

REGIONE ABRUZZO
AZIENDA UNITÀ SANITARIA LOCALE TERAMO

Circ.ne Ragusa 1, 64100 Teramo
C.F. 00115590671

Direttore Generale: Dott. Maurizio Di Giosia

Deliberazione n° 1542 del 23 AGO. 2022

U.O.C. ACQUISIZIONE BENI E SERVIZI

OGGETTO: AFFIDAMENTO DELLA FORNITURA DEI SERVIZI SPECIALISTICI AVENTI AD OGGETTO LA VERIFICA PERIODICA ANALISI DI RISCHIO, ATTIVITA' DI IMPATTO SULLA PROTEZIONE DEI DATI, VULNERABILITY ASSESSMENT E PIANO SICUREZZA INFORMATICA. TRATTATIVA DIRETTA N. 3118069 CIG 9327901B68.

Data 3/08/22 Firma 
Il Responsabile dell'Istruttoria
Dott. Emiliano Capasso

Data 3/08/22 Firma 
Il Responsabile del Procedimento
Dott. Emiliano Capasso

Il Direttore della U.O.C. proponente con la sottoscrizione del presente atto, a seguito dell'istruttoria effettuata, attesta che l'atto è legittimo nella forma e nella sostanza ed è utile per il servizio pubblico.

VISTO: Il Direttore del Dipartimento Amministrativo
(Dott.ssa Rossella Di Marzio) 


Data 6.8.2022 Firma 
Il Direttore dell'UOC: Dott. Vittorio D'Ambrosio

PARERE DEL DIRETTORE AMMINISTRATIVO

- favorevole
 - non favorevole
- (con motivazioni allegate al presente atto)



Data 22-8-2022

Firma 
Il Direttore Amministrativo: Dott. Franco Santarelli

PARERE DEL DIRETTORE SANITARIO

- favorevole
 - non favorevole
- (con motivazioni allegate al presente atto)



Data 22-08-2022

Firma 
Il Direttore Sanitario: Dott. Maurizio Brucchi

REGIONE ABRUZZO
AZIENDA UNITÀ SANITARIA LOCALE TERAMO
Circ.ne Ragusa 1, 64100 Teramo
C.F. 00115590671

Direttore Generale: Dott. Maurizio Di Giosia

IL DIRETTORE DELLA U.O.C. ACQUISIZIONE BENI E SERVIZI dott. Vittorio D'Ambrosio

VISTA la nota acquisita al prot. N. 52465/22 del 09/05/2022 (all.1), a firma del Dirigente Responsabile dell'U.O.S.D. Segreteria di Direzione dott.ssa Valeria Violante e del Direttore Generale dott. Maurizio Di Giosia con la quale si richiede di avviare la procedura necessaria all'affidamento dei servizi specialistici aventi ad oggetto la verifica periodica analisi di rischio, attività di impatto sulla protezione dei dati, vulnerability assessment e piano sicurezza informatica;

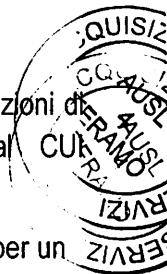
PREMESSO che a seguito di incontri tra quest'ufficio e la U.O.S.D. Segreteria di Direzione, data la complessità dell'attività e l'elevato profilo di confidenzialità dei dati oggetto di verifica, si è deciso di rinnovare il rapporto contrattuale con la ditta Infoteam S.r.l. già affidataria di precedenti servizi supporto inerenti la disciplina della Privacy;

ATTESO che l'intervento di cui sopra è previsto nel Programma biennale 2021/2022 – delle acquisizioni di beni e servizi, approvato con deliberazione n. 698 del 09/04/2021 ed identificato al CU n. **S00115590671202200028**, per un valore complessivo di € 130.000,00 IVA esclusa;

RITENUTO, dato il carattere ripetitivo dei servizi in oggetto, di istruire una procedura di affidamento per un periodo di tre anni (36 mesi);

VISTI gli artt.:

- 30 comma 1 del D. Lgs. n. 50/2016 che disciplina i principi per l'aggiudicazione e l'esecuzione di appalti e concessioni e stabilisce che: *"L'affidamento e l'esecuzione di appalti di opere, lavori, servizi, forniture e concessioni.....si svolge nel rispetto dei principi di economicità, efficacia, tempestività e correttezza. Nell'affidamento degli appalti e delle concessioni, le stazioni appaltanti rispettano, altresì, i principi di libera concorrenza, non discriminazione, trasparenza, proporzionalità, nonché di pubblicità con le modalità indicate nel presente codice..."*;
- 36 co. 1 del D. Lgs. n. 50/2016 che disciplina, in particolare, i principi da seguire nell'affidamento di contratti di valore inferiore alla soglia di rilevanza comunitaria, ai sensi del quale *"l'affidamento e l'esecuzione di lavori, servizi e forniture di importo inferiore alle soglie di cui all'articolo 35 avvengono nel rispetto dei principi di cui agli articoli 30, comma 1, 34 e 42, nonché del rispetto del principio di rotazione degli inviti e degli affidamenti e in modo da assicurare l'effettiva possibilità di partecipazione delle microimprese, piccole e medie imprese. Le stazioni appaltanti applicano le disposizioni di cui all'articolo 50"*;



- 1 comma 2 lett. a) della legge n. 120/2020 così come modificato dal DL n. 77 del 31.5.2021 per il quale fino al 30 giugno 2023, in deroga a quanto stabilito all'art. 36 comma 2 del D. Lgs. n. 50/2016, è consentito alle stazioni appaltanti di procedere, per l'acquisizione di servizi e forniture, mediante affidamento diretto per importi inferiori a € 139.000,00;
- 54 commi 1, 2 e 3 - del D. Lgs. 50/2016 che disciplina l'istituto dell'accordo quadro con unico operatore economico;

PRECISATO che il presente provvedimento vale anche quale determina a contrarre, ai sensi dell'art. 32 comma 2 del D. Lgs. n. 50/2016;

RILEVATO che ai fini della tracciabilità dei pagamenti il numero di CIG che identifica la procedura è il seguente: **9327901B68**;

DATO ATTO che, quest'ufficio in data 18/07/2022 inoltrava, alla ditta Infoteam Srl (P. Iva 01538680685), Trattativa Diretta sulla piattaforma Mepa n. 3118069 finalizzata all'acquisizione di un preventivo per la fornitura triennale dei servizi specialistici aventi ad oggetto la verifica periodica analisi di rischio, attività di impatto sulla protezione dei dati, vulnerability assessment e piano sicurezza informatica;

DATO ATTO che, in data 25/07/2022, la ditta Infoteam Srl (P. Iva 01538680685) trasmetteva propria miglior offerta (all.2) per la fornitura dei servizi in oggetto ad un costo complessivo triennale di € 125.000,00 iva esclusa così come dettagliato nella seguente tabella:



Servizio	Metrica	Quantità	Costo	Totale
<i>Supporto nelle procedure di valutazione, designazione e monitoraggio ed analisi del rischio dei RT</i>	A canone	--	--	€ 50.000,00
<i>Servizio di supporto alla redazione delle DPIA</i>	A consumo	10 DPIA	€ 1.200,00	€ 12.000,00
<i>Vulnerability assessment (VA)</i>	A consumo	2 VA	€ 4.000,00	€ 8.000,00
<i>Analisi del rischio trattamento dati (AR)</i>	A consumo	2 AR	€ 5.000,00	€ 10.000,00
<i>Attività per il mantenimento del sistema di protezione dati</i>	A canone	--	--	€ 45.000,00
Totale iva esclusa				125.000,00

VISTO il parere favorevole espresso dalla dott.ssa Valeria Adriana Violante circa l'idoneità dell'offerta rispetto alle esigenze espresse dalla Direzione Generale nella nota prot. N. 52465/22 del 09/05/2022;

RITENUTO di affidare alla ditta Infoteam Srl (P. Iva 01538680685) con sede legale in Viale Pindaro, 14 - 65127 Pescara (PE) la fornitura triennale dei servizi specialistici aventi ad oggetto la verifica periodica analisi di rischio, attività di impatto sulla protezione dei dati, vulnerability assessment e piano sicurezza informatica per un importo complessivo di € 125.000,00 iva esclusa;

RITENUTO, quindi

- di doversi rendere il presente provvedimento immediatamente esecutivo al fine di garantire, con la massima tempestività, le forniture di che trattasi;
- di nominare quale direttore dell'esecuzione del contratto (D.E.C.), la dott.ssa Valeria Adriana Violante, Dirigente Responsabile dell'U.O.S.D. Segreteria di Direzione, ricorrendo nel caso di specie i presupposti di cui al par. 10 delle Linee Guida ANAC n. 3 trattandosi di fornitura sanitaria caratterizzata da particolare complessità sotto il profilo legale, considerato che la fornitura in argomento, impone il coinvolgimento di unità operative diverse dalla proponente;

D E L I B E R A

per tutti i motivi esplicitati in narrativa e che debbono intendersi per integralmente riportati e trascritti nel presente dispositivo

- 1) **DI AFFIDARE**, ai sensi dell'art. 1 comma 2 lett. a) della legge n. 120/2020 così come modificato dal DL n. 77 del 31.5.2021, alla ditta Infoteam Srl (P. Iva 01538680685) con sede legale in Viale Pindaro, 14 - 65127 Pescara (PE) la fornitura dei servizi in oggetto ad un costo complessivo triennale di € 125.000,00 iva esclusa così come dettagliato nella seguente tabella:

Servizio	Metrica	Quantità	Costo	Totale
<i>Supporto nelle procedure di valutazione, designazione e monitoraggio ed analisi del rischio dei RT</i>	A canone	--	--	€ 50.000,00
<i>Servizio di supporto alla redazione delle DPIA</i>	A consumo	10 DPIA	€ 1.200,00	€ 12.000,00
<i>Vulnerability assessment (VA)</i>	A consumo	2 VA	€ 4.000,00	€ 8.000,00
<i>Analisi del rischio trattamento dati (AR)</i>	A consumo	2 AR	€ 5.000,00	€ 10.000,00
<i>Attività per il mantenimento del sistema di protezione dati</i>	A canone	--	--	€ 45.000,00
Totale iva esclusa				125.000,00



- 2) **DI DETERMINARE** la spesa per l'intera fornitura di che trattasi in € **152.500,00** iva inclusa;
- 3) **DI DARE ATTO** che alla spesa complessiva di € **152.500,00** iva inclusa come sopra determinata, si farà fronte con le autorizzazioni di spesa di cui al prospetto finanziario in calce al presente provvedimento;
- 4) **DI NOMINARE** quale direttore dell'esecuzione del contratto (D.E.C.), la dott.ssa Valeria Adriana Violante, Dirigente Responsabile dell'U.O.S.D. Segreteria di Direzione, ricorrendo nel caso di specie i presupposti di cui al par. 10 delle Linee Guida ANAC n. 3 trattandosi di fornitura sanitaria caratterizzata da particolare complessità sotto il profilo legale, considerato che la fornitura in argomento, impone il coinvolgimento di unità operative diverse dalla proponente;
- 5) **DI DICHIARARE** il presente provvedimento immediatamente esecutivo al fine di garantire, con la massima tempestività, le forniture di che trattasi;

IL DIRETTORE GENERALE

Preso atto:

- che il Dirigente proponente il presente provvedimento, sottoscrivendolo, ha attestato che lo stesso, a seguito dell'istruttoria effettuata, è, nella forma e nella sostanza, legittimo ed utile per il servizio pubblico, ai sensi e per gli effetti di quanto disposto dall'art. 1 della legge 20/94 e successive modifiche;
- che il Direttore Amministrativo ed il Direttore Sanitario hanno espresso formalmente parere favorevole

DELIBERA

di approvare e far propria la proposta di cui trattasi che qui si intende integralmente riportata.




IL DIRETTORE GENERALE

Dott. Maurizio Di Giosia



Azienda Unità Sanitaria Locale 4 - Teramo

U.O.C. Acquisizione Beni e Servizi

ALLEGATI ALLA DELIBERAZIONE

Allegato 1 - nota prot. N. 52465/22 del 09/05/2022 (pag. 1)

Allegato 2 – offerta tecnico/economica ditta Infoteam Srl (P. Iva 01538680685) (pag. 2-10)

allegati n. 10



{

Direzione Generale



ASL TERAMO PROTOCOLLO UNICO

Posta Interna



Prot. n.0052465/22 del 09/05/2022

Al Direttore dell'UOC
Acquisizione Beni e Servizi
Dott. Vittorio D'Ambrosio

OGGETTO: Richiesta avvio procedura per l'affidamento del servizio specialistico avente ad oggetto verifica periodica analisi del rischio, l'attività di valutazione impatto sulla protezione dei dati, Vulnerability Assessment e piano sicurezza informatica.

Con riferimento all'oggetto, richiamata la delibera n. 329 del 17 febbraio 2022, con la quale questa Azienda ha provveduto, tra l'altro, ad approvare il Regolamento aziendale per la protezione dei dati personali dell'ASL di Teramo, tenuto conto della necessità che il Titolare provveda a verifiche periodiche sulla sicurezza delle misure di protezione dei dati, compresa la *vulnerability assessment* e che siano eseguite, secondo gli esiti delle procedure di gara per la selezione dei fornitori, specifiche attività per la periodica analisi del rischio e l'eventuale valutazione d'impatto sulla protezione dei dati, considerato che lo svolgimento delle attività suddette attengono a professionalità altamente specializzate nel settore della protezione dei dati, non presenti attualmente nell'organico interno, s'invita la S.V. a voler predisporre gli atti necessari al fine di reperire anche mediante affidamento diretto un operatore economico specializzato.

Data la complessità dell'attività e l'elevato profilo di confidenzialità dei dati oggetto di verifica, si chiede, altresì, di valutare la possibilità di rinnovare il rapporto contrattuale con il precedente contraente nei limiti di spesa autorizzabili.

Cordiali saluti

Il Responsabile della UOSD

Segreteria di Direzione

dott. Valeria Adriana Violante

Il Direttore Generale
Dott. Maurizio Di Giosia

**Servizi di supporto
alla protezione dei dati
e alla
sicurezza delle Informazioni**



Sommario

1	Premessa	3
2	Normativa di riferimento.....	3
3	Oggetto dell'offerta.....	3
4	Descrizione dei servizi	3
4.1	Supporto nelle procedure di valutazione, designazione e monitoraggio ed analisi del rischio dell'operato dei Responsabili del trattamento	3
4.1.1	Supporto alle funzioni interne dell'Azienda nelle procedure di valutazione e designazione del Responsabile del trattamento	3
4.1.2	Attività di monitoraggio e analisi del rischio dell'operato dei Responsabili del trattamento	4
4.2	Attività di valutazione d'impatto (DPIA)	4
4.3	Vulnerability assessment	5
4.4	Attività di analisi del rischio	5
4.5	Eventuali attività richieste dal cliente per il mantenimento del sistema di protezione dati implementato presso l'ente.....	6
5	Gruppo di lavoro	6
5.1	Project Manager (PM).....	7
5.2	Specialista protezione dati (SPD).....	7
5.3	Consulente legale protezione dati (CLP).....	7
5.4	IT Security Specialist (CSS).....	7
6	Vincolo di Riservatezza.....	8
7	Arco temporale	8
8	Offerta Economica	8
9	Condizioni di fornitura:	9

<

3

1 Premessa

I servizi offerti, oltre a presentare le attività da eseguire e le risorse che saranno impegnate, illustra le attività che saranno erogati per supportare le unità organizzative aziendali - responsabili del sistema di gestione della protezione dei dati e del controllo dell'adeguato livello di sicurezza - negli adempimenti di cui alle normative ed agli standard di sicurezza di seguito indicati.

2 Normativa di riferimento

Il quadro normativo di riferimento per i servizi proposti è costituito dai dispositivi legislativi che definiscono e regolamentano la gestione della sicurezza delle informazioni e delle infrastrutture informatiche:

- Regolamento Europeo sulla Protezione dei Dati n. 679/2016 (di seguito GDPR)
- D. Lgs. 196/03 e ss. mm. ii. - "Codice in materia di Trattamento dei Dati Personali" (c.d. Codice della Privacy)
- PNRR: Piano nazionale di rilancio e resilienza e prime misure di rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure, D. L. 31 maggio 2021, n. 77, pub. in G.U. n. 129 del 31 maggio 2021, ed. straordinaria
- Perimetro di Sicurezza Nazionale Cibernetica - D.L.105/2019 convertito in L. 133/2019
- UNI ISO 27001:2013 – Sistema di Gestione per la Sicurezza delle Informazioni
- Piano Triennale dell'Agenzia per l'Italia Digitale per l'Informatica nella Pubblica Amministrazione 2020-2022

3 Oggetto dell'offerta

Le attività della proposta in oggetto riguardano i seguenti servizi:

1. Attività di monitoraggio periodico dell'operato dei Responsabili del trattamento
2. Attività di valutazione di impatto (DPIA)
3. Vulnerability assessment (VA)
4. Analisi del rischio trattamento dati dell'organizzazione
5. Eventuali attività per il mantenimento del sistema di protezione dati implementato presso l'ente

4 Descrizione dei servizi

4.1 Supporto nelle procedure di valutazione, designazione e monitoraggio ed analisi del rischio dell'operato dei Responsabili del trattamento

4.1.1 Supporto alle funzioni interne dell'Azienda nelle procedure di valutazione e designazione del Responsabile del trattamento

Il ruolo del partner tecnologico diventa ancora più cruciale per il successo e la messa in sicurezza aziendale. Quando occorre scegliere un prodotto od una soluzione, prima di ogni altro tipo di valutazione, è opportuno considerare quel prodotto o soluzione possa contribuire all'aumento della sicurezza informatica aziendale, al di là dei relativi costi o della capacità di approvvigionamento.

L'attività prevede quindi di definire ed attuare delle procedure di selezione e valutazione dei processi di acquisizione, con particolare riferimento all'acquisizione di **applicativi, asset informatici e dispositivi medici**, al fine di scongiurare potenziali rischi informatici ed organizzativi.

Il servizio erogato alle unità organizzative aziendali coinvolte nella valutazione e successiva designazione del fornitore, consisterà pertanto nell'assistenza in merito al complessivo processo di verifica del fornitore in materia di sicurezza, al fine di valutare la presenza di garanzie sufficienti (e dunque delle misure tecniche ed organizzative adeguate al rischio) affinché il trattamento effettuato dalle terze parti soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato; dalla richiesta al fornitore della Check list di



4

3

2

valutazione al successivo parere e supporto alla valutazione della rispondenza ai requisiti ed alle misure di sicurezza, l'attività sarà sviluppata dal team di consulenti, con il supporto dell'area informatica aziendale del DPO.

Nella fase di designazione del fornitore a Responsabile del trattamento (ex art 28 GDPR), il team di consulenti si occuperà della sottoscrizione dell'Accordo sulla Protezione dei Dati, ossia l'Atto di designazione del Responsabile del Trattamento, coordinando le attività tra il fornitore ed il Titolare.

4.1.2 Attività di monitoraggio e analisi del rischio dell'operato dei Responsabili del trattamento

Il Titolare ha l'obbligo di monitorare l'operato dei Responsabili con particolare riguardo ai punti indicati nelle istruzioni impartite e alla verifica della conformità dell'esecuzione dei servizi erogati rispetto a quanto stabilito nella fase preliminare di attivazione degli stessi e validati in termini di Protezione dei Dati Personali. A tal fine, l'attività di monitoraggio del fornitore potrà essere condotta dal nostro team di consulenti per mezzo di verifiche/audit di "Seconda parte" e consisterà nella verifica dell'adeguatezza delle misure in essere rispetto ai requisiti richiesti nei confronti dei fornitori e nella verifica dell'effettiva corrispondenza alle procedure aziendali, con particolare riguardo ai seguenti punti:

- rispetto delle istruzioni impartite dal Titolare;
- verifica della conformità dell'esecuzione dei servizi erogati;
- essere l'interfaccia per l'organizzazione di eventuali audit;
- specificare le funzioni aziendali coinvolte nell'audit.

L'output dell'attività di analisi sarà costituito da un'analisi del rischio volta ad individuare il divario tra la situazione attuale e quella che rappresenta una corretta gestione trattamento dei dati da parte del responsabile del trattamento, accompagnata da un piano di trattamento del rischio che indicherà le azioni di mitigazione/risoluzione raccomandate per contrastare le minacce rilevate.

4.2 Attività di valutazione d'impatto (DPIA)

Il servizio, riferito a trattamenti effettuati dal Titolare, comprende le seguenti attività:

- Analisi dei requisiti di una DPIA attraverso il supporto per identificare e verificare i flussi di dati ed i progetti chiave, portando a termine una selezione di progetti o attività di trattamento dei dati, per determinare se e quando una DPIA sia necessaria in linea con il GDPR;
- Assistenza guidata alla redazione di una DPIA che comprenderà il coinvolgimento dei Responsabili del Trattamento e la somministrazione di schede tecniche valutative del servizio, attività di audit e richiesta di informazioni suppletive che si ritengano necessarie per la redazione della Valutazione d'Impatto.

Il documento di valutazione sarà predisposto in ottemperanza alle linee guida WP248 ed alle procedure interne dell'Azienda, specificando in particolare:

- Oggetto della DPIA
- Trattamenti soggetti a DPIA
- Metodologie di conduzione
- Indicazione dei principali impatti privacy
- Alternative per minimizzare o evitare gli impatti negativi
- Consultazione dell'autorità di controllo
- Eventuali cambiamenti al processo
- Definizione dei criteri di idoneità/adeguatezza delle misure di sicurezza.

4.3 Vulnerability assessment

L'obiettivo del servizio è quello di verificare lo stato di sicurezza dell'infrastruttura ed alla predisposizione - qualora necessario - del conseguente remediation plan ed individuare potenziali vulnerabilità e/o errori di configurazione presso l'infrastruttura esterna e/o interna del Cliente, le quali potrebbero essere sfruttate da attori malevoli esterni od interni per esfiltrare dati o compromettere i sistemi.

Difatti, come richiesto oramai da numerose normative di settore e standard internazionali, l'attuazione di misure tecnico-organizzative di sicurezza non è di per sé sufficiente a garantire - e soprattutto a dimostrare, in termini di *accountability* - l'effettiva messa in sicurezza dell'infrastruttura contro attacchi esterni ed interni.

A tal fine è al contrario necessario procedere con un piano vulnerability assessment condotti ad intervalli regolari, tanto dall'interno quanto dall'esterno e finalizzati a verificare l'efficacia ed efficienza delle contromisure adottate, in modo da poter dimostrare come il sistema di information security sia stato sottoposto ai dovuti test di funzionamento.

L'eventuale esito negativo dei test - qualora gli stessi rilevino cioè l'esistenza di vulnerabilità - sarebbe in realtà da leggere, in tal caso, come assolutamente positivo, in quanto permetterebbe al Cliente di venire a conoscenza delle proprie debolezze e risolverle/mitigarle per tempo, documentando le azioni di remediation intraprese ed effettuando successivamente un nuovo test di verifica del superamento della problematica.

4.4 Attività di analisi del rischio

Il nuovo quadro normativo in materia di protezione dei dati personali presuppone un processo di analisi che è prioritario rispetto a qualsiasi scelta in materia di protezione dei dati, in particolare, l'art. 24 del Regolamento UE 2016/679 (cd. GDPR) richiede che ciascun titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, conduca una preventiva analisi dei rischi che impattano sui diritti e le libertà delle persone e metta in atto misure tecniche e organizzative adeguate a garantire e dimostrare la conformità alla normativa.

Ciò detto il servizio svolto di analisi del rischio andrà a misurare del livello di sicurezza dell'azienda andando a svolgere un'attività di analisi preventiva sulla cui base poter parametrare le misure di sicurezza dell'organizzazione e quindi valutare il rischio intrinseco delle attività che l'organizzazione pone in essere. L'obiettivo della valutazione del rischio privacy è quindi l'implementazione di un piano di gestione del rischio.

L'analisi e la valutazione sarà essere svolta in diverse fasi:

- individuazione della tipologia di dati personali e dei trattamenti effettuati in azienda;
- identificazione delle minacce, dei potenziali danni e della relativa probabilità di accadimento;
- attuazione delle misure di protezione da applicare e programmazione delle verifiche periodiche;
- valutazione del rischio residuo.

I parametri di valutazione del rischio sono:

- il contesto;
- l'asset e il suo valore, da cui dipende l'impatto;
- la minaccia e la sua verosimiglianza o probabilità;
- le vulnerabilità e la loro gravità o i controlli di sicurezza e la loro robustezza.

Il documento di analisi dei rischi e piano di gestione del rischio sarà il risultato dell'audit volto a condurre una preventiva analisi che consenta di calcolare il livello di rischio intrinseco prendendo in considerazione tutta l'organizzazione del titolare e, quindi, tutte le attività di trattamento che da questa vengono svolte, valutare i controlli già implementati, calcolare quindi il livello di rischio residuo per l'organizzazione e pianificare il suo piano di trattamento secondo le modalità ritenute più opportune. Il parametro preso in considerazione in

U
★

5

6

tale analisi non sarà solo quello di business, ma riguarderà principalmente la tutela dei diritti e le libertà delle persone/interessati.

4.5 Eventuali attività richieste dal cliente per il mantenimento del sistema di protezione dati implementato presso l'ente

Tale attività prevede il supporto alle unità organizzative aziendale nella corretta applicazione del sistema di protezione dei dati personali implementato presso di esso.

Il supporto riguarderà tutti gli ambiti del sistema privacy per cui si manifestasse la necessità di una consulenza ed assistenza specifica nella corretta applicazione del GDPR.

Attività di supporto:

- Assistenza nelle procedure di gestione di eventuali Data Breach
- Supporto nella corretta applicazione della disciplina sugli impianti di videosorveglianza e televigilanza
- Assistenza nelle procedure di gestione dei diritti dell'interessato
- Supporto nella individuazione, descrizione e gestione di nuovi eventuali trattamenti e conseguente gestione del registro del trattamento dei dati (ex art. 30 del Regolamento), nonché nella redazione di informative/consensi qualora fossero necessari.

5 Gruppo di lavoro

Per garantire l'efficienza dei servizi proposti e lo sviluppo della presente offerta, le attività saranno erogate da un team di lavoro composto da specialisti in possesso di comprovate esperienze pluriennali e adeguate certificazioni di competenza di Privacy Consultant, DPO e sicurezza informatica.

Le risorse del gruppo di lavoro hanno un ottimo livello di conoscenza dei seguenti punti:

- normativa nazionale italiana ed europea in materia di protezione dei dati e in particolare del RGPD,
- delle tecnologie informatiche e misure di sicurezza dei dati,
- risk management,
- Sicurezza informatica,
- Software gestione GDPR.

Il Team di lavoro che erogherà i servizi sarà composto dalle seguenti figure professionali:

Acronimo	Figura Professionale	Attività
PM	Project Manager	Gestione servizi offerti
SPD	Specialista Protezione dati	Erogazione servizi GDPR – Risk assessment
CLP	Consulente Legale Protezione dei Dati	Valutazioni d'impatto – Monitoraggio RT
CSS	IT Security Specialist	DPIA - Vulnerability assessment

I servizi saranno coordinati da un Project Manager appositamente incaricato che agirà quale figura di riferimento per l'Azienda e per la verifica e la definizione degli stati di avanzamento di attività.

Al fine di consentire al team di lavoro anzidetto di adempiere correttamente agli incarichi conferiti rispettando gli obblighi e le tempistiche richieste dalla normativa, l'Azienda dovrà utilmente collaborare

fornendo ogni dato e informazione che si renda necessario od opportuno per la puntuale prestazione dei servizi.

5.1 Project Manager (PM)

Sarà il coordinatore ed il responsabile delle attività proposte: costituisce il punto di riferimento sia dei referenti dell'Azienda che del gruppo di lavoro.

Le principali competenze e funzioni di questa figura professionale sono:

- Approfondita e consolidata esperienza nel project management e di coordinatore delle attività, in particolare nell'ambito P.A., di progetti complessi ed articolati per Pubbliche Amministrazioni centrali e locali.
- Esperienza nella pianificazione, nei processi di controllo, nella programmazione ed organizzazione delle risorse umane a sua disposizione nello sviluppo di progetti applicativi complessi.
- Gestione delle attività quotidiane del team, delle tempistiche e del rispetto della pianificazione.

5.2 Specialista protezione dati (SPD)

Figura che dovrà supportare il referente dell'azienda e il Project Manager nel mettere a punto le idonee misure tecniche e organizzative ai fini del trattamento di dati personali.

Le attività tipiche di questa figura professionale sono:

- interfacciarsi con il DPO
- esecuzione delle attività in riferimento al GDPR (valutazione fornitore)
- supportare il project manager nella fase dell'erogazione del servizio nell'ambito del GDPR
- coordinare le attività di valutazione della sicurezza svolte dal sistemista senior.

5.3 Consulente legale protezione dati (CLP)

Dovrà supportare e assistere il Project Manager e il referente dell'Azienda nella predisposizione di modelli contrattuali e di modulistica, monitoraggio preventivo dei rischi legali connessi al trattamento e corsi di formazione.

Le attività tipiche di questa figura professionale sono:

- redazione DPIA
- revisione della documentazione e predisposizione di adeguata contrattualistica (nomine responsabili del trattamento)
- formazione per il personale
- conduzione degli audit
- verifica della conformità al Regolamento Europeo 679/2016, al D. Lgs. n. 196/2003 e delle misure di sicurezza adottate dall'Appaltatore.

5.4 IT Security Specialist (CSS)

Si occuperà di identificare i requisiti e di definire modelli di flussi informativi e di oggetti da gestire per l'erogazione dei servizi di adeguamento normativo dei sistemi informativi. Ha una competenza ampia ed approfondita in tutti i campi ICT (software, hardware, reti e SAN), al quale abbina la capacità di interagire con i referenti dell'Azienda e il Project Manager. Redige la reportistica tecnica, progetta ed esegue i test,

sia nel complesso che per singoli moduli componenti, identifica le vulnerabilità e diagnostica le possibili cause.

Le attività tipiche di questa figura professionale sono:

- Curare l'esecuzione dei servizi di valutazione della sicurezza del sistema informativo
- Assistere nella valutazione e selezione di componenti software adatti a soddisfare completamente o parzialmente i requisiti specificati
- Erogare le attività di VA
- Fornire consulenza specialistica nella gestione dei sistemi informativi in esercizio
- Supportare l'attività di riorganizzazione dei processi tecnologici

6 Vincolo di Riservatezza

Il fornitore si impegna a garantire la riservatezza delle informazioni di cui verrà a conoscenza nel corso dell'attività di servizio, e s'impegna a non divulgare alcun tipo di informazione se non previa autorizzazione scritta da parte dell'Azienda.

Il fornitore osserverà le norme previste dal GDPR in materia di trattamento dei dati personali.

Il fornitore al termine dell'attività non potrà utilizzare, divulgare, trasmettere, trattare, cedere, vendere, a qualsiasi titolo le informazioni e i dati acquisiti durante il periodo contrattuale, consegnando all'Azienda ogni documento o altro elaborato realizzato in base al presente contratto.

7 Arco temporale

L'erogazione dei servizi ed in generale di tutte le attività descritte nella presente proposta è prevista su di un arco temporale pari a mesi 36.

8 Offerta Economica

Con riferimento ai servizi ed alle forniture previste nei paragrafi precedenti, si esplicita la scheda economica per i Servizi professionali sopra descritti:

Servizio	Metrica	Quantità	Costo	Totale
<i>Supporto nelle procedure di valutazione, designazione e monitoraggio ed analisi del rischio dei RT</i>	A canone	--	--	€ 50.000,00
<i>Servizio di supporto alla redazione delle DPIA</i>	A consumo	10 DPIA	€ 1.200,00	€ 12.000,00
<i>Vulnerability assessment (VA)</i>	A consumo	2 VA	€ 4.000,00	€ 8.000,00
<i>Analisi del rischio trattamento dati (AR)</i>	A consumo	2 AR	€ 5.000,00	€ 10.000,00
<i>Attività per il mantenimento del sistema di protezione dati</i>	A canone	--	--	€ 45.000,00
Totale iva esclusa				125.000,00
Iva				27.500,00
Totale Iva Inclusa				152.500,00

9 Condizioni di fornitura:

IVA	A Vostro carico
Termini di Pagamento quota canoni	Canone trimestrale
Termini di Pagamento quota a consumo	Rendicontazione trimestrale
Durata del contratto	36 mesi
Fatturazione	Trimestrale posticipata
Modalità di Pagamento	Bonifico bancario
Inizio lavori	Da concordare



18

U.O.C. Acquisizione Beni e Servizi

Rif areas

CIG: 9327901B68

Ditta aggiudicataria: Infoteam Srl (P. Iva 01538680685)

Spesa anno 2022 € 16.944,45 sottoconto 070202012700 UA_ABS/2022/1/209
(01/09/2022-31/12/2022)

Spesa anno 2023 € 58.833,33 sottoconto 070202012700 UA_ABS/2023/1/40

Spesa anno 2024 € 58.833,33 sottoconto 070202012700 UA_ABS/2024/1/15

Spesa anno 2025 € 33.888,89 sottoconto 070202012700 UA_ABS/2025/1/8
(01/01/2025-31/08/2025)

Fonte di finanziamento: FSN

Data 6.8.2022



Il Dirigente dell'U.O.C. proponente

dott. Vittorio D'Ambrosio

U.O.C. Attività Economiche e Finanziarie

Si attesta la REGOLARITÀ CONTABILE della presente spesa che trova capienza nel Bilancio di previsione anno 2022

Data: 12/08/2022

Il Contabile

Il Dirigente

ASL 4 TERAMO
U.O.C. Attività Economiche e Finanziarie
IL DIRIGENTE RESPONSABILE
Dott.ssa Antonella Di Silvestre

Della suestesa deliberazione viene iniziata la pubblicazione il giorno 23 AGO. 2022 con prot. n. 2884/22 all'Albo informatico della ASIA per rimanervi 15 giorni consecutivi ai sensi del d.lgs. n. 267/2000 e della L. n. 28/1992.



Firma _____

L'Addetto alla pubblicazione informatica

- La suestesa deliberazione diverrà esecutiva a far data dal _____ quindicesimo giorno successivo alla pubblicazione.
- La suestesa deliberazione è stata dichiarata "immediatamente eseguibile"

La trasmissione al Collegio Sindacale è assolta mediante pubblicazione sull'Albo Aziendale.

Per l'esecuzione (E) ovvero per opportuna conoscenza (C) trasmessa a:

Coordinamenti/Dipartimenti e Distretti		Unità Operative		Staff	
Coordinamento Staff di Direzione		Segreteria Generale e Affari Legali		UOC Controllo di gestione	
Dipartimento Amministrativo	<input type="checkbox"/> E <input type="checkbox"/> C	Acquisizione Beni e Servizi	<input type="checkbox"/> E <input type="checkbox"/> C	UOC Formazione, Qualità e Comunicazione Strategica	<input type="checkbox"/> E <input type="checkbox"/> C
Dipartimento Tecnico-Logistico	<input type="checkbox"/> E <input type="checkbox"/> C	Attività Economiche e finanziarie	<input type="checkbox"/> E <input type="checkbox"/> C	UOSD Ufficio Relazioni con il Pubblico	<input type="checkbox"/> E <input type="checkbox"/> C
Dipartimento Assistenza Territoriale	<input type="checkbox"/> E <input type="checkbox"/> C	Gestione del Personale	<input type="checkbox"/> E <input type="checkbox"/> C	UOSD Servizio Prevenzione e Protezione Sicurezza Interna	<input type="checkbox"/> E <input type="checkbox"/> C
Coordinamento Assistenza Ospedaliera	<input type="checkbox"/> E <input type="checkbox"/> C	Attività Amministrative Assistenza Territoriale e Distrettuale	<input type="checkbox"/> E <input type="checkbox"/> C	UOSD CUP Aziendale e monitoraggio Liste di attesa	
Dipartimento Emergenza Urgenza	<input type="checkbox"/> E <input type="checkbox"/> C	Patrimonio, Lavori e manutenzioni	<input type="checkbox"/> E <input type="checkbox"/> C		<input type="checkbox"/> E <input type="checkbox"/> C
Dipartimento Cardio-Toraco-Vascolare	<input type="checkbox"/> E <input type="checkbox"/> C	Sistemi Informativi	<input type="checkbox"/> E <input type="checkbox"/> C		<input type="checkbox"/> E <input type="checkbox"/> C
Dipartimento Chirurgico	<input type="checkbox"/> E <input type="checkbox"/> C	Attività amm.ve Dipartimenti Prevenzione e Salute Mentale	<input type="checkbox"/> E <input type="checkbox"/> C		
Dipartimento Salute Mentale	<input type="checkbox"/> E <input type="checkbox"/> C	Attività amm.ve dei Presidi Ospedalieri	<input type="checkbox"/> E <input type="checkbox"/> C		<input type="checkbox"/> E <input type="checkbox"/> C
Dipartimento Oncologico	<input type="checkbox"/> E <input type="checkbox"/> C	Direzione medica e gestione complessiva del PO di Teramo	<input type="checkbox"/> E <input type="checkbox"/> C		<input type="checkbox"/> E <input type="checkbox"/> C
Dipartimento Medico	<input type="checkbox"/> E <input type="checkbox"/> C	Direzione medica e Gestione complessiva PO di Atri	<input type="checkbox"/> E <input type="checkbox"/> C		<input type="checkbox"/> E <input type="checkbox"/> C
Dipartimento dei Servizi	<input type="checkbox"/> E <input type="checkbox"/> C	Direzione medica e Gestione complessiva PO di Giulianova	<input type="checkbox"/> E <input type="checkbox"/> C	altre Funzioni di Staff	
Dipartimento di Prevenzione	<input type="checkbox"/> E <input type="checkbox"/> C	Direzione medica e Gestione complessiva PO di Sant'Omero	<input type="checkbox"/> E <input type="checkbox"/> C	Comitato Unico di Garanzia	<input type="checkbox"/> E <input type="checkbox"/> C
Dipartimento Materno-Infantile	<input type="checkbox"/> E <input type="checkbox"/> C	Area Distrettuale Adriatico	<input type="checkbox"/> E <input type="checkbox"/> C	Resp.le Prevenzione Corruzione e Trasparenza	<input type="checkbox"/> E <input type="checkbox"/> C
Distretto di	<input type="checkbox"/> E <input type="checkbox"/> C	Area Distrettuale Gran Sasso - Laga	<input type="checkbox"/> E <input type="checkbox"/> C	Internal Audit	<input type="checkbox"/> E <input type="checkbox"/> C
	<input type="checkbox"/> E <input type="checkbox"/> C	Servizio Farmaceutico Territoriale	<input type="checkbox"/> E <input type="checkbox"/> C	Organismo indipendente di valutazione	<input type="checkbox"/> E <input type="checkbox"/> C
	<input type="checkbox"/> E <input type="checkbox"/> C	Medicina Penitenziaria	<input type="checkbox"/> E <input type="checkbox"/> C	Ufficio Procedimenti Disciplinari	<input type="checkbox"/> E <input type="checkbox"/> C
	<input type="checkbox"/> E <input type="checkbox"/> C	Servizio Dipendenze Patologiche	<input type="checkbox"/> E <input type="checkbox"/> C	Gestione del Rischio	<input type="checkbox"/> E <input type="checkbox"/> C
	<input type="checkbox"/> E <input type="checkbox"/> C	Farmacia Ospedaliera di	<input type="checkbox"/> E <input type="checkbox"/> C	Relazioni Sindacali	<input type="checkbox"/> E <input type="checkbox"/> C
	<input type="checkbox"/> E <input type="checkbox"/> C	U.O. di	<input type="checkbox"/> E <input type="checkbox"/> C		
	<input type="checkbox"/> E <input type="checkbox"/> C		<input type="checkbox"/> E <input type="checkbox"/> C		