

UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

Il dirigente della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

in virtù della delega conferita con deliberazione N°232/2015

HA ASSUNTO LA PRESENTE DETERMINAZIONE

N. 266 del 29/03/2024

**OGGETTO: AFFIDAMENTO, TRAMITE TRATTATIVA MEPA, AI SENSI DELL'ART.50
COMMA 1 LETT.B DEL D.LGS. 36/2023, DEL SERVIZIO EROGATO COME SAAS DEL SI-
STEMA DI SICUREZZA INFORMATICA CYBER DEFENCE DENOMINATO CERBEYRA
AI FINI DELL'ADEGUAMENTO AL REGOLAMENTO EUROPEO N.2016/79 DEL 27 GIU-
GNO 2016 (GDPR "GENERAL DATA PROTECTION REGULATION") – PERIODO
01/03/2024 – 28/02/2025 - CIG: B0CD0F2734**

Esercizi/o e conto 2024-2025 502020106 Centri/o di costo 1000115

- **Importo presente Atto: € 26.840,00**

- **Importo esercizio corrente: € 22.366,70**

Budget

- **Assegnato: € -**

- **Utilizzato: € -**

- **Residuo: € -**

Autorizzazione n°: 2024/1 sist inf

Servizio Risorse Economiche: **Giovanna Evangelista**

UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici Proposta n° DT-269-2024

L'estensore

Silvia Placidi

Il Responsabile del Procedimento

Giuseppe Navanteri

**Il Dirigente della UOSD Ingegneria Clinica e Tec-
nologie e Sistemi Informatici**

Giuseppe Navanteri

La presente determinazione si compone di n° 9 pagine e dei seguenti allegati che ne formano parte integrante e sostanziale:

Allegato 1 composto da num. 5 pagine

Allegato 2 composto da num. 3 pagine

Il Dirigente della UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici

- Visto il decreto legislativo 30.12.1992, n. 502 e successive modificazioni ed integrazioni;
- Visto il decreto legislativo 16.10.2003, n. 288 e il decreto legislativo 23.12.2022, n. 200 “Riordino della disciplina degli Istituti di ricovero e cura a carattere scientifico”;
- Vista la legge regionale 23.01.2006, n. 2;
- Visto l’Atto Aziendale adottato con deliberazione n. 153 del 19.02.2019 ed approvato dalla Regione Lazio con DCA n. U00248 del 02.07.2019, modificato e integrato con la delibera 1254 del 02.12.2020, n.46 del 21/01/2021 e n.380 del 25/03/2021, approvate dalla Direzione Salute ed Integrazione Sociosanitaria della Regione Lazio, con Determinazione n.G03488 del 30/03/2021;
- Vista la deliberazione IFO n. 1 del 2.01.2024 di insediamento del Direttore Generale f.f. Dott.ssa Laura Figorilli;
- Viste le deliberazioni n. 212 del 16.03.2022 e n. 154 del 28.02.2022 con le quali sono stati nominati rispettivamente la Dott.ssa Laura Figorilli quale Direttore Amministrativo ed il Dott. Ermete Gallo quale Direttore Sanitario degli Istituti Fisioterapici Ospitalieri;
- Visto il D.M. del Ministero della Salute del 8 maggio 2020 di conferma del riconoscimento del carattere scientifico dell’IRCCS di diritto pubblico a Istituti Fisioterapici Ospitalieri (IFO) relativamente alla disciplina di “oncologia” per l’Isti-

tuto Nazionale Tumori Regina Elena (IRE) e alla disciplina di “dermatologia” per l’Istituto San Gallicano (ISG);

Visto il D.Lgs n.36 del 31 marzo 2023 s.m.i., avente ad oggetto “Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici”;

Premesso che con l’entrata in vigore del Regolamento Europeo 2016/79 del 27 giugno 2016 (GDPR “General Data Protection Regulation”), l’U.E. ha uniformemente regolamentato la materia della protezione delle persone fisiche con riguardo al trattamento dei dati personali;

che con circolare AgID n. 1/2017 del 17 marzo 2017 recante: “Misure minime di sicurezza ICT per le pubbliche amministrazioni (DPCM 1 agosto 2015)” indica alle pubbliche amministrazioni le misure minime per la sicurezza ICT da adottare entro tempistiche circoscritte, al fine di proteggere il patrimonio informatico ed i dati gestiti al suo interno, da eventuali minacce più comuni e frequenti cui sono soggetti i sistemi informativi”;

Preso atto in particolare, della nuova regolamentazione giuridica della privacy di che tratta che prevede un cambio radicale nell’impostazione della tutela dei dati personali, che dovrà concretizzarsi in un “modello organizzativo” da implementare in ragione di un’attenta analisi dei rischi e a seguito di un’autovalutazione finalizzata all’adozione delle migliori strategie volte a presidiare i trattamenti di dati effettuati in ottica di privacy by design e privacy by default, e cioè in base a un approccio non più di tipo formale o limitato alla mera adozione di misure di sicurezza, ma a un sistema organizzativo caratterizzato da un’attenzione multidisciplinare alle specificità della struttura e della tipologia di trattamento, sia dal punto di vista della sicurezza informatica, sia in conformità agli obblighi legali;

Considerato che i principali elementi da implementare rispetto all’attuale quadro normativo sono così riassumibili:

- 1) Diritti degli interessati (conoscitivi e di controllo), dati personali e trattamenti
- 2) Obblighi dei titolari del trattamento e organizzazione
- 3) Adozione di specifiche policy e documenti interni
- 4) Semplificazioni di compliance interna
- 5) Misure di sicurezza

Considerata

pertanto la necessità degli IFO di adeguare i propri sistemi in modo da essere in linea con la normativa nell'adottare nuove regole riguardanti il trattamento, la gestione e la protezione dei dati personali, in conformità al soprarichiamato Regolamento EU sulla privacy (GDPR) sia mediante l'innalzamento del proprio livello informatico e sia mediante l'individuazione di eventuali interventi correttivi;

che con la creazione della rete telematica è stato costruito un modello topologico che ha visto gli IFO come snodo di collegamento della rete locale verso il mondo Internet e questo ha richiesto che nella realizzazione di tale rete fossero acquisiti e configurati adeguati apparati di protezione per la sicurezza dei dati di questo Ente;

che il sistema di sicurezza informatica dell'Ente è negli anni sempre più importante e cruciale per via della crescente informatizzazione dei servizi che vede una maggiore esposizione alla rete internet per l'accesso alle banche dati esterne e della parallela diffusione e specializzazione delle minacce alla sicurezza;

che attualmente la rete interna degli IFO garantisce:

- l'accesso alla rete interna e alla navigazione a circa 1800 postazioni utenti, tra collaboratori interni ed esterni all'Istituto che operano dagli uffici e/o da remoto e tutti necessitano costantemente di accedere a banche dati raggiungibili mediante internet
- l'accesso a sistemi informativi
- servizio di firewall per la rete interna

- protezione del servizio di posta elettronica

Dato atto

che la sicurezza informatica è vista come un'emergenza a tutti i livelli istituzionali e rappresenta una priorità all'interno delle strategie di sviluppo dell'Unione Europea in considerazione delle capacità di penetrazione degli attacchi cyber e cibernetici;

che risulta quindi necessario affrontare in modo strutturato l'approccio alla riduzione del rischio informatico, a fronte di numerose e sempre più crescenti violazioni informatiche ai danni di aziende pubbliche e private attraverso l'utilizzo delle dovute risorse tecnologiche e organizzative nonché di competenze, con l'obiettivo di governare le identità, rilevare le minacce, proteggere i dati, ripristinare i sistemi e poter garantire la continuità operativa dei servizi essenziali che eroga l'Ente;

che, in particolare, è stato implementato uno strumento di firewall che ha garantito in questi anni la protezione della rete dalle minacce alla sicurezza e, vista la criticità del servizio, era stato individuato un prodotto leader di mercato, denominato CERBEYRA ed erogato dalla società VOLA SPA, che offrì tutte le migliori garanzie di sicurezza e stabilità;

che non si può pertanto rischiare il malfunzionamento del principale strumento utilizzato per la sicurezza perimetrale della rete;

Verificato

che tali servizi professionali e tecnologici, sono estremamente necessari per il monitoraggio e l'analisi continua dei dati e degli eventi di sicurezza a protezione del patrimonio informativo aziendale e intendono supportare gli IFO per tutte le fasi della gestione del rischio cyber (Identity, Protect, Detect, Respond, Recover) al fine di:

- Rafforzare le misure tecniche per la protezione dei propri asset e dei propri servizi digitali

- Aumentare le capacità di rilevazione e contrasto degli incidenti di sicurezza
- Sensibilizzare e rendere consapevole tutto il personale in servizio su rischi e minacce cibernetiche
- Accrescere le competenze specifiche dello staff tecnico
- Rivedere e migliorare la compliance al GDPR, anche alla luce di vari interventi di riorganizzazione interna

Preso atto

che attraverso il servizio di Cyber Security, denominato CERBYRA e fornito dalla società VOLA SPA, si contribuisce all'analisi tecnica per stabilire quali azioni intraprendere al fine di ridurre, per quanto possibile, il rischio di attacchi o manomissioni alle componenti hardware e software installate nei vari uffici dell'Ente;

che CERBYRA è una piattaforma certificata AGID (Agenzia per l'Italia digitale) ed offre un'attività di analisi continua a difesa delle informazioni e del dominio ciberneticò per mantenere al sicuro le informazioni critiche necessarie degli IFO;

che la piattaforma CERBYRA offre i suoi servizi in modalità SaaS (Software as a Service), e la sua interfaccia user friendly permette di monitorare, con grafici e report, l'andamento delle vulnerabilità ed implementare soluzioni e proposte per risolvere le criticità dei sistemi e delle applicazioni web attraverso:

- **Vulnerability Assessment** che consente di identificare le vulnerabilità presenti su siti e applicativi web, reti, host interni e rete intranet
- **Cyber Feed e Cyber Reputation** che permette di controllare costantemente il World Wide Web alla ricerca di informazioni su specifici assets
- **Cyber Control Center** che garantisce un supporto alla sicurezza delle postazioni di lavoro dei dipendenti e dei collaboratori che lavorano da remoto al di fuori della rete aziendale

- **Asset Management** che consente di realizzare un inventario delle proprie risorse e dispositivi hardware e software per gestire al meglio le risorse ICT evitando sprechi
- **Threat Intelligence** che permette di ottenere informazioni reali sui sempre più sofisticati attacchi informatici

Constatato	che occorre garantire l'assistenza sistemistica, hardware e software, oltre che promuovere le attività di analisi e prevenzione di potenziali minacce digitali e proteggere la sicurezza delle informazioni all'interno ed all'esterno dell'organizzazione in tempo reale utilizzando algoritmi avanzati di machine learning;
Valutato	positivamente che, al fine di prevenire pregiudizi alla sicurezza delle reti, dei sistemi informativi e dei servizi informatici dell'Ente, la UOSD Tecnologie e Sistemi Informatici ha la necessità di affidare la fornitura del servizio di Cyber-defence alla società VOLA SPA;
Letto	l'art.50 comma 1 lett. b) del D. Lgs. 36/2023, per il quale “le stazioni appaltanti procedono all'affidamento di lavori, servizi e forniture [...] con affidamento diretto dei servizi e forniture, ivi compresi i servizi di ingegneria e architettura e l'attività di progettazione, di importo inferiore a 140.000 euro, anche senza consultazione di più operatori economici”;
Verificato	che non sono attivi Accordi Quadro o Convenzioni Consip per l'affidamento in oggetto;
Considerato	che invece il servizio di che trattasi è presente sul Me.PA di CONSIP sotto la categoria “Supporto e consulenza in ambito ICT” ed è inserito a catalogo dall'operatore economico VOLA SPA;

- Dato atto** che, al fine di procedere all’acquisto del software in parola, la scrivente UOSD ha avviato sul Me.PA di Consip la Trattativa Diretta n. 4162548 avente ad oggetto “Richiesta di offerta per il Servizio di Checklist, Redazione e Gestione del Registro Attività, Registro Password e Privacy/Data Protection in ambito di Sanità Elettronica ai fini dell’adeguamento degli IFO al GDPR (Allegato 1 al presente atto a formarne parte integrante e sostanziale);
- che, entro la data stabilita per la scadenza della ricezione dell’offerta la stessa società ha provveduto ad inviare un’offerta d’importo pari a € 22.000,00 oltre Iva (Allegato 2 al presente atto a formarne parte integrante e sostanziale);
- Valutato** che l’importo della suddetta offerta risulta congruo e in linea con gli importi di mercato relativi ad analoghe forniture e che, in conseguenza, è possibile procedere con l’affidamento della trattativa MEPA di che trattasi per un importo complessivo di € 26.840,00 Iva inclusa alla società VOLA SPA per il servizio in oggetto - CIG: B0CD0F2734;
- Tenuto conto** che la complessiva spesa pari ad € 22.00,00 oltre Iva al 22% e cioè pari ad € 26.840,00 Iva inclusa a copertura del periodo 01 marzo 2024 – 28 febbraio 2025 può essere registrata così come segue:
- € 22.366,70 sul bilancio economico 2024 sul conto 502020106
 - € 4.473,30 sul bilancio economico 2025 sul conto 502020106
- Attestato** che il presente provvedimento, a seguito dell’istruttoria effettuata, nella forma e nella sostanza è ritenuto adeguato e sufficiente in relazione al principio del risultato di cui all’art.1 del Dlgs n.36/2023 ed è totalmente legittimo e utile per il servizio pubblico, ai sensi dell’art. 1 della legge 14 gennaio 1994, n. 20 e successive modifiche, nonché alla stregua dei criteri di economicità e di efficacia di cui all’art. 1, primo comma, della legge 7 agosto 1990, n. 241, come modificata dalla legge 11 febbraio 2005, n. 15;

DETERMINA

Secondo l'art.50, comma 1, lettera b), del decreto legislativo del 31 marzo 2023 n. 36 e per i motivi esposti in narrativa che si intendono integralmente confermati, precisando che il presente provvedimento assume la valenza della decisione di contrarre di cui all'art. 17, comma 1, d.lgs. 36/2023, ai sensi del comma 2 del medesimo articolo;

- Affidare alla società VOLA SPA il servizio erogato come SaaS del sistema di sicurezza informatica CERBEYRA ai fini dell'adeguamento al Regolamento Europeo n. 2016/79 del 27 giugno 2016 (GDPR "General Data Protection Regulation") a copertura del periodo 01/03/2024 – 28/02/2025 e per un importo complessivo di € 22.000,00 oltre onere di legge al 22% - CIG: B0CD0F2734;
- Attestare che la spesa di € 22.000,00 oltre Iva al 22%, pari a € 26.840,00 Iva inclusa può essere registrata così come segue:
 - € 22.366,70 sul bilancio economico 2024 sul conto 502020106
 - € 4.473,30 sul bilancio economico 2025 sul conto 502020106
- Tramettere apposito ordine NSO;
- Nominare DEC del contratto il Sig. Umberto Santi.

La UOSD Ingegneria Clinica e Tecnologie e Sistemi Informatici curerà tutti gli adempimenti per l'esecuzione della presente determinazione.

Il Dirigente della UOSD Ingegneria Clinica e Tecnologie e Sistemi In-
formatici

Giuseppe Navaneri

Documento firmato digitalmente ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

Tipologia di Rdo: Trattative Dirette

- SERVIZI PROFESSIONALI AVANZATI PER LA SICUREZZA DELLE INFORMAZIONI;
- SERVIZIO DI CYBER SECURITY E THREAT INTELLIGENCE CERBEYRA .

Dati Principali

Numero RDO

4162548

Nome RDO

Richiesta di offerta per il Servizio di Checklist, Redazione e Gestione del Registro Attività, Registro Password e Privacy/Data Protection in ambito di Sanità Elettronica ai fini dell'adeguamento degli IFO al GDPR

Tipologia di contratto

Appalto di servizi

Tipologia di procedura

Affidamento diretto dei servizi e forniture, ivi compresi i servizi di ingegneria e architettura e l'attività di progettazione, di importo inferiore a 140.000 euro

Regolamento applicabile alla procedura telematica

Regolamento MEPA eProcurement Acquistinrete

Ruoli e Autorizzazioni

Responsabile del procedimento

GIUSEPPE NAVANTERI

NVNGPP84P23D086R

Soggetto Stipulante/Soggetti Stipulanti

GIUSEPPE NAVANTERI NVNGPP84P23D086R

Stazione Appaltante

AMMINISTRAZIONI ENTI ED AZIENDE DEL S.S.N. > AZIENDE OSPEDALIERE, POLICLINICI, IRCCS e ISTITUTI ZOOPROFILATTICI > I.R.C.C.S. ISTITUTI FISIOTERAPICI OSPITALIERI ROMA

Ente Committente

AMMINISTRAZIONI ENTI ED AZIENDE DEL S.S.N. > AZIENDE OSPEDALIERE, POLICLINICI, IRCCS e ISTITUTI ZOOPROFILATTICI > I.R.C.C.S. ISTITUTI FISIOTERAPICI OS...

Date

Pubblicazione

13/03/2024 13:46

Inizio presentazione offerte

13/03/2024 13:46

Termine ultimo presentazione offerte

15/03/2024 12:00

Data limite stipula contratto

16/05/2024 12:00

Giorni dopo la stipula per consegna beni/decorrenza

10

Dettaglio

Criterio Aggiudicazione

Minor Prezzo

CIG

BOCDOF2734

CUP

-

CPV

Identificativo

72212732-9

72322000-8

Descrizione

Servizi di programmazione di software di sicurezza dei dati

Categoria

Supporto e consulenza in ambito ICT

Fornitura

50

Formulazione offerta economica

VALORE ECONOMICO

Decimali Offerta

2

Termini di pagamento

30 GG DATA RICEVIMENTO FATTURA

Importo presunto fornitura

€ 23.180,00

Dati consegna e fatturazione

Fatturazione: VIA ELIO CHIANESI 53 - PRESSO UO INFORMATICA CED ROMA (ROMA); Consegna: VIA ELIO CHIANESI 53 - PRESSO UO INFORMATICA CED ROMA (ROMA); Aliquote: secondo la normativa vigente

Inviti

Partita IVA

Ragione sociale

01766360463

VOLA

Offerta Economica relativa a

Descrizione Richiesta di offerta per il Servizio di Checklist, Redazione e Gestione del Registro Attività, Registro Password e Privacy/Data Protection in ambito di Sanità Elettronica ai fini dell'adeguamento degli IFO al GDPR

RdO nr. 4162548

Numero lotto 0

Amministrazione titolare del procedimento

Ente acquirente	I.R.C.C.S. ISTITUTI FISIOTERAPICI OSPITALIERI ROMA		
Ufficio	UOSD TECNOLOGIE E SISTEMI INFORMATICI		
Codice fiscale	02153140583	Codice univoco ufficio	Non presente
Indirizzo sede	Via elio chianesi 53 - presso uo informatica ced		
Città	Roma		
Recapito telefonico	0652662444		
Email	GIUSEPPE.NAVANTERI@IFO.IT		
Punto ordinante	GIUSEPPE NAVANTERI		

Concorrente

Forma di partecipazione

Singolo operatore economico

Ragione sociale/Denominazione

VOLA

Partita IVA

01766360463

Tipologia societaria

Società per azioni (SPA)

Oggetto dell'Offerta

Formulazione dell'Offerta Economica = Valore economico (Euro)

Nome	Valore
Valore offerto	22000,00

Il Concorrente, nell'accettare tutte le condizioni specificate nella documentazione del procedimento, altresì dichiara:

- che la presente offerta è irrevocabile ed impegnativa sino al termine di conclusione del procedimento, così come previsto nella lex specialis;
- che la presente offerta non vincolerà in alcun modo la Stazione Appaltante/Ente Committente;
- di aver preso visione ed incondizionata accettazione delle clausole e condizioni riportate nel Capitolato Tecnico e nella documentazione di Gara, nonché di quanto contenuto nel Capitolato d'oneri/Disciplinare di gara e, comunque, di aver preso cognizione di tutte le circostanze generali e speciali che possono interessare l'esecuzione di tutte le prestazioni oggetto del Contratto e che di tali circostanze ha tenuto conto nella determinazione dei prezzi richiesti e offerti, ritenuti remunerativi;
- di non eccepire, durante l'esecuzione del Contratto, la mancata conoscenza di condizioni o la sopravvenienza di elementi non valutati o non considerati, salvo che tali elementi si configurino come cause di forza maggiore contemplate dal codice civile e non escluse da altre norme di legge e/o dalla documentazione di gara;
- che i prezzi/sconti offerti sono omnicomprensivi di quanto previsto negli atti di gara;
- che i termini stabiliti nel Contratto e/o nel Capitolato Tecnico relativi ai tempi di esecuzione delle prestazioni sono da considerarsi a tutti gli effetti termini essenziali ai sensi e per gli effetti dell'articolo 1457 cod. civ.;
- che il Capitolato Tecnico, così come gli altri atti di gara, ivi compreso quanto stabilito relativamente alle modalità di esecuzione contrattuali, costituiranno parte integrante e sostanziale del contratto che verrà stipulato con la stazione appaltante/ente committente.

ATTENZIONE: QUESTO DOCUMENTO NON HA VALORE SE PRIVO DELLA SOTTOSCRIZIONE A MEZZO FIRMA DIGITALE

SISTEMI DI E-PROCUREMENT