudicataria sarà, pertanto, sottoposta ad un processo di valutazione che potrà portare, di volta in volta, all'applicazione di penali direttamente conseguenti da comportamenti difformi rispetto agli obblighi contrattuali.

Pertanto qualora venissero riscontrate inadempienze rispetto ai livelli di servizio richiesti nel presente Capitolato, la Committenza, si riserva l'applicazione delle penali di seguito descritte
In caso di mancato rispetto di quanto richiesto e qui descritto, ferme restando eventuali implicazioni di carattere civile o penale e la richiesta dei danni, saranno applicate le penali riportate nei punti seguenti:

- 0,15 per mille del valore del contratto per ogni ora lavorativa di ritardo nell'esecuzione delle prestazioni indicate all'art. 4;
- 0,5 per mille del valore del contratto per ogni giorno di ritardo nell'esecuzione delle prestazioni indicate all'art. 4
- 0,5 per mille del valore del contratto per l'impiego (sia per gli interventi on-site che da remoto) di personale non qualificato
- 0,5 per mille del valore del contratto per qualsiasi attività causa di malfunzionamenti tali da provocare disagio grave a una o più unità funzionali. In questo caso la penale si applica per tutto il periodo di durata del disagio indipendentemente dalla durata dell'inadempienza.
- 0,5 per mille del valore del contratto per ogni giornata di ritardo oltre i 10 giorni lavorativi per inviare l'offerta con l'indicazione del numero di giornare di sviluppo e/o manutenzione software necessarie
- 0,5 per mille del valore del contratto per ogni giornata di assitenza di ritardo oltre i 5 giorni lavorativi alla data di accettazione dell'offerta da parte dell'ente
- 0,5 per mille del valore del contratto per ogni giornata di ritardo oltre le 20 giornate lavorative per la restituzione dell'offerta, dalla data della richiesta dell'ente, nel caso di richieste particolarmente articolate e complesse

In caso di segnalazioni di inadempimenti nella fornitura, i referenti aziendali o un loro incaricato

daranno comunicazione scritta alla Ditta tramite Pec di quanto emerso; la Ditta avrà 5 giorni solari di tempo dal ricevimento della predetta comunicazione, per presentare le proprie controdeduzioni scritte.
Nel caso in cui il Fornitore non risponda o non dimostri che l'inadempimento non è ad esso imputabile, l'Azienda Sanitaria provvederà ad applicare le penali di cui al punto precedente, senza che la Ditta possa sollevare alcuna obiezione. Delle penali applicate sarà data comunicazione alla Ditta a mezzo posta elettronica certificata.
Per ogni inadempienza relativa al mancato rispetto di quanto contenuto nella documentazione relativa alla nomina responsabile trattamento dati (vedi istruzioni operative) comporterà l'applicazione di una penale pari a € 500,00.
Nel caso in cui all'esito degli audit effettuati dal Titolare del trattamento o da terzi incaricati, le misure tecniche, organizzative e/o di sicurezza adottate dal Responsabile del trattamento e/o Sub-responsabile del trattamento risultino inadeguate o, comunque, vengano riscontrate evidenze di violazioni gravi commesse dal Responsabile del trattamento o Sub-responsabile del trattamento dei dati personali, sarà applicata una penale di € 500,00.

In caso di mancato rispetto del Protocollo di Legalità del 19.06.2018 con la Prefettura di Ferrara (clausola 5): penale nella misura del 10% del valore del contratto ovvero, qualora lo stesso non sia determinato o determinabile, una penale pari al valore delle prestazioni al momento eseguite; le già menzionate penali saranno applicate mediante automatica detrazione, da parte della stazione appaltante, del relativo importo dalle somme dovute all'impresa in relazione alle prestazioni eseguite.

Qualsiasi difformità ed inadempienza a quanto descritto e richiesto al punto "9. *Cybersecurity*", ferme restando eventuali implicazioni di carattere civile o penale, daranno luogo all'applicazione di una penale pari a **€ 1.050,00** per ogni giorno consecutivo (solare) del protrarsi della difformità/inadempienza

In caso di segnalazioni di inadempimenti nella fornitura del servizio, i referenti aziendali o un loro incaricato daranno comunicazione scritta alla Ditta tramite Pec di quanto emerso; la Ditta avrà 5 giorni solari di tempo dal ricevimento della predetta comunicazione, per presentare le proprie controdeduzioni scritte.
Nel caso in cui il Fornitore non risponda o non dimostri che l'inadempimento non è a esso imputabile, l'Istituto provvederà ad applicare le penali di cui al punto precedente, senza che la Ditta possa sollevare alcuna obiezione. Delle penali applicate sarà data comunicazione alla Ditta a mezzo posta elettronica certificata.

L'applicazione delle penali avverrà in modo automatico, previa comunicazione formale, attraverso l'incameramento del deposito cauzionale e/o attraverso l'emissione da parte dell'ufficio amministrativo competente dell' Azienda Sanitaria, di una nota d'addebito, ai sensidell'art.15, comma 1, D.P.R. 633/72.

Le stazioni appaltanti hanno il diritto di valersi della garanzia, nei limiti dell'importo massimo garantito, per l'eventuale maggiore spesa sostenuta per il completamento dei lavori, servizi o forniture nel caso di risoluzione del contratto disposta in danno dell'esecutore. Possono altresì incamerare la garanzia per il pagamento di quanto dovuto dall'esecutore per le inadempienze derivanti dalla inosservanza di norme e prescrizioni dei contratti collettivi, delle leggi e dei regolamenti sulla tutela, protezione, assicurazione, assistenza e sicurezza fisica dei lavoratori addetti all'esecuzione dell'appalto.

7. Misure di sicurezza e normativa sul trattamento dei dati personali

Il sistema/servizi offerto/i dovrà essere conforme alla vigente normativa in materia di protezione

dei dati personali (Regolamento EU 2016/679) ed in particolare ai principi di privacy by default e privacy by design.
Per sanare le eventuali non rispondenze a quanto previsto (per i software progettati ed implementati prima dell'entrata in vigore del sopracitato regolamento) il fornitore dovrà indicare un piano di adeguamento e concordare con l'Azienda eventuali soluzioni tecniche e/o organizzative per eliminare o ridurre i rischi.

Il fornitore sarà designato responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento UE n. 679/2016 e D. Lgs.196/2003 come modificato dal D. Lgs. N. 101/2018.
Il sistema offerto dovrà essere costantemente aggiornato e conforme a quanto richiesto dagli adeguamenti normativi di AGID e del GDPR.
L'Azienda effettua delle attività di vulnerability assessment al fine di verificare la sicurezza dei propri sistemi, il fornitore si impegna ad effettuare un'analisi congiunta degli esiti entro 2 settimane da scansione e a pianificare le eventuali attività per la messa in sicurezza dei sistemi di propria competenza (2 settimane per update o vulnerabilità molto gravi, 6 mesi per upgrade o vulnerabilità basse/medie).
Qualora il software oggetto di contratto sia classificato come Medical Device dovranno essere rispettate le relative normative del settore anche in relazione ai test da effettuare a valle degli interventi a garanzia della conservazione della certificazione nel tempo.

Il dettaglio dei tipi di dati trattati e delle operazioni consentite, le politiche di gestione della sicurezza, i meccanismi di gestione degli utenti, il sistema di gestione delle autorizzazioni devono essere chiaramente comunicate al servizio competente dell'Azienda Ospedaliero Universitaria di Ferrara a inizio contratto.

Inoltre, è richiesto al fornitore di dare evidenza delle procedure adottate al proprio interno per la gestione della sicurezza, con particolare riferimento alle indicazioni di cui al GDPR.

8. Obblighi di riservatezza

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'Azienda.

L'obbligo di cui sopra sussiste, altresì, relativamente a tutto il materiale originario o predisposto in esecuzione del Contratto. Tali obblighi non concernono i dati che siano o divengano di pubblico dominio.

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 sopra e risponde nei confronti dell'Azienda per eventuali violazioni dell'obbligo di riservatezza commesse dai suddetti soggetti.

In caso di inosservanza degli obblighi descritti l'Azienda ha facoltà di dichiarare risolto di diritto il Contratto, fermo restando che il Fornitore sarà tenuto a risarcire tutti i danni che ne dovessero derivare.

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'Azienda.

Sarà possibile ogni operazione di auditing da parte dell'Azienda attinente alle procedure adottate dal Contraente in materia di riservatezza e degli altri obblighi assunti dal presente contratto.

Il Fornitore non potrà conservare copia di dati e programmi dell'Azienda, né alcuna documentazione inerente ad essi dopo la scadenza del Contratto e dovrà, su richiesta, ritrasmetterli all'Azienda.
Il Fornitore s'impegna, altresì, a rispettare quanto previsto dal regolamento UE 2016/679 e dal D.Lgs. n.51/2018. Il fornitore, in relazione a quanto oggetto di prestazione e alle informazioni e documenti dei quali sia venuto in possesso, a qualsiasi titolo, nell'esecuzione delle prestazioni oggetto del presente appalto, si impegna, fatto salvo in ogni caso il diritto al risarcimento dei danni subiti dall'interessato, ad attuare nell'ambito della propria struttura e di quella degli eventuali collaboratori, sotto la propria responsabilità, ai sensi del regolamento UE 2016/679, tutte quelle misure e norme di sicurezza e di controllo atte ad evitare il rischio di alterazione, distruzione o perdita, anche parziale, nonché d'accesso non autorizzato, o di trattamento non consentito, o non conforme alle finalità del presente contratto.

Con la stipula del contratto di appalto, la ditta, ai sensi dell'art. 28 del regolamento, è nominata Responsabile del trattamento dei dati, per gli adempimenti previsti nel contratto di appalto e nei limiti e per la durata dello stesso. La nomina di Responsabile è valida per tutta la durata del contratto d'appalto e si considererà revocata a completamento dell'incarico.

Con riferimento all'attività di trattamento dei dati personali cui concorre la Ditta, la stessa assicura massima cooperazione e assistenza al fine di consentire la redazione da parte del Titolare della eventuale DPIA e, in ogni caso, garantisce l'applicazione delle azioni di mitigazione previste nella DPIA o comunque ritenute idonee dall'Azienda.

La Ditta dovrà garantire all'Azienda, tenuto conto dello stato della tecnica, dei costi, della natura, dell'ambito e della finalità del relativo trattamento, l'adozione, sia nella fase iniziale di determinazione dei mezzi di trattamento, che durante il trattamento stesso, di ogni misura tecnica ed organizzativa che riterrà opportuna per garantire ed attuare i principi previsti in materia di protezione dati e a tutelare i diritti degli interessati.

In linea con i principi di privacy by default, dovranno essere trattati, per impostazione predefinita, esclusivamente quei dati personali necessari per ogni specifica finalità del trattamento, e che in particolare non siano accessibili dati personali ad un numero indefinito di soggetti senza l'intervento di una persona fisica.

La Ditta assicura, altresì, la tenuta di apposito registro dei trattamenti che, su richiesta, viene messo a disposizione dell'Azienda e/o dell'Autorità di controllo.

Le Parti riconoscono e convengono che il rispetto delle istruzioni di cui all'atto di nomina, nonché alle prescrizioni della normativa applicabile, non producono l'insorgere di un diritto in capo al Responsabile del trattamento al rimborso delle eventuali spese che lo stesso potrebbe dover sostenere per conformarsi.

9. CyberSecurity

Qualsiasi apparato hw e sw (PC, workstation, server, etc.) collegato alla rete aziendale dovrà conformarsi alle politiche aziendali in tema di cybersecurity.

9.1 Misure di protezione dai malware

Stante la costante minaccia a cui sono costantemente sottoposti tutti i sistemi informatici è necessario per il fornitore adottare tutte le misure necessarie di protezione dai malware.
A pena di esclusione, quindi, il fornitore dovrà descrivere tutte le misure adottate per la protezione di quanto oggetto di fornitura dai malware specificando quali sistemi verranno protetti e mediante quali modalità tecniche.
Quanto fornito a protezione dei malware sarà oggetto di valutazione qualitativa da parte

del servizio competente dell'Azienda Sanitaria.

9.2 Accesso agli ambienti del Titolare

All'atto della stipula contrattuale verranno stabilite le credenziali della persona di riferimento che sarà l'unico a poter richiedere variazioni sulle utenze di accesso al sistema informatico dell'AOU di Ferrara.

In ragione annuale, verrà chiesto alla persona di riferimento un aggiornamento sulle credenziali attive, in funzione del quale verranno successivamente eliminate eventuali utenze che risultassero non più necessarie

Il Fornitore potrà accedere alle reti, ai sistemi e agli ambienti che il Titolare metterà a disposizione, relativamente al proprio ambito di competenza, attraverso le modalità di connessione definite.

L'infrastruttura utilizzata dovrà rispettare i requisiti minimi definiti e descritti nel seguito.

Si sottolinea che, ancorché salvaguardate le problematiche di protezione dei dati personali, il Fornitore dovrà tener conto del rischio di furto, perdita accidentale e/o distruzione di patrimonio informativo, inteso come le basi dati, il codice sorgente e/o le soluzioni prodotte, le infrastrutture e le personalizzazioni sviluppate nonché le informazioni e i dati trattati, per quanto di sua competenza.

Nel caso di accesso a reti, sistemi e ambienti del Titolare, il Fornitore dovrà:

- Richiedere in forma scritta la creazione di una nuova utenza che dovrà contenere l'identificativo della persona a cui verrà assegnata, l'ambito di utilizzo, il ruolo, l'ambiente e la durata. Le utenze richieste dovranno essere univoche, personali e utilizzate in modo che l'accesso alle informazioni da parte di ogni singolo utente sia limitato alle sole (principio del "minimo privilegio") informazioni di cui necessita (principio del "need-to-know") per lo svolgimento dei propri compiti;
- Inviare una tempestiva comunicazione in caso di variazione delle mansioni o delle attività in modo che il profilo venga adeguato alle effettive nuove esigenze; effettuare una revisione periodica delle utenze al fine di individuare le utenze inattive e quelle che necessitano di una modifica;
- Richiedere immediatamente la disabilitazione di un'utenza assegnata ad un suo dipendente o collaboratore nei seguenti casi:
    - Interruzione del rapporto di lavoro con il Fornitore;
    - Cambio di mansione che non necessita dell'accesso ai sistemi informatici /applicazioni del Titolare;
    - Utenze inattive emerse nella revisione periodica.

Tutto il personale autorizzato del Fornitore dovrà:

- Eseguire l'accesso ai sistemi e agli ambienti tramite le proprie credenziali di accesso personali (ad esempio user ID, password) e con gli strumenti forniti dal Titolare;
- Custodire ed utilizzare le proprie credenziali di accesso con la massima cautela al fine di evitare l'intercettazione, volontaria o fortuita, delle stesse da parte di terzi evitando in ogni caso di comunicarle ad altri e non consentendo a nessun'altra persona di utilizzarle.

Il Fornitore dovrà garantire sugli ambienti del Titolare da esso gestiti che l'accesso alle informazioni, servizi e sistemi avvenga in modo sicuro per prevenire l'accesso da parte di utenti che non hanno i necessari diritti e pertanto impedire trattamenti non autorizzati.

9.3 Modalità e specifiche di connessione

Il fornitore, qualora occorra, per specifiche esigenze, potrà usufruire di una connessione

remota (dove per remota è da intendersi eseguita da sedi non del Titolare) ai sistemi del Titolare. Questa sarà possibile, previe le opportune e necessarie autorizzazioni, solo attraverso: connessioni dedicate conformi alle politiche aziendali.
La connettività VPN-Client, che dovrà essere nominale, è autorizzata solo in casi eccezionali e corredata da opportuna motivazione scritta.
La connettività Internet e l'apparato remoto lato Fornitore saranno a suo carico.
Il Titolare fornirà le specifiche di configurazione, a cui la connettività VPN deve rispondere, che dovranno essere applicate dal Fornitore.
Il fornitore dovrà accettare le modalità di accesso dall'esterno previste e comunicate dall'Azienda senza nulla opporre e senza che questo possa pregiudicare le forniture e i servizi previsti o possa andare a discapito di prestazioni, sia in termini quantitativi che in termini qualitativi. In questo senso, di base, non saranno accettate richieste di connessioni cosiddette lan-to-lan, né di aperture di firewall per fini di accesso, compresi i forward dall'interno verso l'esterno.

9.4 Misure di sicurezza fornitore

Nel seguito sono indicate le misure minime relative alla CyberSecurity che il fornitore deve soddisfare. Tali misure devono intendersi come requisiti minimi da soddisfare a pena di esclusione.
Il fornitore dovrà dare evidenza del rispetto di tali requisiti al servizio competente dell'Azienda Sanitaria.

Politica di sicurezza
• Il fornitore è tenuto al rispetto delle politiche di sicurezza informatica e privacy in uso presso l'AOU di Ferrara. Qualora il fornitore disponesse di una propria security policy essa deve essere coerente con l'analogo documento della Committente.

Ruoli e responsabilità
• Il fornitore si impegna a non rivelare informazioni che possano pregiudicare la sicurezza dell'AOU di Ferrara.
• Il fornitore deve definire chiaramente i ruoli e le responsabilità in materia di sicurezza.
• I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere comunicati chiaramente durante il processo di selezione o di incarico dei dipendenti e collaboratori da parte del fornitore, mediante gli specifici accordi del caso (es. clausole di riservatezza).
• Il fornitore deve essere conforme al c.d. "Provvedimento Amministratori di Sistema"("Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" - 27 novembre 2008) del Garante per la Protezione dei Dati Personali.
• Il fornitore non deve prestare i propri loghi, le proprie divise, i propri segni distintivi a terzi che potrebbero perpetrare attacchi di social engineering nei confronti dell' AOU di Ferrara.

Gestione incidenti
• Il fornitore deve disporre di una procedura per la risposta agli incidenti informatici.
• Il fornitore deve comunicare tempestivamente ad AOU di Ferrrara eventuali incidenti di sicurezza informatica che lo riguardino e che possano compromettere la fornitura in oggetto.
• In particolar modo egli è tenuto a fornire alla Committente, tramite apposito incident report, i dettagli relativi all'evento e alle successive azioni correttive di contenimento eseguite, mediante canali comunicativi precedentemente concordati.
• In caso di incidente che coinvolga informazioni di proprietà di AOU di Ferrara il fornitore

deve garantire alla Committente, o alle figure da essa ingaggiate, l'accesso ai propri locali e sistemi per la verifica e/o l'accertamento del caso da parte della medesima.

Gestione asset
• Il fornitore deve mantenere un registro, periodicamente aggiornato, delle risorse informatiche (hardware, software, rete) utilizzate per l'elaborazione delle informazioni relative ad AOU di Ferrara.

Controllo accessi logici
• Il fornitore deve rispettare i criteri di creazione, conservazione e gestione delle credenziali di accesso in accordo con le regole definite da AOU di Ferrara.
• Deve essere utilizzato un apposito sistema di controllo degli accessi logici e gli accessi devono avvenire mediante utenza nominale nel rispetto dei principi del "need to know" e del "least privilege". Deve almeno essere utilizzata una combinazione nome utente/password. Le password devono rispettare un adeguato livello di complessità, coerente con quanto indicato in merito nella politica di AOU di Ferrara.
• Il collegamento da remoto alla rete di AOU di Ferrara deve avvenire esclusivamente mediante protocolli cifrati (es. VPN) da utenze univoche autorizzate.
• Protocolli notoriamente obsoleti e non sicuri (es. Telnet) non devono essere utilizzati

Log
• Devono essere presenti adeguati meccanismi di log in relazione alle attività effettuate.
• Devono essere implementati adeguati appositi meccanismi di monitoraggio dei log.
• Le registrazioni devono essere marcate temporalmente e adeguatamente protette da manomissioni e accessi non autorizzati.

Sicurezza della rete
• Ogni comunicazione deve essere adeguatamente protetta mediante l'applicazione di specifici protocolli crittografici non obsoleti.
• Eventuali forniture che comportino l'interfacciamento della rete aziendale verso l'esterno a qualsivoglia titolo e per qualsiasi scopo devono avvenire esclusivamente mediante canali di comunicazione preventivamente concordati con la Committente e da essa validati.
• La rete del fornitore deve essere protetta da appositi strumenti di protezione perimetrale (es. firewall, IDS/IPS) attraverso i quali è possibile intercettare e bloccare il traffico non autorizzato.

Sicurezza delle postazioni di lavoro
• Le postazioni di lavoro utilizzate dal fornitore devono essere dotate di software antimalware aggiornato.
• Le postazioni di lavoro utilizzate dal fornitore devono essere dotate di un sistema operativo non obsoleto e mantenuto dal fornitore stesso.
• Le postazioni di lavoro utilizzate dal fornitore devono essere adeguatamente aggiornate secondo un processo strutturato di patching di eventuali vulnerabilità.
• La dotazione software a bordo della postazione di lavoro deve essere ridotta al minimo indispensabile, compatibilmente con i compiti che devono essere svolti.
• Gli utenti non devono essere in grado di disattivare o aggirare le impostazioni di sicurezza né installare applicazioni non autorizzate (ad esempio, prevedendo che non dispongano di privilegi amministrativi).

Continuità operativa
• Devono essere presenti specifici meccanismi di tutela della continuità operativa affinché sia garantita la disponibilità del dato.
• Deve essere garantita la conservazione sicura delle copie di backup.

Sviluppo sicuro & Hardening

• Il sistema di Test deve essere mantenuto distinto da quello di produzione.
• Devono essere utilizzati appositi strumenti di scansione statica del codice sorgente (Static Application Security Testing) per garantire la sicurezza del codice medesimo sin dalle prime fasi del ciclo di sviluppo, in ottica di "security by design".
• Deve essere evitato il ricorso a linguaggi obsoleti e a librerie/package di supporto allo sviluppo obsolete o comunque affette da vulnerabilità.
• Devono essere effettuate attività di identificazione a priori delle possibili minacce (cd. "threat modelling"). In particolare, devono essere condotte verifiche di ricerca di vulnerabilità note, preliminari alla messa in produzione.
• Il fornitore deve effettuare opportune attività di hardening del proprio prodotto, attraverso operazioni di configurazione specifica che garantiscono la minimizzazione dell'impatto dovuto da possibili vulnerabilità (cd. security by default).

Gestione delle vulnerabilità

• Il fornitore si impegna ad effettuare attività di vulnerability assessment e a garantire la risoluzione delle medesime nei tempi concordati con AOU di Ferrara.
• (solo per forniture a rischio alto) il fornitore si impegna a effettuare o commissionare a proprie spese attività di penetration testing e garantire la risoluzione delle medesime nei tempi concordati con AOU di Ferrara.

Patching

• Il fornitore deve disporre di un processo strutturato per effettuare l'aggiornamento software dell'oggetto di fornitura, attraverso il quale garantisce la tempestiva installazione delle modifiche applicative in accordo con gli SLA definiti.
• Il fornitore deve mantenere traccia delle attività di patching effettuate.
• Il fornitore si impegna anche a garantire l'aggiornamento tecnologico di quanto oggetto di fornitura in maniera tale da non pregiudicare l'aggiornamento di sicurezza dei server e delle infrastrutture in genere fornite dall'Azienda AOU di Ferrara a supporto del presente progetto applicativo.

Elementi preferenziali

Sono considerati elementi preferenziali:
• il rispetto dei principali standard e framework in materia di sviluppo sicuro (es. NIST Secure Software Development Framework) in fase di sviluppo del software.

10. Restrizioni all'esportazione

Il Cliente non può utilizzare i Cloud Service, la Documentazione e altri Materiali Cloud in eventuali stati ove questi non possono essere utilizzati in ragione della normativa sul controllo delle esportazioni e delle sanzioni commerciali in vigore negli Stati Uniti, nella UE, in Germania o eventuali altre norme sul controllo delle esportazioni e sanzioni commerciali applicabili. Il Cliente non deve permettere l'utilizzo dei Cloud Service, della Documentazione e di altri Materiali Cloud a nessun utente finale con il quale sono vietate transazioni ai sensi delle condizioni del Contratto. Maggiori informazioni sull'Osservanza della normativa sul Controllo delle Esportazioni e delle Sanzioni da parte di SAP (SAP's Export Control and Sanctions Compliance) sono reperibili all'indirizzo: https://www.sap.com/about/agreements/export-statements.html.

11. Prezzi e validità del contratto

Il presente contratto ha validità di 3 anni con decorrenza dalla data che verrà indcata nel contratto, con possibilità di rinnovo di uteriori anni 2, i prezzi e le condizioni che risulteranno dall'aggiudicazione resteranno fissi e invariabili per tutta la durata del contratto.

Durante il periodo di rinnovo, i servizi dovranno essere eseguiti alle stesse condizioni tecniche, economiche e modalità previste in sede di gara, senza che per questo l'aggiudicatario possa sollevare eccezione.
Alla scadenza del contratto o dell'eventuale rinnovo, l'Azienda Sanitaria si riserva la facoltà di prorogarne la durata per il tempo strettamente necessario alla conclusione delle procedure necessarie per l'individuazione del nuovo contraente ai sensi dell'art. 120, comma 11 del Codice e comunque per un periodo massimo di 180 giorni. In tal caso il contraente sarà tenuto all'esecuzione delle prestazioni oggetto del contratto agli stessi o più favorevoli prezzi, patti e condizioni.

12. Obblighi in materia di sicurezza e salute sul lavoro

L'AOU di Ferrara, come previsto dall'art 26 c1-lettera b del D.Lgs n. 81/2008 e s.m.i, in un Fascicolo **Informativo**, fornisce alle ditte partecipanti dettagliate informazioni sui rischi specifici esistenti negli ambienti in cui sono destinate ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla propria attività. Il **Fascicolo Informativo** può essere visionato al seguente link: ***https://www.ausl.fe.it/ausl-comunica/bandi-di-gara/fornitori/informazioni-sui-rischi***

Restano immutati gli obblighi a carico delle imprese e dei lavoratori autonomi in merito alla salute e alla sicurezza sul lavoro.

13. Risoluzione del contratto

L'Azienda Sanitaria avrà la facoltà di risolvere "ipso facto et jure" il contratto, mediante semplice dichiarazione stragiudiziale intimata via pec, secondo quanto stabilito all'art.122 del D.Lgs. 36/2023 e nelle seguenti ipotesi:

a) nel caso di mancato adempimento delle prestazioni contrattuali a perfetta regola d'arte, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute negli atti di gara e in essi richiamati, ai sensi dell'art.1456 del Codice civile;
b) in caso di cessazione dell'attività o in caso di procedure concorsuali intraprese a carico dell'aggiudicatario;
c) in caso di subappalto non autorizzato dall'Azienda Sanitaria;
e) qualora l'Azienda Sanitaria notifichi n. due diffide ad adempiere senza che la Ditta ottemperi a quanto intimato;
f) in caso di violazione dell'obbligo di riservatezza;
g) in caso di mancato adempimento agli obblighi previsti per la tracciabilità dei flussi finanziari dell'appalto;
h) in caso di mancata osservanza del Codice di comportamento adottato dalla stazione appaltante con Delibera del Direttore Generale n.166 del 29.05.2018;
i) in caso di violazione degli impegni previsti dal Patto di integrità accettato in sede di partecipazione a gara;
l) in caso di mancato rispetto del Protocollo di Legalità
m) in caso di rifiuto del Responsabile del trattamento e Sub-responsabile di consentire l'audit al Titolare del Trattamento

In caso di risoluzione del contratto l'Azienda Sanitaria applicherà quanto previsto all'art.124 del D.Lgs. 36/2023.
L'azienda sanitaria ha il diritto di valersi della garanzia, nei limiti dell'importo massimo garantito, per l'eventuale maggiore spesa sostenuta per il completamento dei lavori, servizi o forniture nel caso di risoluzione del contratto disposta in danno dell'esecutore. Possono altresì incamerare la garanzia per il pagamento di quanto dovuto dall'esecutore per le inadempienze derivanti dalla

inosservanza di norme e prescrizioni dei contratti collettivi, delle leggi e dei regolamenti sulla tutela, protezione, assicurazione, assistenza e sicurezza fisica dei lavoratori addetti all'esecuzione dell'appalto.

14. Responsabilità

L'Azienda Sanitaria è esonerata da ogni responsabilità per danni, infortuni o altro che dovesse accadere al personale della Ditta aggiudicataria nell'esecuzione del contratto, convenendosi a tale riguardo che qualsiasi eventuale onere è già compensato e compreso nel corrispettivo del contratto stesso.

La Ditta aggiudicataria risponde pienamente per danni a persone e/o cose che potessero derivare dall'espletamento delle prestazioni contrattuali e imputabili a essa e ai suoi dipendenti e dei quali danni fosse chiamata a rispondere l'Azienda Sanitaria che fin da ora s'intende sollevata ed indenne da ogni pretesa o molestia.

L'aggiudicatario è responsabile della perfetta esecuzione del servizio a lui affidata e degli oneri che dovessero eventualmente essere sopportati dall'Azienda Sanitaria inconseguenza dell'inosservanza di obblighi facenti carico a lui o al personale da esso dipendente.

15. Fatturazione, Pagamento, Ordini e documenti di trasporto

Ai sensi di quanto previsto dall'art.1, commi da 209 a 213 della Legge 24/12/2007 n. 244, e successive modificazioni, e dal Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche di cui al Decreto del Ministero dell'Economia e delle Finanze 3 aprile 2013, n. 55, le fatture devono essere trasmesse all'Azienda Sanitaria esclusivamente in formato elettronico, attraverso il Sistema Di Interscambio (SDI).

L'obbligo di fatturazione elettronica ricade nei confronti dei soggetti italiani titolari di Partita IVA. Sono pertanto esclusi dall'applicazione tutti i fornitori privi di Partita IVA e i fornitori esteri.
Il Fornitore si obbliga a fatturare secondo le modalità previste dalla normativa, anche se secondaria, vigente in materia, nonché dal presente contratto.

La manutenzione verrà fatturata su base trimestrale posticipata.

I pagamenti saranno effettuati entro il termine di legge decorrente dalla data di ricevimento della fattura elettronica (tramite SDI) qualora l'Azienda Sanitaria Contraente abbia riscontrato la regolarità della stessa, e sussistano i presupposti e le condizioni per la sua liquidazione (acquisizione completa della documentazione necessaria a comprovare il diritto del creditore, tra cui i documenti di trasporto, riscontro della regolarità della fornitura o della prestazione, rispondenza della fattura ai requisiti quantitativi e qualitativi ordinati e consegnati, ai termini ed alle condizioni pattuite contrattualmente).

Qualora le fatture emesse non siano regolari e/o conformi a quanto sopra indicato e non sia quindi possibile procedere alla liquidazione, e sempre che non siano state già rifiutate (tramite SDI) nei casi e nei modi previsti dalla normativa di settore, l'Azienda Sanitaria Contraente sospenderà la liquidazione della fattura fino alla avvenuta regolarizzazione e procederà a formalizzare al Fornitore una formale contestazione da inviare tramite pec contenente le relative motivazioni ed eventuale richiesta di emissione di nota di credito parziale o totale. La contestazione vale come sospensione dei termini di pagamento della fattura.

Il Fornitore dovrà provvedere a regolarizzare la fattura e/o a trasmettere la documentazione richiesta e/o a emettere la nota di credito richiesta entro 10 giorni dal ricevimento della contestazione.

Decorso il termine dei 10 giorni senza alcun riscontro o senza che la posizione sia stata regolarizzata, la stazione appaltante applicherà una penale per ogni giorno di sospensione pari allo 3 per mille, così come previsto dall'articolo 126 del Codice degli Appalti. La stazione appaltante provvederà al pagamento della fattura per la parte eventualmente liquidabile, mentre per quanto non regolarizzato la liquidazione della fattura resterà sospesa; in ogni caso non sono dovuti interessi di qualsiasi natura, né costi di recupero.

In caso di contestazione della fattura i termini di pagamento decorreranno dal ricevimento della documentazione richiesta e/o della nota di credito e/o della fattura correttamente emessa in sostituzione di quella integralmente contestata (o rifiutata). In ogni caso sulle fatture contestate e/o la cui liquidazione è sospesa (per qualsiasi ragione) e/o rifiutata, non sono dovuti interessi di qualsiasi natura, né costi di recupero.

In nessun caso sono dovuti interessi anatocistici.

L'importo forfettario di €40 di cui all'art.6 D.Lgs 231/2002, potrà essere riconosciuto, nei casi e alle condizioni ivi previste, per i crediti scaduti ceduti e/o non ceduti, per contratto di cessione ovvero, in caso di effettivo svolgimento di attività di recupero, per sollecito di pagamento e/o con riferimento alla somma complessivamente ingiunta e/o azionata (e alla pluralità delle fatture azionate). Mentre nulla potrà essere riconosciuto in caso di cessioni di crediti futuri (non ancora sorti al momento della cessione). In ogni caso l'importo forfettario di €40 non sarà dovuto (e non sarà esigibile) con riferimento a ogni singola fattura e sono esclusi automatismi risarcitori**.**

Di seguito si riportano i dati essenziali per la trasmissione delle fatture:

Azienda Ospedaliero-Universitaria di Ferrara:
I.P.A. (indice delle Pubbliche Amministrazioni): AOU_FE
codice univoco ufficio (per ricevimento fatture): BFBVJ7

Gli originali delle fatture dovranno essere così intestati:
AZIENDA OSPEDALIERO-UNIVERSITARIA DI FERRARA
Codice fiscale: 01295950388
P.IVA: IT01295950388
Sede Legale: Via Aldo Moro 8 Cona (Ferrara) - 44124 Ferrara (FE)
Le fatture dovranno, inoltre, contenere **tassativamente** gli importanti seguenti elementi:

- indicazione dettagliata della merce consegnata/servizio prestato
- indicazione della determina dell'Ente appaltante che ha dato luogo all'ordine
- indicazione del numero dell'ordine aziendale informatizzato

Inoltre, ai sensi della Legge 23 dicembre 2014, n.190 (legge di stabilità per il 2015), le Aziende Sanitarie rientrano fra le Pubbliche Amministrazioni tenute ad applicare lo Split Payment IVA; pertanto, il pagamento delle fatture per la cessione di beni e le prestazioni di servizi dei fornitori sarà effettuato separando i pagamenti, ossia versando l'imponibile al fornitore e l'IVA (ancorché regolarmente esposta in fattura) direttamente all'Erario.

A tale scopo dovrà essere riportata in fattura la dicitura seguente "Scissione dei pagamenti – art.17 TER DPR 633/72 (Decreto MEF 23/01/2015).

L'applicazione dello split payment non si applica ai fornitori esteri.

Il mancato rispetto delle disposizioni sopra esplicitate non consentirà il pagamento delle fatture.

L'Azienda Sanitaria procederà ai pagamenti delle fatture secondo le normative vigenti in materia.

La Ditta aggiudicataria avrà l'obbligo di assicurare lo svolgimento del servizio anche in caso di ritardato pagamento.

La ditta rinuncia a far valere, nei casi previsti dal presente articolo, qualsiasi eccezione d'inadempimento di cui all'art.1460 del Codice civile. Ogni caso di arbitraria interruzione delle prestazioni contrattuali sarà ritenuto contrario alla buona fede e la ditta sarà considerata diretta responsabile di eventuali danni causati all'Azienda Sanitaria e dipendenti da tale interruzione. Tale divieto nasce dalla necessità e dall'importanza di garantire il buon andamento dell'Ente Pubblico, nonché di tutelare gli interessi collettivi dei quali l'AOU è portatrice.

I corrispettivi saranno pagati con le modalità previste dal presente capitolato e saranno subordinati:

- alla regolarità contributiva della ditta (qualora la ditta aggiudicataria risultasse debitrice il pagamento delle fatture sarà in ogni caso subordinato alla regolarizzazione del debito stesso; è fatto salvo, in caso di mancata regolarizzazione dei debiti verso l'INPS il diritto dell'Istituto di trattenere dalle somme dovute alla ditta appaltatrice gli importi di contributi omessi e relativi accessori);
- alla verifica di cui all'articolo 48 bis del DPR 602/73.

La Ditta aggiudicataria, ai sensi dell'art.3, della Legge 136 del 13/08/2010 e s.m., assume l'obbligo di tracciabilità dei flussi finanziari.

In base alle disposizioni della legge regionale n.11/2004 e s.m.i. e dei successivi atti attuativi, l'Azienda Sanitaria di cui alla presente gara deve emettere, dal 30 giugno 2016, gli ordini esclusivamente in forma elettronica. Inoltre, da tale data il fornitore deve garantire l'invio dei documenti di trasporto elettronici a fronte degli ordini ricevuti e delle consegne effettuate.

Il fornitore deve, pertanto, dotarsi degli strumenti informatici idonei alla gestione dei nuovi adempimenti telematici. Per i dettagli tecnici si rinvia alla sezione dedicata al sito dell'Agenzia Intercent-ER http://intercenter.regione.emilia-romagna.it, che contiene tutti i riferimenti del Sistema Regionale per la dematerializzazione del Ciclo Passivo degli Acquisti (formato dei dati, modalità di colloquio, regole tecniche, ecc.), nonché al Nodo telematico di Interscambio No TI-ER.

In alternativa, le imprese possono utilizzare le funzionalità per la ricezione degli ordini e l'invio dei documenti di trasporto elettronici che sono messe a disposizione sulla piattaforma di Intercent-ER all'indirizzo https://piattaformaintercenter.regione.emila-romagna.it/portale/ previa registrazione.

Le spese di bonifico applicate dall'Istituto Tesoriere, secondo quanto previsto dalla convenzione in essere alla data di pagamento, sono a carico della ditta aggiudicataria.

Inoltre, ai sensi delle disposizioni previste dall'art 9-ter, comma 8, del Decreto-legge 19 giugno 2015 n. 78, come modificato dall'articolo 1, comma 557 della legge 30 dicembre 2018, n.145 e dalle indicazioni operative di cui alla circolare interministeriale prot. 2051-P-08/02/2019, le fatture elettroniche relative ai Dispositivi Medici dovranno altresì riportare la valorizzazione degli elementi componenti il codice articolo, come sotto dettagliato:

<Codice Tipo>	'DMX, con X=[1|2/0] a seconda del tipo di dispositivo medico oggetto dell'operazione. Quindi: 1 per "Dispositivo medico o Dispositivo diagnostico in vitro" 2 per "Sistema o kit Assemblato" 0 nel caso in cui non si sia in grado di identificare il numero di repertorio
<Codice	Numero di registrazione attribuito al dispositivo medico nella

Valore>	Banca dati e Repertorio Dispositivi Medici, ai sensi del decreto del Ministro della salute 21 dicembre 2009 (GU n.17 del 22 gennaio 2010) o decreto del Ministro della salute 23 dicembre 2013 (G.U. Serie Generale, n. 103 del 06 maggio 2014). Per i dispositivi medici e i dispositivi diagnostici in vitro che, sulla base delle disposizioni previste, dal decreto del Ministro della salute 21 dicembre 2009 e dal decreto del Ministro della salute 23 dicembre 2013 non sono tenuti all'iscrizione nella Banca dati/ Repertorio dei dispositivi medici, o per i quali le aziende fornitrici di dispositivi medici alle strutture del Servizio Sanitario Nazionale non sono in grado di identificare il numero di repertorio, il campo è trasmesso con il valore 0.

16. Acquisto in danno

Qualora l'Azienda Sanitaria riscontrasse, anche in sede di prima fornitura, la non conformità, sia nella qualità sia nella quantità, della merce ai requisiti richiesti e pattuiti e qualora non venissero rispettati i termini di consegna previsti dal capitolato, invierà formale contestazione con specifica delle motivazioni e con invito a conformarsi nel termine che sarà ritenuto congruo.

Inoltre, l'Azienda Sanitaria avrà il diritto di acquistare presso altre ditte i prodotti occorrenti a danno del fornitore inadempiente; resterà, cioè, a carico dell'inadempiente sia la differenza per l'eventuale maggiore prezzo rispetto a quello convenuto sia ogni altro maggiore onere o danno comunque derivante all'Azienda a causa dell'inadempienza stessa

17. Modifiche del contratto e subappalto

Il contratto di appalto potrà essere modificato, senza una nuova procedura di affidamento, ai sensi dell'art 120 del D.Lgs. 36/2023, al verificarsi delle seguenti condizioni:

- in caso di acquisti per un quinto dell'importo art. 120 comma 9, per un importo massimo del 20% sul contratto oneri fiscali esclusi;
- in caso di proroga tecnica di 180 gg per complessivi € 95.000,00 art 120 comma 11 del D.Lgs. 36/2023;

È ammesso il subappalto nei limiti e con le modalità previste dall'art.119 del D.Lgs.36/2023.

Non può essere affidata in subappalto l'integrale esecuzione della fornitura e delle prestazioni oggetto del contratto, può essere eventualmente ammesso il subappalto per le sole attività accessorie.

Il contratto tra appaltatore e subappaltatore/subcontraente ai sensi della legge 13 agosto 2010, n.136 e s.m., dovrà contenere le seguenti clausole:

(Obblighi del subappaltatore/subcontraente relativi alla tracciabilità dei flussi finanziari)

1. *L'impresa (…), in qualità di subappaltatore/subcontraente dell'impresa (…) nell'ambito del contratto sottoscritto con l'Ente (…), identificato con il CIG n. (…) /CUP n. (…), assume tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'articolo 3 della legge 13 agosto 2010, n. 136 e successive modifiche.*
2. *L'impresa (…), in qualità di subappaltatore/subcontraente dell'impresa (…), si impegna a dare immediata comunicazione all'Ente (…) della notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria.*

3. *L'impresa (…), in qualità di subappaltatore/subcontraente dell'impresa (…), si impegna ad inviare copia del presente contratto all'Ente (…)*

18. Divieto di cessione del contratto e dei crediti

1. È fatto assoluto divieto al Fornitore di cedere, a qualsiasi titolo, il contratto, a pena di nullità delle cessioni stesse, salvo quanto previsto dall'art. 120 co. 1, lett. d) n. 2 del D.lgs. n. 36/2023.

2. Per la cessione dei crediti si applicano le seguenti disposizioni.

3. Ai sensi e per gli effetti di cui all'art.6 dell'allegato II.14 del D.Lgs.n.36/2023, ai fini dell'opponibilità alla stazione appaltante (intendendosi per essa l'Amministrazione stipulante il contratto), la cessione dei crediti deve essere stipulata mediante atto pubblico o scrittura privata autenticata e deve essere notificata alla medesima stazione appaltante all'indirizzo pec indicato contrattualmente o in mancanza quello reperibile sui pubblici registri.

4. Fatto salvo il rispetto degli obblighi di tracciabilità, la cessione dei crediti da corrispettivo d'appalto (del presente contratto) è efficace e opponibile alla stazione appaltante qualora questa non la rifiuti con comunicazione da trasmettere tramite pec al cedente (all'indirizzo di posta elettronica certificata indicata nel contratto) e al cessionario (all'indirizzo di posta elettronica certificata da cui proviene la comunicazione e documentazione inerente la cessione), oppure per entrambi i casi agli indirizzi di posta certificata reperibili sui pubblici registri **entro trenta** giorni dalla notifica della cessione.

5. Il rifiuto è valido e rende la cessione dei crediti inopponibile alla stazione appaltante a prescindere dal fatto che il contratto (sottostante alle fatture cedute) sia o meno in corso di esecuzione al momento della notifica della cessione. Conseguentemente, la cessionaria non potrà avanzare alcuna pretesa nei confronti della stazione appaltante.

6. In via generale non sono ammesse cessioni dei crediti riferite a fatture già pagate alla cedente, le cessioni dei crediti riferite a più amministrazioni e quelle prive di riferimento specifico circa il titolo e l'oggetto del credito ceduto.

7. In ogni caso le cessioni dei crediti rifiutate, qualora per qualsiasi ragione dovessero essere fatte valere verso la stazione appaltante, dovranno essere rinotificate nelle forme di legge.

8. La stazione appaltante cui è stata notificata la cessione può opporre al cessionario tutte le eccezioni opponibili al cedente in base al presente contratto.

19. Clausola Whistleblowing

L'impresa si impegna a comunicare al proprio personale che opera nel contesto lavorativo dell'Azienda Sanitaria, il collegamento ipertestuale alla pagina dell'Azienda dedicata all'istituto del whistleblowing, al fine di renderlo edotto dei propri diritti e relative tutele raggiungibile al seguente indirizzo:
https://whistleblowing.ospfe.it/

20. Recesso dal contratto

Fermo restando quanto previsto dagli articoli 88, comma 4-ter e 92, comma 4, del codice delle leggi antimafia e delle misure di prevenzione, di cui al decreto legislativo 6 settembre 2011, n. 159 la stazione appaltante può recedere dal contratto secondo quanto stabilito all'art.123 del D.Lgs.

36/2023. L'Azienda Sanitaria può inoltre avvalersi della facoltà di recesso consentita dall'art.1671 del Codice civile.

Qualora l'impresa aggiudicataria dovesse recedere dal contratto prima della scadenza convenuta, l'Azienda Sanitaria, oltre a incamerare la garanzia, si riserva di addebitare le eventuali maggiori spese insorgenti per l'assegnazione ad altra ditta.

21. Clausola di revisione prezzi

I presente articolo disciplina le modalità di revisione dei prezzi per il presente contratto, in conformità con le disposizioni del Codice dei Contratti Pubblici.
La revisione dei prezzi sarà applicabile qualora si determina una variazione del costo della fornitura o del servizio, in aumento o in diminuzione, superiore al 5 per cento dell'importo complessivo e operano nella misura dell'80 per cento del valore eccedente la variazione del 5 per cento applicata alle prestazioni da eseguire, come previsto dall'articolo 60 del Codice dei Contratti Pubblici.

Ai fini della determinazione della variazione dei costi e dei prezzi di cui al punto precedente, si utilizzano gli indici sintetici elaborati dall'ISTAT con riguardo ai contratti di servizi e forniture, anche disaggregati, dei prezzi al consumo, dei prezzi alla produzione dell'industria e dei servizi e gli indici delle retribuzioni contrattuali orarie.
L'appaltatore potrà presentare richiesta scritta di revisione dei prezzi alla stazione appaltante, corredata dalla documentazione che attesti la variazione degli indici di prezzo.

La stazione appaltante valuterà la richiesta entro 30 giorni dalla ricezione della stessa. In caso di esito positivo, la revisione dei prezzi sarà formalizzata mediante atto aggiuntivo al contratto. La revisione dei prezzi non potrà, in nessun caso, alterare la natura generale del contratto né comportare una modifica sostanziale delle prestazioni previste.
Le nuove condizioni economiche determinate dalla revisione dei prezzi saranno applicabili a partire dal 30° giorno successivo alla data di accettazione da parte della stazione appaltante.

22. Brevetti industriali e diritti d'autore

La Ditta assume ogni responsabilità in ordine all'uso di dispositivi, o per l'adozione di soluzioni tecniche, o di altra natura, che violino diritti di brevetto, di autore ed in genere di privativa altrui.

Qualora venga promossa nei confronti dell'Azienda Sanitaria azione giudiziaria da parte di terzi che vantino diritti su beni acquistati o presi in locazione o licenza d'uso la Società/Ditta sosterrà tutte le spese di giudizio nonché gli oneri conseguenti.

Qualora l'azione giudiziaria sia fondata l'Azienda appaltante ha diritto al risarcimento dei danni eventualmente subiti (danno d'immagine e divieto all'uso) e la facoltà di dichiarare risolto il contratto di diritto.

23. Clausole contrattuali di cui all'Intesa per la Legalità del 19.06.2018 della Prefettura di Bologna

Clausola n. 1
L'impresa dichiara di essere a conoscenza di tutte le norme pattizie di cui alla Intesa per la Legalità, sottoscritta il 19.06.2018 con la Prefettura di Bologna, tra l'altro consultabile al sito http://www.prefettura.it/bologna/multidip/index.htm, e che qui si intendono integralmente riportate, e di accettarne incondizionatamente il contenuto e gli effetti.

Clausola n. 2

L'impresa si impegna a comunicare alla stazione appaltante l'elenco delle imprese coinvolte nel piano di affidamento nell'esecuzione dei lavori, servizi o forniture con riguardo alle forniture ed ai servizi di cui all'art. 3, lett. a) dell'Intesa, nonché ogni eventuale variazione successivamente intervenuta per qualsiasi motivo.
Ove i suddetti affidamenti riguardino i settori di attività a rischio di cui all'art. 1, comma 53, della L. 190/2012, la sottoscritta impresa si impegna ad accertare preventivamente l'avvenuta o richiesta iscrizione della ditta sub affidataria negli elenchi prefettizi dei fornitori, prestatori di servizi ed esecutori di lavori non soggetti a tentativi di infiltrazione mafiosa.

Clausola n. 3
L'impresa si impegna a denunciare immediatamente alle Forze di Polizia o all'Autorità Giudiziaria ogni illecita richiesta di denaro, prestazione o altra utilità ovvero offerta di protezione nei confronti dell'imprenditore, degli eventuali componenti la compagine sociale o dei rispettivi familiari (richiesta di tangenti, pressioni per indirizzare l'assunzione di personale o l'affidamento di lavorazioni, forniture o servizi a determinate imprese, danneggiamenti, furti di beni personali o di cantiere).

Clausola n. 4
La sottoscritta impresa si impegna a segnalare alla Prefettura l'avvenuta formalizzazione della denuncia di cui alla precedente clausola 3 e ciò al fine di consentire, nell'immediato, eventuali iniziative di competenza.

Clausola n. 5
La sottoscritta impresa dichiara di conoscere e di accettare la clausola risolutiva espressa che prevede la risoluzione immediata ed automatica del contratto, ovvero la revoca dell'autorizzazione al subappalto o subcontratto, qualora dovessero essere comunicate dalla Prefettura, successivamente alla stipula del contratto o subcontratto, informazioni interdittive analoghe a quelle di cui agli artt. 91 e 94 del D.Lgs. 159/2011, ovvero la sussistenza di ipotesi di collegamento formale e/o sostanziale o di accordi con altre imprese partecipanti alle procedure concorsuali d'interesse.
Qualora il contratto sia stato stipulato nelle more dell'acquisizione delle informazioni del Prefetto, sarà applicata a carico dell'impresa, oggetto dell'informativa interdittiva successiva, anche una penale nella misura del 10% del valore del contratto ovvero, qualora lo stesso non sia determinato o determinabile, una penale pari al valore delle prestazioni al momento eseguite; le predette penali saranno applicate mediante automatica detrazione, da parte della stazione appaltante, del relativo importo dalle somme dovute all'impresa in relazione alle prestazioni eseguite.

Clausola n. 6
La sottoscritta impresa dichiara di conoscere e di accettare la clausola risolutiva espressa che prevede la risoluzione immediata ed automatica del contratto, ovvero la revoca dell'autorizzazione al subappalto o subcontratto, in caso di grave e reiterato inadempimento delle disposizioni in materia di collocamento, igiene e sicurezza sul lavoro anche con riguardo alla nomina del responsabile della sicurezza e di tutela dei lavoratori in materia contrattuale e sindacale.

Clausola n. 7
La sottoscritta impresa dichiara di essere a conoscenza del divieto per le stazioni appaltanti pubbliche di autorizzare subappalti a favore delle imprese partecipanti alle operazioni di selezione e non risultate aggiudicatarie, salvo le ipotesi di lavorazioni altamente specialistiche o nei casi in cui l'accordo per l'affidamento del subappalto sia intervenuto successivamente all'aggiudicazione.

Clausola n. 8
La sottoscritta impresa si impegna a dare comunicazione tempestiva alla Prefettura e all'Autorità giudiziaria di tentativi di concussione che si siano, in qualsiasi modo, manifestati nei confronti dell'imprenditore, degli organi sociali o dei dirigenti di impresa. Dichiara altresì di essere a conoscenza che il predetto adempimento ha natura essenziale ai fini dell'esecuzione del contratto

e che il relativo inadempimento darà luogo alla risoluzione espressa del contratto stesso, ai sensi dell'art. 1456 c.c. ogni qualvolta nei confronti di pubblici amministratori e di funzionari che abbiano esercitato funzioni relative alla stipula ed esecuzione del contratto, sia stata disposta misura cautelare e sia intervenuto rinvio a giudizio per il delitto previsto dall'art. 317 c.p.

Clausola n. 9
La sottoscritta impresa dichiara di conoscere e di accettare la clausola risolutiva espressa, di cui all'art. 1456 c.c., ogni qualvolta nei confronti dell'imprenditore o dei componenti la compagine sociale o dei dirigenti dell'impresa, sia stata disposta misura cautelare o sia intervenuto rinvio a giudizio per taluno dei delitti di cui agli artt. 317 c.p., 318 c.p., 319 c.p., 319 bis c.p., 319 ter c.p., 319 quater c.p., 320 c.p., 322 c.p., 322 bis c.p., 346 bis c.p., 353 c.p. e 353 bis c.p".

Clausola n. 10
La sottoscritta impresa si obbliga ad inserire in tutti i subcontratti la clausola risolutiva espressa nel caso in cui emergano informative interdittive a carico dell'altro subcontraente; tale clausola dovrà essere espressamente accettata dalla impresa subcontraente.

Clausola n. 11
La sottoscritta impresa dichiara di conoscere e di accettare la clausola risolutiva espressa ovvero la revoca dell'autorizzazione al subappalto o subcontratto, in caso di grave e reiterato inadempimento delle disposizioni in materia di collocamento, igiene e sicurezza sul lavoro anche con riguardo alla nomina del responsabile della sicurezza e di tutela dei lavoratori in materia contrattuale e sindacale.

24. Spese Accessorie

Ogni spesa inerente e conseguente al contratto è a carico dell'aggiudicatario.

25. Segnalazioni all'Anac

Fermo restando quanto previsto dalle Linee Guida n. 6 approvate dall'Anac con delibera n. 1293 del 16.11.2016, in caso di false dichiarazioni rilasciate dall'impresa aggiudicataria in sede di gara, emerse durante la fase della consegna, del collaudo ed esecuzione dei servizi, l'Azienda Sanitaria procederà alla segnalazione all'ANAC (per l'adozione dei provvedimenti che riterrà di dover applicare). Alla segnalazione all'Autorità, l'Azienda Sanitaria procederà ad incamerare il deposito cauzionale definitivo.

Qualora le false dichiarazioni attengano ai requisiti di ammissione alla procedura di gara, l'Azienda Sanitaria procederà inoltre, oltre a quanto sopra indicato, alla risoluzione del contratto ed all'applicazione di ogni altra azione prevista dal presente Capitolato Speciale per i casi di risoluzione del contratto.

26. Controversie e Foro competente

Le controversie su diritti soggettivi, derivanti dall'esecuzione del presente contratto, non saranno deferite ad arbitri.

Per ogni controversia giudiziale relativa alla presente gara è competente esclusivamente il Foro di Bologna, mentre per le controversie che dovessero insorgere nell'esecuzione della fornitura/servizio è competente, esclusivamente, il Foro in cui ha sede l'Azienda Sanitaria che è parte in causa.

Per accettazione
(firma digitale del Legale Rappresentante)