CAPITOLATO TECNICO
ACQUISIZIONE IN "SERVICE" DI UN SISTEMA DIAGNOSTICO PER LA DETERMINAZIONE DELL'INFEZIONE DA HELICOBACTER PYLORI E DELL'INTOLLERANZA AL LATTOSIO
PER LE NECESSITA' DELLA UOC LABORATORIO ANALISI DELLA ASL DI PESCARA

ART. 1 Oggetto della fornitura
La presente procedura di gara, ai sensi dell'art. 50 comma 1, lettera b) del D.Lgs 36/2023, ha per oggetto la fornitura in service di un sistema diagnostico per la determinazione dell'infezione gastroduodenale da Helicobacter pylori e dell'intolleranza al lattosio costituito da test diagnostico e analizzatore per la determinazione del rapporto isotopico 13C/12C, su campioni di aria espirata (**Breath test**), in seguito al metabolismo del substrato marcato somministrato, per le necessità della UOC Laboratorio Analisi della ASL di Pescara.

ART. 2 Durata e valore dell'appalto
La fornitura avrà durata annuale. Sono previste, altresì, le seguenti opzioni:
- opzione di estensione del 20% del contratto, ai sensi dell'art. 120, comma 9, del D. Lgs. n. 36/2023;
- opzione di proroga, ai sensi dell'art. 120, comma 10, del D. Lgs. n. 36/2023;

Ai sensi dell'art. 14, comma 4, del D. Lgs. n. 36/2023 e s.m.i., il valore complessivo a base d'asta della presente procedura di gara, riferito alla sua durata annuale e alle opzioni sopra indicate, è stimato in **€ 68.000,00** Iva esclusa, così ripartito:

a) prezzo annuale a base d'asta **€ 40.000,00** al netto di Iva;
b) opzione di estensione del 20% del valore del contratto **€ 8.000,00** al netto di Iva;
c) proroga tecnica **€ 20.000,00** al netto di Iva;

ART. 3 Requisiti minimi della fornitura
La fornitura in service comprende tutte le prestazioni di servizi e forniture di beni necessari a garantire il funzionamento del sistema, secondo quanto stabilito nel presente capitolato e nella ulteriore documentazione di gara.
Nello specifico, l'affidamento comprenderà le caratteristiche di seguito elencate, le quali sono da ritenersi indispensabili, pena l'esclusione dalla procedura.

Il sistema richiesto dovrà essere composto da:

a. Strumentazione analitica ad infrarossi non dispersiva (NDIR) per la determinazione del rapporto isotopico $^{12}C/^{13}C$ nell'espirato.

b. PC, gruppo UPS e stampante dedicati allo strumento.

c. Substrato per somministrazione orale a base di urea marcata con ^{13}C.

d. Substrato per somministrazione orale a base di lattosio marcato con ^{13}C.

e. Accessori per l'esecuzione dei test.

f. Manutenzione ordinaria e straordinaria.

g. Aggiornamento strumentale e software.

La Ditta proponente dovrà assicurare un periodo di formazione del personale addetto alla esecuzione dei test richiesti, previo accordo con la UOC di Laboratorio Analisi.

Caratteristiche minime della fornitura a pena di esclusione

a. Strumentazione nuova di fabbrica e di ultima generazione.
b. Conformità alla normativa CE/IVDr.
c. Collegamento bidirezionale con il LIS del Laboratorio Analisi per la gestione dei dati analitici.
d. Specialità medicinale dotata di AIC (Autorizzazione Immissione in Commercio) italiana per il test dedicato alla determinazione dell'infezione da Helicobacter pylori.
e. Fornitura completa degli accessori (cannucce e provette o sacchi per il campionamento)
h. Aggiornamento strumentale e software.

ART. 4 Tipologia di test richiesti, fabbisogno annuo presunto e cadenza sedute analitiche

Ref.	Tipo di test richiesto	Fabbisogno annuo presunto n. test/anno	Sedute analitiche settimanali
1	Diagnosi dell'infezione da Helicobacter pylori: - ^{13}C Urea breath test	700	2
2	Studio intolleranza al lattosio: - ^{13}C Lattosio breath test	700	2

Si precisa che il volume delle prestazioni indicato nella precedente tabella è da ritenersi puramente indicativo, e potrà variare in più o in meno in relazione al fabbisogno effettivo dell'Azienda. Pertanto, l'aggiudicatario non potrà pretendere alcun compenso aggiuntivo a motivo delle maggiori o minori quantità richieste.
L'entità della somministrazione sarà diluita nel tempo e correlata al reale fabbisogno dell'Azienda, dipendente dalle necessità assistenziali da soddisfare durante la vigenza contrattuale.

ART. 5 Caratteristiche della "fornitura in service"
I prodotti offerti dovranno essere conformi al Regolamento Europeo n. 745/2017.
La fornitura dovrà inoltre rispettare le caratteristiche di seguito descritte.

a) Fornitura in service di apparecchiature
La fornitura in argomento comprende le apparecchiature necessarie all'esecuzione degli esami richiesti. La strumentazione proposta deve essere nuova di fabbrica e di ultima generazione e deve essere pienamente rispondente ai requisiti minimi indicati al precedente art. 3.
Essa deve possedere la marcatura CE-IVDr e deve essere conforme alle vigenti disposizioni normative nazionali e internazionali, alle disposizioni regolamentari e tecniche, nonché in materia di sicurezza.
La ditta aggiudicataria curerà il trasporto, l'installazione, il collaudo e la messa in funzione dell'apparecchiatura oggetto di fornitura, verificando, all'atto della consegna e prima della sua messa in funzione, il corretto funzionamento, l'integrità dello strumento e degli accessori forniti e la rispondenza alle leggi e alle norme tecniche vigenti, rilasciando apposito rapporto tecnico.
L'apparecchiatura sarà consegnata alla U.O. utilizzatrice nel suo imballo, in modo da essere protetta contro qualsiasi manomissione o danno da maneggiamento. Gli imballaggi devono essere conformi alla normativa vigente e dovranno essere smaltiti a carico della ditta fornitrice. Deterioramenti per negligenza e/o insufficienti imballaggi o in conseguenza del trasporto, conferiscono all'Azienda il diritto di rifiutare i beni, in danno alla ditta aggiudicataria. I componenti che dovessero risultare alterati o danneggiati prima della loro installazione e consegna definitiva saranno immediatamente rimossi e sostituiti a spese della ditta aggiudicataria. È altresì a carico della ditta aggiudicataria la disinstallazione dell'apparecchiatura alla scadenza del contratto.

b) Fornitura in somministrazione di reagenti
La ditta aggiudicataria dovrà garantire la fornitura in somministrazione dei reagenti occorrenti all'effettuazione del test nella quantità presunta richiesta.
I reagenti offerti devono rispondere pienamente ai requisiti minimi indicati nella presente gara e dovranno essere provvisti di marcatura CE-IVDR e CE-MD dove applicabile. I reagenti necessari all'avviamento della strumentazione e ai relativi collaudi previsti dalle normative vigenti dovranno essere forniti dall'aggiudicataria in sconto merce e al di fuori del materiale offerto per le determinazioni analitiche richieste con la presente gara.

c) Fornitura di calibratori, controlli, consumabili e accessori
Dovranno essere forniti, a cura e spese della ditta aggiudicataria, i calibratori, i controlli, i consumabili e gli accessori necessari all'esecuzione del numero di determinazioni richieste.
In offerta devono essere indicati tutti i materiali necessari al sistema per l'effettiva esecuzione degli esami richiesti. Per materiale di consumo deve intendersi anche quello occorrente per la refertazione (come toner, cartucce per stampante, ecc.).
I calibratori dovranno esser forniti in quantità sufficiente ad ogni necessità di calibrazione tenuto conto anche della stabilità dei prodotti utilizzati. I controlli dovranno essere almeno su due livelli, aventi valore, rispettivamente, nell'ambito della normalità e delle patologie ed essere in quantità idonea alle necessità operative.

d) Servizio di manutezione e assistenza tecnica
La fornitura "in service" è comprensiva del servizio di assistenza tecnica "full risk", ovvero di tutti quei servizi necessari a garantire la continuità delle prestazioni oggetto di fornitura.
In particolare, il servizio comprenderà:
- la manutenzione preventiva/ordinaria, ovvero l'esecuzione di interventi a cadenze fisse, programmate e gestite secondo un piano di manutenzione concordato tra la ditta aggiudicataria e il Responsabile del laboratorio. Il piano dovrà prevedere almeno una verifica

di sicurezza annua secondo le normative vigenti;
- la manutenzione straordinaria, inclusi i pezzi di ricambio, necessaria a garantire il corretto funzionamento del sistema fornito, il mantenimento del bene alle condizioni originali e comunque pienamente rispondente ai livelli di sicurezza e prestazione richiesti dalle norme.

L'assistenza tecnica dovrà essere garantita tramite Centri e/o tecnici autorizzati dalla Ditta produttrice o esclusivista della strumentazione e, eventualmente, con connessione remota dello strumento via VPN con il servizio tecnico della ditta fornitrice a scopo di monitoraggio quotidiano, prevenzione del fermo strumentale e tele aggiornamento dello strumento offerto.
Saranno in ogni caso a carico della Ditta i consumi di reagenti, consumabili e materiale accessorio, imputabili a documentato malfunzionamento dell'apparecchiatura, nonché quelli relativi alla messa a punto della strumentazione in occasione di ogni intervento di manutenzione.
Oltre a quanto sinora specificato, l'offerta dovrà prevedere i seguenti servizi minimi:

- almeno due manutenzioni programmate per anno;
- la presenza presso il laboratorio di personale idoneo ad eseguire l'intervento entro 48 ore solari dalla richiesta di intervento, esclusi i festivi, con risoluzione del guasto entro le successive 24 ore solari (8 ore lavorative);
- formazione del personale tecnico e supporto scientifico.

ART. 6 Modalità di esecuzione della fornitura – Consegne

I tempi per la consegna e l'installazione delle attrezzature non potranno essere superiori a 60 giorni solari complessivi dalla data di emissione dell'ordine.
Fermo restando quanto previsto al successivo art. 18 in materia di inadempienze e penalità, in caso di ritardo superiore a 15 giorni consecutivi, l'Azienda potrà risolvere il contratto con comunicazione a mezzo PEC. In tal caso, oltre al risarcimento dei danni, verrà addebitata alla ditta aggiudicataria anche la differenza derivante dalla maggiore spesa eventualmente sostenuta per l'acquisizione delle apparecchiature da altra ditta.
L'Amministrazione si riserva di indicare in fase di ordine una data di consegna successiva qualora sussistano esigenze di coordinamento con eventuali lavori di predisposizione dei locali.
L'apparecchiatura deve essere consegnata, installata e collaudata presso i locali della U.O. di destinazione, previo accordo con il Direttore della struttura.
Restano a carico della ditta aggiudicataria:

- il trasporto;
- il trasferimento dell'apparecchiatura al locale di destinazione, compreso l'utilizzo di eventuali macchine di sollevamento e tutto quanto necessario alla corretta e completa installazione della stessa;
- l'imballaggio e il suo smaltimento,
- la custodia dei materiali fino all'installazione.

Ogni sostituzione di apparecchiatura deve essere avallata dal dirigente responsabile della U.O. utilizzatrice.
I tempi per la consegna dei reagenti e del materiale consumabile non potranno essere superiori a 10 (dieci) giorni solari complessivi dalla data di emissione dell'ordine. In caso di urgenza, con espressa e motivata indicazione sull'ordinativo trasmesso al fornitore, la consegna dei prodotti dovrà avvenire entro e non oltre 5 (cinque) giorni dal momento della trasmissione dell'ordine, esclusi festivi.
All'atto della consegna la validità residua dei prodotti non può essere inferiore ai 3/4 della validità complessiva, salvo espressa autorizzazione dell'utilizzatore a ricevere prodotti con una scadenza inferiore.
Al momento della consegna i trasportatori dovranno rilasciare apposita certificazione atta a dimostrare che tutto il materiale (reagenti, calibratori e controlli) sia stato trasportato a temperatura controllata.

La quantità dei reagenti e del restante materiale consegnato sarà esclusivamente quella accertata presso il magazzino ricevente e dovrà essere riconosciuta ad ogni effetto dal fornitore.
Per quanto riguarda il controllo qualitativo della merce, resta inteso che la firma per ricevuta, rilasciata al momento della consegna, non impegnerà all'accettazione la ASL di Pescara, che si riserva il diritto di verificare la corrispondenza qualitativa in sede di effettivo utilizzo della merce consegnata, oppure sottoponendo la stessa ad analisi tecniche di laboratorio.
La ditta aggiudicataria si impegna ad accettare la relazione di analisi e, nel caso in cui la merce non corrisponda a quanto convenuto, a pagare le relative spese, oltre, naturalmente, alle sanzioni previste nel presente capitolato.
I prodotti che presenteranno difetti o discordanze saranno tenuti a disposizione della ditta aggiudicataria e restituiti anche se tolti dal loro imballo originario, e la ditta stessa dovrà provvedere alla sostituzione, entro 5 (cinque) giorni solari, con materiale nella qualità stabilita e nella quantità richiesta.

ART. 7 Clausola Consip

Qualora durante il periodo di vigenza contrattuale, il sistema di convenzioni per l'acquisto di beni e servizi delle Pubbliche Amministrazioni realizzato dal Ministero dell'Economia e delle Finanze ai sensi dell'art. 26 della Legge 488/99 (CONSIP), dalla Centrale Regionale Acquisti, comprendesse anche le forniture di prodotti di cui alla presente gara, a condizioni più vantaggiose a seguito di aggiudicazioni di gare centralizzate disposte dalla CONSIP, l'Azienda può richiedere la risoluzione del contratto, salvo che la ditta aggiudicataria non offra di adeguare la propria offerta rispetto a quella più vantaggiosa.

ART. 8 Equivalenza

In relazione alle caratteristiche tecniche richieste si precisa che la stazione appaltante applica il c.d. principio di equivalenza ex art. 79 e Allegato II.5, Parte II, lett. A, commi 7 e 8, del D. Lgs. n. 36/2023 e ss.mm. e ii. Qualora, infatti, la descrizione dei beni messi a gara dovesse individuare una fabbricazione o provenienza determinata o un procedimento particolare, un marchio o un brevetto determinato, un tipo o un'origine o una produzione specifica che avrebbero come effetto di favorire o eliminare talune imprese o prodotti, detta previsione deve intendersi integrata dalla menzione "o equivalente". Pertanto l'impresa concorrente può presentare un bene anche non conforme alle specifiche riportate nel presente capitolato purché funzionalmente equivalente dal punto di vista clinico ed è obbligato a segnalarlo con separata dichiarazione da allegare alla relativa scheda tecnica. In tal caso l'impresa concorrente deve provare, con qualsiasi documento appropriato, che le soluzioni da lui proposte ottemperano in maniera equivalente ai requisiti definiti nelle specifiche tecniche.

ART. 9 Criterio di aggiudicazione

Fermo restando il possesso dei requisiti minimi richiesti l'aggiudicazione della fornitura avverrà sulla base del criterio del minor prezzo ai sensi dell'art. 108 comma 3 del D. Lgs 36/2023.

ART. 10 Documenti tecnici

Con riferimento all'apparecchiatura in service, il possesso dei requisiti (minimi e qualitativi) indicati dal presente capitolato dovrà essere comprovato dalle schede tecniche, dai manuali d'uso e dalla ulteriore documentazione tecnica prodotta in sede di offerta tecnica.
La suddetta documentazione dovrà essere in lingua italiana ovvero dovrà essere tradotta in italiano e ad essa dovranno essere allegate tutte le certificazioni in corso di validità.

Le ditte partecipanti, inoltre, ai fini della valutazione tecnica, dovranno presentare una relazione firmata dal Legale Rappresentante, volta ad illustrare, in relazione al prodotto offerto, le specifiche tecniche, le caratteristiche e gli elementi propri dello strumento rispetto ai requisiti tecnici – minimi e qualitativi – stabiliti dal presente capitolato, fornendo tutti gli elementi e la documentazione ritenuta utile per effettuare una completa valutazione dell'offerta tecnica.
Devono inoltre essere specificati i termini di consegna dell'apparecchiatura proposta e i tempi di installazione e di avviamento a pieno regime della stessa.
Dovranno essere esplicitati, altresì, le modalità del servizio di assistenza e il piano/programma di formazione.
Nell'offerta tecnica, ai fini della relativa valutazione, dovranno essere descritti dettagliatamente tutti i reagenti, i calibratori, i controlli e i materiali di consumo necessari all'esecuzione delle determinazioni analitiche richieste, indicando in modo chiaro:

a) nome commerciale dei prodotti, il tipo di confezionamento e relativi codici;
b) nome della ditta produttrice;
c) caratteristiche e schede tecniche dei reagenti e degli ulteriori prodotti offerti;
d) modalità di conservazione;
e) tempo di validità minima del materiale fornito e a confezione aperta;
f) tipo e quantità di ogni reagente/materiale necessario all'esecuzione della determinazione richiesta, in rapporto all'apparecchiatura offerta;
g) modalità di smaltimento dei rifiuti liquidi e solidi al fine di consentire alla ASL di Pescara di adempiere alle disposizioni in materia.

Nell'offerta tecnica dovranno essere inoltre riportate le caratteristiche del software del sistema offerto.
Le ditte partecipanti dovranno effettuare, a pena di esclusione, mediante proprio personale tecnico qualificato, un sopralluogo obbligatorio, per il corretto posizionamento degli strumenti negli spazi adibiti all'installazione.

I sopralluoghi potranno avvenire dal lunedì al venerdì dalle ore 10 alle ore 13, previo preventivo accordo con il Direttore della UOC Laboratorio Analisi della Asl di Pescara. Si fornisce, a tal proposito, il seguente contatto:

- Dott. Giancarlo Di Iorio giancarlo.diiorio@asl.pe.it

Il sopralluogo dovrà essere effettuato dal legale rappresentante della ditta o da un suo incaricato.
L'amministrazione provvederà a rilasciare un'attestazione dell'avvenuto sopralluogo.

L'aggiudicatario sarà tenuto a garantire la piena compatibilità del sistema offerto con i locali di installazione in termini impiantistici e di pesi e dimensioni (nel rispetto della normativa cogente in materia di rumorosità e di calore sviluppato, nonché di ingombro utile a garantire il lavoro in condizione di sicurezza per gli operatori).

ART. 11 Valutazione delle offerte
Il possesso dei requisiti minimi e dei requisiti qualitativi è verificato dalla Commissione giudicatrice. I requisiti minimi, in quanto indispensabili, devono essere posseduti dall'offerta presentata a pena di esclusione mentre i requisiti qualitativi sono oggetto di attribuzione di punteggio di qualità. Pertanto, la Commissione giudicatrice verificherà preliminarmente il possesso di tutte le caratteristiche minime previste dagli atti di gara e, una volta "ammessa" l'offerta tecnica, procederà alla valutazione qualitativa.

Qualora dalla documentazione tecnica presentata fosse impossibile desumere le caratteristiche tecnico-qualitative della fornitura utili per l'attribuzione del punteggio, quest'ultimo sarà pari a 0 per le voci in esame.

ART. 12 Obblighi generali del fornitore

Il fornitore è tenuto ad eseguire tutte le prestazioni a perfetta regola d'arte, nel rispetto delle norme vigenti e secondo le modalità, i termini e le prescrizioni stabiliti dagli atti di gara. Le prestazioni contrattuali dovranno essere conformi alle caratteristiche tecniche e commerciali, nonchè alle specifiche indicate nell'offerta tecnica.

Il fornitore si obbliga ad osservare, nell'esecuzione delle prestazioni contrattuali, tutte le norme e le prescrizioni legislative e regolamentari applicabili, siano esse di carattere generale o specificatamente inerenti al settore merceologico cui i beni appartengono e in particolare quelle di carattere tecnico di sicurezza, di igiene e sanitarie vigenti, incluse quelle che dovessero essere emanate successivamente alla conclusione del contratto.

In particolare, il fornitore contraente si impegna a:

- rispettare, per quanto applicabili, le norme internazionali e N-ISO vigenti per la gestione e l'assicurazione della propria qualità e delle proprie prestazioni;
- predisporre tutti gli strumenti e i metodi, comprensivi della relativa documentazione, al fine di consentire alla Asl Pescara di verificare la conformità dei prodotti offerti agli atti di gara;
- predisporre tutti gli strumenti e i metodi, comprensivi della relativa documentazione, atti a garantire elevati livelli di servizio, compresi quelli relativi alla sicurezza e alla riservatezza.

Gli eventuali maggiori oneri derivanti dall'obbligo di osservare le prescrizioni di cui sopra, anche se entrate in vigore successivamente alla stipula del contratto, resteranno ad esclusivo carico del fornitore contraente, intendendosi in ogni caso remunerati con il corrispettivo contrattuale; il fornitore contraente non potrà, pertanto, avanzare pretesa di indennizzi e/o compensi a tale titolo nei confronti dell'ASL di Pescara.

Il fornitore contraente si impegna espressamente a manlevare e tenere indenne l'ASL di Pescara da tutte le conseguenze derivanti dall'eventuale inosservanza delle prescrizioni di cui alla presente gara, incluse, tra l'altro, quelle derivanti da danni arrecati all'ASL o a terzi in relazione alla mancata osservanza delle vigenti norme tecniche, di sicurezza, d'igiene e sanitarie.

La ditta fornitrice si obbliga a dare immediata comunicazione all'Azienda di ogni circostanza che abbia influenza sull'esecuzione delle obbligazioni contrattuali.

Il fornitore contraente si impegna a mantenere i requisiti richiesti per l'affidamento dell'appalto in oggetto fino alla completa e perfetta esecuzione dello stesso e si impegna, altresì, a dare immediata comunicazione della sopravvenuta perdita dei requisiti di legge.

Le attività contrattuali da svolgersi presso le sedi aziendali dovranno essere eseguite senza interferire con il normale lavoro degli uffici; modalità e tempi dovranno comunque essere concordati con l'ASL di Pescara.

Il fornitore contraente si impegna ad avvalersi di personale specializzato che potrà accedere agli uffici dell'ASL nel rispetto di tutte le prescrizioni di sicurezza e di accesso, fermo restando che sarà cura ed onere del fornitore contraente acquisire e verificare preventivamente le relative procedure.

Il fornitore contraente è obbligato a consentire alla ASL di procedere, in qualsiasi momento e senza preavviso, alle verifiche della piena e corretta esecuzione delle prestazioni oggetto del contratto, nonché a prestare la propria collaborazione per lo svolgimento di tali verifiche.

ART. 13 Accettazione e collaudi

Il fornitore deve attenersi esclusivamente alla Procedura di Collaudo emessa dalla UOC Ingegneria Clinica denominata PCOL01 del 22/10/2024 ed approvata con Delibera n° 1850 del 09/12/2024. La

Procedura è consultabile sul sito aziendale www.asl.pe.it – sezione "documenti aziendali" e/o pagina Ingegneria Clinica-HTA.

ART. 14 Documentazione dei prodotti forniti

Dovrà essere garantita la disponibilità di manuali d'uso e manuali di service dei prodotti. Tale documentazione dovrà essere redatta o tradotta in lingua italiana.

In particolare, la società aggiudicataria si impegna a fornire gratuitamente, all'inizio della fornitura, quanto segue:

a) manuali di servizio del sistema offerto;

b) manuali d'uso, manutenzione e informazione sui rischi specifici (schede di sicurezza) dell'apparecchiatura e dei singoli reagenti, in lingua italiana;

c) precise indicazioni sulla scelta e sull'uso di idonei dispositivi di protezione individuale (D.P.I.) per gli addetti;

d) registro di manutenzione consigliato per interventi che possono essere eseguiti dall'utilizzatore;

e) formazione del personale preposto all'utilizzo dell'apparecchiatura, con eventuale utilizzo di materiale didattico e/o mezzi audiovisivi.

La ditta aggiudicataria dovrà inoltre fornire al dirigente responsabile del laboratorio o suo delegato, tutte le informazioni (marca, modello, matricola, codice Civab o CND, ecc.) dell'apparecchiatura fornita in formato elettronico.

ART. 15 Periodo di prova

La ASL di Pescara si riserva un congruo periodo di prova di 6 mesi consecutivi, decorrenti dall'avvenuto collaudo con esito positivo del sistema oggetto di fornitura, al fine di accertare la rispondenza dell'apparecchiatura, dei reagenti e dei relativi materiali di consumo a quanto dichiarato dalla ditta in sede di offerta, nonché la buona qualità della metodica, dei prodotti e della strumentazione forniti. Tale periodo decorrerà dalla data in cui gli strumenti saranno funzionanti, come riconosciuto dal verbale di collaudo.

Terminato tale periodo di prova, la U.O. utilizzatrice eseguirà il test-run della macchina, atto a verificare:

- precisione;
- accuratezza;
- operatività (test continuo);
- consumi effettivi.

Superato il suddetto test, il sistema analitico sarà considerato, a tutti gli effetti, idoneo e operativo.

Nel caso di esito negativo della prova, la ASL di Pescara si riserva la facoltà di concordare una ulteriore definitiva ripetizione per un periodo massimo di ulteriori tre mesi.

Nell'ipotesi di nuovo esito negativo, la ASL ha facoltà di risoluzione del contratto per inadempimento.

Nulla sarà dovuto al fornitore, ad eccezione dei pagamenti delle forniture riconosciute regolari, effettuate durante il periodo di prova e in ogni caso dopo l'avvenuto collaudo.

Qualora l'esito negativo della prova sia conseguenza di false dichiarazioni sottoscritte dalla ditta aggiudicataria nei documenti di gara, la ASL di Pescara tratterrà immediatamente la cauzione a disposizione, ferme restando le conseguenze penali e patrimoniali previste dalla legge e dal presente Capitolato.

Conseguentemente, con analoga procedura, si provvederà a favore della seconda ditta migliore offerente in graduatoria.

In caso di contestazioni, le verifiche saranno effettuate in contraddittorio con la ditta fornitrice.

ART. 16 Aggiornamento tecnologico

Qualora, durante il periodo di fornitura, la ditta aggiudicataria fosse in grado di commercializzare sistemi e dispositivi (apparecchiature, software, reagenti, materiali di consumo, ecc.) maggiormente evoluti e tecnologicamente più avanzati rispetto a quelli che hanno costituito oggetto del contratto, essa dovrà presentare alla ASL la proposta di aggiornamento tecnologico senza maggiorazione dei prezzi.
Gli aggiornamenti tecnologici dovranno essere concordati e autorizzati dalla stazione appaltante.

ART. 17 Norme di prevenzione e sicurezza

Nella fase di montaggio ed installazione della fornitura, nonché durante gli interventi di manutenzione, la ditta aggiudicataria deve adottare tutti gli accorgimenti più idonei a garantire l'incolumità delle persone addette ai lavori, nonché per evitare danni ai beni pubblici e privati.
La ASL è, pertanto, esonerata da ogni responsabilità per danni, infortuni o altro che dovesse accadere al personale della ditta aggiudicataria durante l'esecuzione della fornitura, convenendosi al riguardo che qualsiasi eventuale onere è compreso nel corrispettivo della fornitura stessa.
Il soggetto aggiudicatario è, altresì, pienamente responsabile degli eventuali danni arrecati, per fatto proprio o dei propri dipendenti, a cose e/o persone.
La ditta aggiudicataria sarà tenuta all'osservanza e all'applicazione di tutte le norme relative alle assicurazioni obbligatorie ed antinfortunistiche, previdenziali ed assistenziali, nei confronti del proprio personale dipendente che avrà accesso agli spazi e ai locali dell'Azienda. È tenuta, inoltre, su richiesta, a fornire evidenza dell'avvenuta stipula delle suddette polizze.
La ditta aggiudicataria dovrà ottemperare alle norme relative alla prevenzione degli infortuni e sarà tenuta al rispetto integrale e all'osservanza di tutte le disposizioni normative in materia di sicurezza sul lavoro (D. Lgs. n. 81/2008 e s.m.i.).
Il personale impiegato dall'impresa nell'appalto deve essere adeguatamente formato secondo i disposti dell'art. 37 del D.lgs. 81/2008, così come modificato dal D. L. n. 146/2021.

ART. 18 Inadempienze e penalità

Per tutta la durata del contratto sarà costantemente monitorata e verificata la qualità dei prodotti forniti.
Eventuali risultati negativi delle verifiche e dei controlli saranno contestati per iscritto dall'Azienda.
La ditta aggiudicataria avrà 10 giorni consecutivi dalla data di ricevimento della predetta comunicazione per prestare le proprie controdeduzioni. Nel caso in cui le stesse non siano ritenute soddisfacenti o nel caso in cui la ditta aggiudicataria non vi ottemperi entro il termine predetto, l'Azienda si riserva la possibilità di applicare una penale.
L'importo della penale verrà detratto dall'importo della fattura relativa al periodo in cui si sono verificate le inadempienze.
Fermo restando quanto previsto in materia di risoluzione del rapporto contrattuale, si stabilisce l'eventuale applicazione delle penali di seguito riportate:

- in caso di non rispondenza degli articoli forniti alle specifiche tecnico-merceologiche dichiarate dalla ditta aggiudicataria in sede di gara d'appalto e a quanto previsto dal capitolato: penale pari al 20% del valore della merce non rispondente, oltre alla richiesta di sostituzione;
- in caso di ritardo nella fornitura dell'apparecchiatura e/o del materiale di consumo: penale giornaliera pari allo 0,3 per mille del valore del contratto per ogni giorno solare di ritardo sulle consegne, fino a un massimo complessivo del 10% del valore del contratto, e con riserva degli eventuali ulteriori danni. Tale penale si applica anche in relazione al rispetto dei tempi di consegna pattuiti per la sostituzione della merce difforme;
- in caso di inadempienza o ritardo rispetto alle condizioni previste all'art. 6)- d) Servizi di assistenza tecnica e manutenzione, sarà applicata una penale giornaliera pari allo 0,3 per mille

del valore del contratto per ogni giorno solare di ritardo, fino a un massimo complessivo del 10% del valore del contratto, e con riserva degli eventuali ulteriori danni;

- in caso di trasporto non conforme alle temperature necessarie alla conservazione del prodotto: € 1.000,00 a trasporto, oltre all'obbligo di sostituzione della merce eventualmente danneggiata.

Le inadempienze sopra elencate devono intendersi a titolo meramente esemplificativo e non esaustivo. Pertanto, in tutti gli altri casi di contestazione di disservizi non espressamente previsti ai punti precedenti verrà applicata una penalità, variabile a seconda della gravità delle infrazioni contestate e del ripetersi delle stesse, fino a un importo massimo pari al 10% del valore del contratto, fatto salvo il risarcimento dei danni arrecati e la facoltà della ASL di Pescara di procedere alla risoluzione del contratto.

ART. 19 Rinvio

Per quanto non espressamente previsto dal presente capitolato speciale, si fa rinvio alla normativa vigente e ai restanti atti di gara.

ART. 20 Informazioni sul trattamento dei dati personali

Ai sensi dell'art. 13 del "*Regolamento UE n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*" (nel seguito anche "Regolamento UE"), la ASL di Pescara (nel seguito anche "ASL") fornisce le seguenti informazioni sul trattamento dei dati personali.

Estremi *identificativi* del titolare del trattamento dei dati e dati di contatto

Il Titolare del trattamento dei dati personali è la ASL di Pescara con sede in, Via R. Paolini, 47 - 65124 Pescara – email: protocollogenerale@asl.pe.it, PEC: protocollo.aslpe@pec.it

DATI DI CONTATTO DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della Protezione dei Dati (RPD) è raggiungibile al seguente indirizzo: ASL di Pescara, Via Battaglione Alpini, 1 – 65017 Penne (PE). email: dpo@asl.pe.it , PEC: dpo.aslpe@pec.it

Gli interessati «possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal [...] regolamento» (articolo 38, paragrafo 4 del Regolamento).

Finalità del trattamento

In relazione alle attività di rispettiva competenza svolta dalla ASL, si segnala che:

a)- i dati forniti dai concorrenti vengono acquisiti dalla ASL per verificare la sussistenza dei requisiti necessari per la partecipazione alla gara e, in particolare, delle capacità amministrative e tecnico-economiche di tali soggetti, richiesti per legge ai fini della partecipazione alla gara, per l'aggiudicazione nonché per la stipula del Contratto, per l'adempimento degli obblighi legali ad esso connessi, oltre che per la gestione ed esecuzione economica ed amministrativa del contratto stesso, in adempimento di precisi obblighi di legge derivanti dalla normativa in materia di appalti e contrattualistica pubblica.

b) tutti i dati acquisiti dalla ASL potranno essere trattati anche per fini di studio e statistici.

Base Giuridica del trattamento

Le basi giuridiche di riferimento per le finalità sopra indicate sono dettate dagli artt. 2-ter e 2-octies, par. 3, lett. h) del D.Lgs.196/2003 per come novellato dal D.Lgs. 101/2018 per l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto e dai seguenti articoli del Regolamento:

- art. 6.1 lettera b) – Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (art. 6.1.b del Regolamento). Infatti, ai sensi del Dlgs 36/2023 e s.m.i., la partecipazione alle procedure per l'affidamento di appalti e concessioni determina l'attivazione di rapporti contrattuali e precontrattuali con la stazione appaltante.
- art. 6.1 lettera e) - Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento
- art. 6.1 lettera c) - il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- art. 9.2 lettera g) - Il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'Interessato

Natura obbligatoria o facoltativa del conferimento dei dati

Il rifiuto di fornire i dati richiesti potrebbe determinare, a seconda dei casi, l'impossibilità di ammettere il concorrente alla partecipazione alla gara o la sua esclusione da questa o la decadenza dall'aggiudicazione, nonché l'impossibilità di stipulare il contratto.

Dati personali appartenenti a categorie particolari e dati personali relativi a condanne penali e reati

Di norma i dati forniti dai concorrenti e dall'aggiudicatario non rientrano tra i dati classificabili come appartenenti a categorie particolari, ai sensi dell'articolo 9, paragrafo 1, del Regolamento UE. I "dati personali relativi a condanne penali e reati" di cui all'art. 10 Regolamento UE sono trattati esclusivamente per valutare il possesso dei requisiti e delle qualità previsti dalla vigente normativa applicabile, ai fini della verifica dell'assenza di cause di esclusione ex art. 94 e segg. D. Lgs. n. 36/2023, in conformità alle previsioni di cui al codice appalti (D. Lgs. n. 36/2023) e al D.P.R. n. 445/2000. Tali dati sono trattati solo nel caso di procedure di appalto

Modalità del trattamento dei dati

Il trattamento dei dati verrà effettuato dalla ASL in modo da garantirne la sicurezza e la riservatezza necessarie e potrà essere attuato mediante strumenti manuali, informatici e telematici idonei a trattare i dati nel rispetto delle misure di sicurezza previste dal Regolamento UE.

Ambito di comunicazione e di diffusione dei dati

I dati potranno essere:

- trattati dal personale della ASL che cura il procedimento di gara o da quello in forza ad altri uffici che svolgono attività ad esso attinente o attività per fini di studio e statistici;

- comunicati a collaboratori autonomi, professionisti, consulenti, che prestino attività di consulenza od assistenza alla ASL in ordine al procedimento di gara, anche per l'eventuale tutela in giudizio, o per studi di settore o fini statistici;
- comunicati ad eventuali soggetti esterni, facenti parte delle Commissioni di aggiudicazione e di collaudo che verranno di volta in volta costituite;
- comunicati, ricorrendone le condizioni, al Ministero dell'Economia e delle Finanze o ad altra Pubblica Amministrazione, alla Agenzia per l'Italia Digitale, relativamente ai dati forniti dal concorrente aggiudicatario;
- comunicati ad altri concorrenti che facciano richiesta di accesso ai documenti di gara nei limiti consentiti ai sensi della legge 7 agosto 1990, n. 241;
- comunicati all'Autorità Nazionale Anticorruzione, in osservanza a quanto previsto dalla Determinazione AVCP n. 1 del 10/01/2008.

Il nominativo del concorrente aggiudicatario della gara ed il prezzo di aggiudicazione dell'appalto, potranno essere diffusi tramite il sito internet della ASL. Inoltre, le informazioni e i dati inerenti la partecipazione del Concorrente all'iniziativa di gara, nei limiti e in applicazione dei principi e delle disposizioni in materia di dati pubblici e riutilizzo delle informazioni del settore pubblico (D. Lgs. 36/2006 e artt. 52 e 68, comma 3, del D.Lgs. 82/2005 e s.m.i.), potranno essere messi a disposizione di altre pubbliche amministrazioni, persone fisiche e giuridiche, anche come dati di tipo aperto. Oltre a quanto sopra, in adempimento agli obblighi di legge che impongono la trasparenza amministrativa (art. 1, comma 16, lett. b, e comma 32 L. 190/2012; art. 35 D. Lgs. n. 33/2012; nonché art. 28 D. Lgs. n. 36/2023), il concorrente/contraente prende atto ed acconsente a che i dati e la documentazione che la legge impone di pubblicare, siano pubblicati e diffusi, ricorrendone le condizioni, tramite il sito internet della ASL.

I dati non saranno trasferiti al di fuori della CE/SEE.

Periodo di conservazione dei dati

Il periodo di conservazione dei dati è di 10 anni dall'aggiudicazione definitiva o dalla conclusione dell'esecuzione del contratto. Inoltre, i dati potranno essere conservati, anche in forma aggregata, per fini di studio o statistici nel rispetto degli artt. 89 del Regolamento UE e 110 bis del Codice in materia di protezione dei dati personali.

Processo decisionale automatizzato

Non è presente alcun processo decisionale automatizzato.

Diritti dell'interessato

Per "interessato" si intende qualsiasi persona fisica i cui dati sono trasferiti dal concorrente alla stazione appaltante.

All'interessato vengono riconosciuti i diritti di cui agli artt. da 15 a 22 del Regolamento UE.

Le basi giuridiche di riferimento per le finalità sopra indicate sono dettate dagli artt. 2-ter e 2-octies, par. 3, lett. h) del D.Lgs.196/2003 per come novellato dal D.Lgs. 101/2018 per l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto e dai seguenti articoli del Regolamento:

- art. 6.1 lettera b) – Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (art. 6.1.b del Regolamento). Infatti, ai sensi del Dlgs 36/2023 e s.m.i., la partecipazione alle procedure per l'affidamento di appalti e concessioni determina l'attivazione di rapporti contrattuali e precontrattuali con la stazione appaltante.
- art. 6.1 lettera e) - Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento
- art. 6.1 lettera c) - il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- art. 9.2 lettera g) - Il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'Interessato

Se in caso di esercizio del diritto di accesso e dei diritti connessi previsti dagli artt. da 15 a 22 del Regolamento UE, la risposta all'istanza non perviene nei tempi indicati o non è soddisfacente, l'interessato potrà far valere i propri diritti innanzi all'autorità giudiziaria (art. 79 del Regolamento UE) o rivolgendosi al Garante per la protezione dei dati personali - con sede in Piazza di Monte Citorio, n. 121, CAP 00186 Roma - mediante apposito reclamo. , come previsto dall'art. 77 del Regolamento UE.

Acquisite le sopra riportate informazioni, partecipando alla gara, il concorrente prende atto ed acconsente espressamente al trattamento dei dati personali come sopra definito.

Il concorrente si impegna ad adempiere agli obblighi di informativa e di consenso, ove necessario, nei confronti delle persone fisiche interessate di cui sono forniti dati personali nell'ambito della procedura di affidamento, per quanto concerne il trattamento dei loro dati personali da parte dell'Amministrazione per le finalità sopra descritte.

ART. 21 Disposizioni in materia di protezione dei dati personali e sicurezza delle informazioni
La Ditta aggiudicataria è tenuta a garantire che le attrezzature fornite abbiano caratteristiche tecniche compatibili con l'adozione delle misure di sicurezza per il trattamento dei dati personali con strumenti elettronici, come indicate nel Reg. UE 2016/679 sulla protezione dei dati (c.d. GDPR).

Sicurezza dei dati (art. 24 e 32 GDPR)

In particolare, nell'offerta tecnica si richiede di fornire indicazioni in merito ai seguenti punti e, per ognuno di essi, gli impegni da parte del fornitore previsti nell'offerta tecnica:
- Inventario dettagliato di moduli, apparecchiature e componenti del sistema e relative modalità di aggiornamento tempestivo in caso di modifiche/upgrade/sostituzioni (Configuration Management).
- Specifica indicazione nell'inventario di cui al punto precedente dell'eventuale presenza di moduli, componenti e servizi utilizzati dal sistema che siano esterni all'attrezzatura residente presso le strutture del committente (es.: servizi cloud, di monitoraggio, ecc…); per ognuno di questi moduli, componenti e servizi utilizzati dovranno essere forniti i relativi dettagli tecnici (es.: dati forniti, direzione in-out, modalità di autenticazione, ecc…)
- Per ogni modulo, componente e servizio del sistema presenza dell'eventuale contenuto di dati residenti *at rest* (es.: presenza di dischi su moduli degli analizzatori o su postazioni di lavoro ad essi asservite);

- Il/i tracciato/i dei dati utilizzato/i ai fini dell'esecuzione degli esami e nell'interscambio con il sistema applicativo LIS di laboratorio e/o verso servizi esterni (es.: monitoraggio);
- Interfacce fisiche delle attrezzature fornite (es.: ethernet), utilizzate nell'ambito del progetto e possibilità di disabilitazione delle interfacce non utilizzate; i collegamenti utilizzati dovranno essere ridondati al fine di limitare l'eventuale interruzione di servizio a causa del malfunzionamento di una interfaccia;
- Descrizione architettura generale della soluzione fornita riportante i dettagli di tutte le attrezzature, dei servizi e dei moduli componenti e degli interfacciamenti verso sistemi/moduli/servizi utilizzati (es.: LIS, sistema di monitoraggio, ecc…)
- Modalità di gestione del processo IAM (Identity and Access Management), sia per le utenze applicative che per le utenze di servizio (es.: interazioni con il sistema LIS e con eventuali servizi esterni) e relativi criteri di sicurezza configurabili; riportare in dettaglio le modalità amministrative di gestione e gli aspetti relativi alla gestione delle autorizzazioni. Indicare la possibilità di poter applicare criteri di *least privilege* a tutte le tipologie di utenze, anche di servizio; attestare che le utenze siano: a) individuali e che sia necessario autenticarsi prima di trattare i dati personali; b) associate ad uno o più profili di autorizzazione;
- Modalità di applicazione di soluzioni di cifratura (*at rest, in transit*) e pseudonimizzaizone dei dati (descrizione eventuale architettura delle soluzioni adottate); Indicazione dei protocolli e delle modalità di gestione delle chiavi;
- Modalità di gestione dei servizi di manutenzione (presso la sede del committente e da remoto): saranno consentite interazioni con il sistema dall'esterno della rete della ASL di Pescara esclusivamente attraverso il sistema VPN messo a disposizione dal committente e secondo le policies aziendali.
- Generazione del log funzionale (tracciamento e registrazione di tutti i tipi di operazioni svolte dalle utenze – anche di servizio – che accedono al sistema tramite le credenziali attribuite) e del log tecnico (tracciamento e registrazione di tutti i tipi di operazioni svolte dagli amministratori di sistema / manutentori che accedono all'applicazione tramite le credenziali attribuite); Possibilità di raccolta di tali log tramite soluzioni di log management da parte del Committente;
- Soluzioni, tecniche e protocolli disponibili per la comunicazione (interscambio e interfacciamento tra i sistemi componenti l'architettura generale del sistema fornito e tra il sistema ed il sistema LIS di laboratorio);
- Modalità di gestione delle configurazioni sicure e dell'*hardening* di tutte le componenti del sistema (anche PC asserviti);
- Modalità di gestione delle vulnerabilità tecniche di sistema e del patch management (con particolare riferimento alla loro installazione/disinstallazione
- Modalità di gestione degli upgrade (es.: software/firmware) per finalità di aggiornamento normativo e di sicurezza.
- Soluzioni di monitoraggio dello stato dei sistemi
- Metodologie di ingegnerizzazione sicura dei sistemi utilizzate per lo sviluppo ed il testing (*Security & Privacy by Design e by Default, defence in depth, default deny, fail securely, least privilege*).
- Eventuale impiego di tool atti a verificare la correttezza del codice riducendo le vulnerabilità.
- Eventuale certificazione ISO 9001 dei processi di sviluppo e manutenzione.
- Modalità di gestione delle personalizzazioni in termini di compatibilità con la linea di produzione standard: descrizione delle modalità esecutive di processo.
- Modalità previste per la garanzia di continuità operativa del sistema secondo gli SLA (Service Level Agreement) concordati con il Committente.
- Modalità di gestione di eventuali incidenti/data breach (anche di eventuali servizi esterni utilizzati nell'ambito della fornitura di servizi al Committente) e fornitura di supporto al per la gestione di tali eventi.

Relativamente a possibili violazioni dei dati personali (c.d. Data Breach), si precisa che nel caso l'applicazione software di gestione/supporto/monitoraggio del sistema sia erogata parzialmente o totalmente da remoto (es.: servizi SaaS o Hosting), il Fornitore è tenuto a dettagliare i servizi ed i dati che vengono comunicati all'esterno comunicare tempestivamente al Committente qualunque malfunzionamento (disponibilità) o violazione dei sistemi e della infrastruttura che li ospita.

Fornire evidenza dell'eventuale certificazione del sistema software come Dispositivo Medico e indicazione delle specifiche misure di sicurezza adottate in base alla Regolamentazione europea vigente.

Le eventuali attività di monitoraggio ed assistenza condotte da remoto così come l'utilizzo di apparecchiature, strumenti, device, connessioni, ecc... da parte del personale tecnico del fornitore dovrà essere conforme alle policies aziendali di sicurezza per i fornitori; in particolare l'esecuzione delle attività di assistenza tecnica e monitoraggio da remoto saranno possibili esclusivamente mediante connessione VPN garantita dalle infrastrutture della ASL di Pescara e con le limitazioni imposte dalle policies organizzative adottate.

L'eventuale sostituzione di moduli e componenti del sistema che contengano dati dovrà avvenire in maniera conforme alle policies aziendali di sostituzione (nel caso di presenza di hard disks – HDD/SSD, questi dovranno essere sostituiti e le parti sostituite consegnate alla UOC Sistemi Informativi per la relativa distruzione fisica).

Il sistema, articolato nelle sue varie componenti, verrà periodicamente sottoposto a Vulnerability Assessment da parte del Committente per la verifica della presenza di vulnerabilità; gli eventuali rilievi saranno comunicati al fornitore tramite specifico report e dovranno essere sanati:

- entro 30 giorni in caso di vulnerabilità non critiche;
- entro 7 giorni in caso di vulnerabilità critiche (salvo specifiche disposizioni del Committente legate alle particolari caratteristiche di urgenza – es.: distacco dalla rete del sistema).

Le modalità di gestione operativa del servizio dovranno essere concordate con il referente dell'Amministrazione al fine di garantire una opportuna gestione delle utenze con accesso privilegiato che dovranno essere profilate in maniera dettagliata.

Per tutto quanto non previsto nelle misure indicate, è necessario fare riferimento alle policies aziendali.

Diritti degli interessati (Capo III GDPR)
Circa i diritti degli interessati si richiede di sapere se il Fornitore abbia implementato (o intenda implementare) specifiche funzionalità in grado di supportare le operazioni di esercizio dei diritti degli interessati, darne evidenza all'Interessato e lasciarne traccia (es.: mediante opportuna registrazione); si richiede inoltre di sapere quali misure il fornitore abbia implementato (o intenda implementare) per fornire assistenza al Committente per garantire il riscontro alla richieste di esercizio dei diritti degli interessati.

ART. 22 Responsabile del trattamento dei dati
Nell'ambito dell'attività oggetto del contratto, l'appaltatore potrà venire a conoscenza e trattare dati comuni e sensibili relativi ai servizi offerti agli utenti della stazione appaltante.
L'appaltatore pertanto ai sensi dell'art. 28 del Regolamento UE, è nominato, con apposito atto, Responsabile del trattamento dei dati, per gli adempimenti previsti nel contratto, nei limiti e per la durata dello stesso.

ART. 23 Principi, diritti e misure tecniche e organizzative - requisiti/schede di audit
Si indicano, in base alla loro applicabilità in relazione al servizio erogato per conto del Titolare, i principi di trattamento, le misure di sicurezza e i diritti degli interessati, secondo le indicazioni del Regolamento UE 2016/679, del D.Lgs. 196/2003 (così come modificato dal D.Lgs. 101/2018) unitamente alle misure di sicurezza previste, per i quali il responsabile si impegna con la sottoscrizione del contratto.
Le indicazioni fornite nel presente allegato relative alle misure di sicurezza sono estrapolate dalle Linee Guida ENISA relative alla sicurezza dei trattamenti di dati personali: esse dovranno essere riportate all'interno del Registro dei Trattamenti del Responsabile.

1) Principi di Trattamento e Diritti degli Interessati

Req.	**Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016)**
A.1	Art. 5.1.b – Misure per garantire la limitazione della finalità del trattamento (dati non utilizzati per altre finalità)
A.2	Art. 5.1.c – Misure per garantire la minimizzazione dei dati del trattamento
A.3	Art. 5.1.d – Misure per garantire la esattezza/qualità dei dati
A.4	Art. 5.1.e – Misure per garantire la limitazione della conservazione
A.5	Art. 15 – Misure per garantire il diritto di Accesso dell'interessato
A.6	Art. 16 – Misure per garantire il diritto di Rettifica
A.7	Art. 17 – Misure per garantire il diritto alla Cancellazione ("Oblio") – ove applicabile
A.8	Art. 18 – Misure per garantire il diritto alla Limitazione del Trattamento
A.9	Art. 19 – Misure per garantire l'obbligo di Notifica in caso di rettifica o cancellazione dei dati personali o limitazione del Trattamento
A.10	Art. 20 – Misure per garantire il diritto alla portabilità dei dati – ove applicabile
A.11	Art. 21 – Misure per garantire il diritto di Opposizione
A.12	Art. 22 - Misure per garantire la sicurezza in caso di processo decisionale automatizzato relativo alle persone fisiche, compresa la *profilazione*

2) Misure di Sicurezza

Il perimetro di sicurezza definito come ambito di applicazione delle misure di sicurezza di seguito elencate è costituito dal servizio effettuato dal Responsabile per conto della ASL di Pescara; di conseguenza le seguenti misure sono applicabili all'organizzazione, alle informazioni/dati, agli strumenti HW, SW e di rete ed al personale coinvolti nell'erogazione del servizio contrattualizzato.

Le presenti misure di sicurezza verranno utilizzate quale riferimento per l'esecuzione degli audit previamente concordati.

CATEGORIA (ENISA)	**ID MISURA**	**DESCRIZIONE DELLA MISURA**
Politiche di sicurezza e procedure per la protezione dei dati personali	1.1	Il Responsabile deve disporre di una propria regolamentazione (o politica di sicurezza) in materia di protezione dei dati personali conforme alla normativa vigente e che disciplini i servizi erogati per conto del Titolare.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	1.2	La regolamentazione di cui al punto precedente deve essere riesaminata e aggiornata almeno su base annuale.
	1.3	La regolamentazione deve essere approvata dalla Direzione e comunicata a tutti i dipendenti e alle parti esterne interessate.
	1.4	La regolamentazione deve disciplinare almeno i seguenti punti: ruoli e responsabilità del personale, misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, per i responsabili e sub-responsabili del trattamento dei dati e per le altre terze parti coinvolte nel trattamento dei dati personali.
Ruoli e responsabilità	2.1	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con la politica di sicurezza.
	2.2	Durante le riorganizzazioni interne o le cessazioni e il cambio di impiego, devono essere chiaramente definite le modalità di revoca dei diritti e delle responsabilità con le rispettive procedure di passaggio di consegne.
	2.3	Deve essere effettuata una chiara individuazione e designazione delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
Riservatezza del personale	3.1	Il Responsabile deve garantire che tutto il personale comprenda le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità devono essere chiaramente comunicati durante la fase di attivazione del Servizio/Contratto.
	3.2	Prima di assumere i propri compiti, il personale del Responsabile deve essere invitato a riesaminare e concordare la Regolamentazione di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
Formazione	4.1	Il Responsabile deve garantire che tutto il personale sia adeguatamente formato sui controlli di sicurezza previsti per il servizio e per gli eventuali sistemi informatici ad esso correlati. Il personale coinvolto nel trattamento dei dati personali deve inoltre essere adeguatamente informato e periodicamente aggiornato in merito ai requisiti in materia di protezione dei dati e agli obblighi previsti dalla normativa vigente attraverso regolari campagne di sensibilizzazione.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	4.2	Il Responsabile deve disporre programmi di formazione (relativi alla protezione dei dati personali e alla sicurezza delle informazioni) strutturati e regolari per il proprio personale, compresi programmi specifici per l'inserimento di eventuali nuovi arrivati (es.: job rotation, nuove assunzioni, ecc...).
Politica controllo accessi	5.1	Specifici diritti di accesso devono essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.
	5.2	Deve essere definita una politica di controllo degli accessi. Nel documento l'organizzazione deve determinare le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.
	5.3	La segregazione dei ruoli per gestire il controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi) dovrebbe essere chiaramente definita e documentata.
Controllo accessi e autenticazione	6.1	Ove fornita dall'Organizzazione, deve essere attuata la politica di controllo accessi applicabile a tutti gli utenti che accedono ai sistemi IT, con particolare riguardo agli aspetti relativi alla creazione, approvazione, riesame ed eliminazione degli account.
	6.2	L'uso di account generici (non personali) deve essere evitato. Nei casi in cui ciò sia necessario, l'utilizzo deve essere autorizzato dal referente dell'Organizzazione. Qualora tale autorizzazione fosse fornita, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.
	6.3	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio, deve essere presente un meccanismo di autenticazione che consenta l'accesso che sia in linea con la politica di controllo degli accessi ove fornita dall'Organizzazione. Come minimo deve essere utilizzata una combinazione di user-id e password.
	6.4	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio, il sistema di controllo degli accessi deve essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano i criteri definiti al punto precedente.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	6.5	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio deve essere possibile configurare i seguenti parametri relativi alle password: complessità, maximum age, password history, lunghezza e il numero di tentativi di accesso non riusciti accettabili. I criteri dovranno essere concordati con il referente dell'Organizzazione (in base alla politica di controllo accessi).
Gestione risorse e degli asset	7.1	Deve essere predisposto un registro delle risorse IT utilizzate per il trattamento dei dati personali (hardware, software e rete), in funzione di quanto applicabile al servizio esternalizzato. Il compito di mantenere e aggiornare il registro deve essere esplicitamente assegnato.
	7.2	Le risorse IT all'interno del registro essere riesaminate e aggiornate regolarmente.
	7.3	I ruoli che hanno accesso alle risorse devono essere definiti e documentati. In particolare devono essere definite le responsabilità in relazione alle risorse.
Sicurezza fisica	8.1	Il perimetro fisico dei locali in cui è ospitata l'infrastruttura IT utilizzata a fini di erogazione del servizio o vengono effettuati trattamenti di dati personali del Titolare deve essere accessibile esclusivamente a personale esplicitamente autorizzato da parte del Responsabile.
	8.2	Il personale autorizzato all'accesso ai locali di trattamento o ai locali in cui è ospitata l'infrastruttura IT per l'erogazione del servizio deve essere dotato di strumenti di identificazione personali (es. badge identificativi, PIN personali).
	8.3	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Deve essere mantenuto e monitorato in modo sicuro un registro fisico o una traccia elettronica del controllo di tutti gli accessi.
	8.4	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.
	8.5	Dovrebbero essere predisposte barriere fisiche per impedire l'accesso fisico non autorizzato.
	8.6	Le aree dei locali non usate dovrebbero essere fisicamente bloccate e periodicamente riesaminate.
	8.7	Nella sala server devono essere predisposti opportuni sistemi antincendio automatici, sistemi dedicati di

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
		climatizzazione e gruppi di continuità (UPS) che garantiscano l'erogazione sicura del servizio secondo quanto stabilito contrattualmente.
	8.8	Il personale di supporto esterno deve avere accesso limitato alle aree protette.
Change management	9.1	L'organizzazione deve adottare un processo di cambiamento che consenta di assicurarsi che tutte le modifiche al sistema/servizio siano opportunamente registrate (anche con eventuali aggiornamenti dell'inventario delle risorse) e monitorate.
	9.2	Ogni Cambiamento al sistema/servizio deve essere previamente segnalato al referente interno dell'organizzazione (committente) e da questi autorizzato. Nella segnalazione devono essere documentati: gli estremi del cambiamento (es.: cambiamento di versione), le tempistiche, eventuali prescrizioni aggiuntive che prevedano azioni da adottare prima che il cambiamento sia operativo (es.: formazione utenti).
	9.3	Lo sviluppo del software deve essere eseguito in un ambiente speciale, non collegato al sistema IT utilizzato per il trattamento dei dati personali in produzione. Quando è necessario eseguire i test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, il fornitore deve predisporre specifiche procedure per la protezione dei dati personali utilizzati nei test.
Logging e monitoraggio	10.1	I log devono essere attivati per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).
	10.2	I log devono essere registrati e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi devono essere sincronizzati con un'unica fonte temporale di riferimento (server NTP).
	10.3	È necessario registrare le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / eliminazione / modifica dei diritti di accesso degli utenti.
	10.4	Non deve essere possibile la cancellazione o modifica del contenuto dei log. Anche l'accesso ai log deve essere registrato oltre al monitoraggio effettuato per la rilevazione di attività insolite.

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	10.5	Deve essere configurato un sistema di monitoraggio per l'elaborazione dei log e la produzione di rapporti sullo stato del sistema e notifica di potenziali allarmi.
Protezione dal malware	12.1	Devono essere attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti
Backup	14.1	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità; devono essere definite e documentate le strategie di backup da applicare ai dati in maniera coerente con il livello di criticità (RPO) dei servizi a cui afferiscono
	14.2	Ai backup deve essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
	14.3	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.
	14.4	Le strategie di backup definite devono essere completate regolarmente.
	14.5	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati.
	14.7	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.
	14.8	Se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa dal titolare dei dati.
Sicurezza Server e Database	15.1	I database e application server devono essere configurati affinché lavorino con un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
	15.2	I database e application server devono elaborare solo i dati personali che sono effettivamente necessari per l'elaborazione al fine di raggiungere i propri scopi di elaborazione.
	15.3	Nei sistemi utilizzati per l'erogazione del servizio, devono essere considerate soluzioni di crittografia per i dati at rest, in transit e in use. Qualora non ritenute applicabili, deve essere data adeguata (documentata) motivazione e devono essere adottate misure

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
		compensative che consentano di proteggere i dati trattati
	15.4	Nei sistemi utilizzati per l'erogazione del servizio, ove possibile, devono essere applicate tecniche di pseudonimizzazione attraverso la separazione dei dati dagli identificatori al fine di evitare il collegamento diretto con l'interessato. In caso non fosse possibile, deve essere fornita adeguata (documentata) motivazione e devono essere adottate misure compensative che consentano di proteggere i dati trattati.
Network/Communication security	16.1	Deve essere predisposta e monitorato il rispetto di una policy per la Sicurezza di Rete (Network Security Policy) e per la gestione delle Comunicazioni Sicure (Network Communication Security) che preveda l'adozione di misure di cifratura delle comunicazioni nell'ambito dei processi di trattamento effettuati (TLS/Https, VPN, SSH, ecc...).
Sicurezza desktop/laptop/mobile	17.1	Gli utenti non devono essere in grado di disattivare o aggirare le impostazioni di sicurezza.
	17.2	Le applicazioni anti-virus e le relative signatures devono essere configurate regolarmente in maniera continuativa.
	17.3	Gli utenti non devono avere i privilegi per installare applicazioni software non autorizzate o disattivare applicazioni autorizzate
	17.4	I sistemi utilizzati per l'erogazione del servizio, devono disporre di un timeout di sessione nel caso in cui l'utente non sia stato attivo per un determinato periodo di tempo (max 10 min).
	17.5	Gli aggiornamenti critici di sicurezza rilasciati dalle case produttrici di software di sistema devono essere installati regolarmente.
	17.6	Non è consentito il trasferimento di dati personali dai Database dei sistemi aziendali alle workstation utilizzate a fini di assistenza tecnica, se non previa esplicita autorizzazione del Responsabile dei Sistemi Informativi. I dati temporaneamente memorizzati devono essere cancellati alla fine della sessione di lavoro.
	17.7	Non deve essere consentito il trasferimento di dati personali da workstation a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	17.8	Deve essere abilitata la crittografia dei dischi delle postazioni di lavoro/laptop/device mobili utilizzate nell'ambito dell'erogazione del servizio
Dispositivi portatili	18.1	Le procedure di gestione dei dispositivi mobili e portatili devono essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
	18.2	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati: non è consentito l'utilizzo di dispositivi personali, salvo eventuali specifiche autorizzazioni.
	18.3	I dispositivi mobili devono essere soggetti alle stesse procedure di controllo degli accessi (al sistema IT) delle altre apparecchiature terminali (client).
	18.4	Il Responsabile deve individuare e comunicare al Titolare un proprio referente a cui attribuire la responsabilità della gestione dei dispositivi mobili e portatili utilizzati nell'ambito dell'erogazione del servizio.
	18.5	Il Responsabile deve essere in grado di cancellare da remoto i dati personali su un dispositivo mobile compromesso, nel caso in cui questo sia utilizzato nell'ambito dell'erogazione del servizio.
	18.6	In caso di utilizzo promiscuo dei dispositivi mobili (fini di erogazione del servizio al titolare e fini privati) deve essere prevista, mediante opportuni software containers sicuri, la separazione dell'uso privato dall'uso aziendale del dispositivo.
	18.7	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
Sicurezza del ciclo di vita delle applicazioni	19.1	Lo sviluppo degli applicativi deve essere conforme alle linee guida per lo sviluppo del software sicuro nella pubblica amministrazione pubblicate da AGID.
Sub-responsabile del trattamento	20.1	Il Responsabile ed i suoi sub-responsabili adottano le linee guida e le procedure relative al trattamento dei dati personali contenute nell'atto di designazione e nei suoi allegati (tra cui il presente documento).
	20.2	Il Responsabile del Trattamento deve osservare le indicazioni fornite nell'atto di designazione in caso di violazione di dati personali e nelle presenti misure di sicurezza.
	20.3	Il Responsabile deve sottoscrivere l'atto di designazione in cui sono contenuti requisiti formali e

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
		obblighi. Il Responsabile del trattamento deve, in risposta, fornire prove documentate sufficienti di conformità (es.: certificazioni di sicurezza, schede tecniche relative alle misure di sicurezza adottate per il servizio/sistema): in caso alternativo, verrà adottata una specifica politica di auditing.
	20.4	Il Responsabile dovrebbe verificare regolarmente la conformità del sub-responsabile al livello concordato di requisiti e obblighi.
	20.5	Il personale del responsabile del trattamento che elabora dati personali deve essere soggetto a specifici accordi documentati di riservatezza / non divulgazione.
Gestione degli incidenti / Violazione dei dati personali	21.1	Il Responsabile deve predisporre un proprio piano di risposta agli incidenti con procedure dettagliate che preveda la comunicazione al titolare (committente), secondo le indicazioni fornite nell'atto di designazione, al fine di garantire una risposta efficace e ordinata agli incidenti e violazioni relativi ai dati personali.
	21.2	Le violazioni dei dati personali, di competenza del Titolare, devono essere segnalate immediatamente alla Direzione. In qualità di Responsabile devono essere adottate specifiche procedure di supporto al Titolare per la notifica e la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR.
	21.3	La procedura di gestione delle violazioni di cui al punto precedente, deve essere documentata: essa deve includere un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.
	21.4	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione eseguite.
Business Continuity	22.1	Il Responsabile deve predisporre un proprio Piano di Continuità Operativa (BCP - Business Continuity Plan) in relazione all'erogazione dei servizio, in linea con quanto previsto dall'Organizzazione (Committente). Tale Piano deve stabilire procedure e controlli da seguire al fine di garantire il livello richiesto di continuità e disponibilità del servizio (ad es.: in caso di incidente / violazione dei dati personali o interruzione del servizio).

CATEGORIA (ENISA)	ID MISURA	DESCRIZIONE DELLA MISURA
	22.2	Il Piano di Continuità Operativa indicato al punto precedente deve includere azioni chiare e assegnazione di ruoli.
	22.3	Il Piano di Continuità Operativa deve essere in linea con il livello di qualità del servizio da garantire all'Organizzazione (Committente), con particolare riguardo alla sicurezza dei dati personali dei processi fondamentali di erogazione.
Cancellazione/eliminazione dei dati	23.1	I supporti di memorizzazione da dismettere devono essere distrutti fisicamente; in caso in cui ciò non sia possibile (es.: per indicazioni contrattuali relative all'assistenza dei dispositivi), prima della loro eliminazione (o riconsegna al fornitore) devono essere sottoposti a tecniche di distruzione dei dati (es.: ripetute operazioni di sovrascrittura con tecniche di clearing/purging).
	23.2	La distruzione di documenti deve avvenire mediante opportuni dispositivi di triturazione.
	23.3	Se sono utilizzati servizi di terzi per eliminare in modo sicuro i supporti di memorizzazione o documenti cartacei, è necessario stipulare uno specifico contratto di servizio e produrre un formale attestato di distruzione.

Data 27 / 11 / 2025

IL COLLEGIO TECNICO

Dott. Giancarlo Di Iorio _____

Dott.ssa Annamaria Facciolini _____

Dott. Paolo De Cono _____