SERVIZIO SANITARIO REGIONALE
ASL ROMA 1

DELIBERAZIONE DEL DIRETTORE GENERALE

N. 1094 **del** 11/06/2026

OGGETTO: Affidamento, ai sensi dell'art. 50 comma 1 lett. b) del D.Lgs. n. 36/2023, del servizio di Data Protection Officer (DPO) per la Asl Roma 1 per un importo pari ad € 119.200,00 IE - CIG BBDDBDCE14

STRUTTURA PROPONENTE: DIPARTIMENTO TECNICO PATRIMONIALE - UOC ACQUISIZIONE BENI E SERVIZI

Centro di Costo: BD0101 L'Estensore:Dott.ssa ALESSANDRA CALIENTO Il presente Atto non contiene dati sensibili

Il Dirigente e/o il Responsabile del procedimento, con la sottoscrizione del presente atto, a seguito dell'istruttoria effettuata, attestano che l'atto è legittimo nella forma e nella sostanza.

Il Responsabile del Procedimento	UOC ACQUISIZIONE BENI E SERVIZI	DIPARTIMENTO TECNICO PATRIMONIALE
BARBARA GENTILE	Dott.ssa CRISTINA FRANCO	Ing. PAOLA BRAZZODURO
Firmatario: BARBARA GENTILE Data: 08/06/2026 10:29:58 CEST	Il sostituto VITTORIO SANTORIELLO Data: 08/06/2026 12:28:14 CEST	Firmatario: PAOLA BRAZZODURO Data: 08/06/2026 12:44:06 CEST

Il funzionario addetto al controllo di budget, con la sottoscrizione del presente atto, attesta che lo stesso non comporta uno scostamento sfavorevole rispetto al budget economico assegnato come di seguito dettagliato per singolo conto:

Costo previsto	Eserciz.	CE/CP	Numero conto	Descrizione conto	Addetto al controllo	Scostamento
€84.830,67	2026	CE	502020189	Altri servizi non sanitari da privato	Ing. Paola Brazzoduro	no
€60.593,33	2027	CE	502020189	Altri servizi non sanitari da privato	Ing. Paola Brazzoduro	no

Il Funzionario addetto al controllo di budget

Ing. PAOLA BRAZZODURO

Firmatario: PAOLA BRAZZODURO
Data: 08/06/2026 12:42:54 CEST

Il Dirigente della UOC Pianificazione Strategica, Programmazione e Controllo di Gestione, con la sottoscrizione del presente atto attesta la coerenza della dichiarazione riferita alla spesa di cui al presente provvedimento del funzionario addetto al controllo del budget, rispetto alla Delibera n. 451 del 11/03/2026

Firmatario: GIORGIO BACCARI
Data: 08/06/2026 17:28:43 CEST

Parere del Direttore Amministrativo Dr. Francesco Quagliariello

Favorevole

Firmatario: FRANCESCO QUAGLIARIELLO
Data: 09/06/2026 08:36:08 CEST

(con motivazioni allegate al presente
Non favorevole

Parere del Direttore Sanitario Dr. Gennaro D'Agostino

Favorevole

Firmatario: GENNARO D'AGOSTINO
Data: 09/06/2026 15:34:02 CEST

(con motivazioni allegate al presente
Non favorevole

Il presente provvedimento si compone di n.21 pagine di cui n.16 pagine di allegati

Il Direttore Generale
Dr. Giuseppe Quintavalle

Firmatario: GIUSEPPE QUINTAVALLE
Data: 11/06/2026 10:12:18 CEST

REGIONE LAZIO

IL DIRETTORE DELLA U.O.C. ACQUISIZIONE BENI E SERVIZI

VISTA la deliberazione del Commissario Straordinario n. 1 del 1° gennaio 2016, con la quale si è provveduto a prendere atto dell'avvenuta istituzione dell'Azienda Sanitaria Locale Roma 1 a far data dal 1° gennaio 2016, come previsto dalla legge regionale n. 17 del 31dicembre 2015 e dal Decreto del Commissario ad acta n. 606 del 30 dicembre 2015;

il Decreto del Presidente della Regione Lazio 10 gennaio 2025, n. T00006 con il quale è stato nominato Direttore Generale dell'Azienda Sanitaria Locale Roma 1, il dott. Giuseppe Quintavalle;

nelle more della sua completa attuazione, che avverrà con opportuna gradualità, l'atto di autonomia aziendale approvato con Deliberazione n. 377 del 4.04.2025, approvato con Deliberazione di Giunta Regionale del 8 maggio 2025 n. 296 e pubblicato sul BURL n. 38 del 13/05/2025;

VISTA la Deliberazione n. 138 del 25.02.2025 avente ad oggetto "*Sistema aziendale di deleghe e conseguente individuazione delle competenze nell'adozione degli atti amministrativi*", con la quale, tra l'altro, sono state individuate le competenze nell'adozione degli atti amministrativi;

VISTO il Decreto Legislativo 31/03/2023 n. 36 e in particolare l'art. 50 comma 1 lett. b) che individua l'affidamento diretto quale strumento per le forniture e servizi di importo inferiore a € 140.000,00 Iva esclusa, anche senza la consultazione preliminare di più operatori economici, assicurando che siano scelti soggetti in possesso di documentate esperienze pregresse idonee all'esecuzione delle prestazioni contrattuali;

PREMESSO che con nota prot. n. 98981 del 28.05.2026 (all. 1) il Direttore della UOC Affari Generali, hanno chiesto l'attivazione di una procedura di gara finalizzata all'affidamento in oggetto per una durata di 12 mesi al fine di garantire la continuità di un servizio ritenuto essenziale;

CONSIDERATO che nel caso di specie si può attivare un affidamento diretto, in base a quanto disposto dall'art. 50 comma 1 lett. b) del D.Lgs. n. 36/2023 col criterio del minor prezzo;

DATO ATTO che, sulla base di quanto sopra evidenziato, in data 29.05/2026 si è provveduto, con registro di sistema PI116951-26 ad acquisire il CIG mediante il Sistema Telematico Acquisti della Regione Lazio STELLA e, conseguentemente, ad affidare il servizio di Data Protection Officer (DPO) per la Asl Roma 1 all'operatore economico Scudo Privacy srl, attestata la comprovata esperienza nelle attività richieste;

che l'operatore economico suddetto è stato individuato nell'elenco dei fornitori presenti sulla piattaforma di approvvigionamento digitale Stella della Regione Lazio "*in considerazione della conoscenza approfondita e consolidata del contesto organizzativo, tecnologico e dei flussi di dati dell'Azienda"*;

dell'offerta formulata dall'operatore economico Scudo Privacy srl - P. IVA 14769431009 - per un importo complessivo di € 119.200,00 iva esclusa (all. 2);

che l'importo stimato dell'appalto è per 12 mesi;

che a decorrere dall'1 gennaio 2024, l'acquisizione del CIG viene effettuata direttamente dalle piattaforme di approvvigionamento digitale certificate che gestiscono il ciclo di vita del contratto, mediante lo scambio di dati e informazioni con la BDNCP;

che, pertanto, è stato acquisito il seguente CIG BBDDBDCE14;

che, sulla base della verifica della rispondenza dei prodotti offerti ai requisiti tecnici indicati in sede di richiesta di preventivo, la struttura richiedente ha verificato la congruità del preventivo formulato dall'operatore economico sopra citato;

RITENUTO pertanto di approvare il preventivo presentato e procedere all'affidamento del servizio in trattazione, ai sensi dell'art. 50 comma 1 lett. b) del D.Lgs n. 36/2023 in favore di Scudo Privacy srl - P. IVA 14769431009 - soggetto in possesso di documentate esperienze pregresse idonee all'esecuzione delle prestazioni contrattuali per un importo complessivo di € 119.2000,00 Iva esclusa, tramite trattativa diretta Registro di sistema PI116951-26;

ATTESO che la spesa complessiva di € 145.424,00 iva al 22% inclusa, derivante dall'adozione del presente atto graverà sul conto economico 502020189 "Altri servizi non sanitari da privato" dal 1.06.2026 al 31.05.2027 secondo la ripartizione di seguito specificata

CE 502020189 "Altri servizi non sanitari da privato"	
01.06.2026 – 31.12.2026	84.830,67 €
01.01.2027 -31.05.2027	60.593,33 €

RILEVATO che in capo al soggetto risultato aggiudicatario, sono state attivate le procedure finalizzate alla verifica dell'assenza della cause di esclusione di cui agli articoli 94 e 95 del D.Lgs. n. 36/2023 e, pertanto, ai sensi dell'art. 17, co. 5;

CONSIDERATO che, ai sensi dell'articolo 55 co. 2 del Decreto, non si applicano i termini dilatori agli affidamenti dei contratti di importo inferiore alle soglie di rilevanza europea;

RITENUTO di provvedere all'assolvimento degli obblighi di pubblicità legale, ai sensi della Delibera ANAC n.582 del 13.12.2023 ed in conformità degli obblighi fissati dal D.Lgs. n. 36/2023, nonché di pubblicare l'esito della procedura in oggetto sul portale istituzionale aziendale sezione "Amministrazione Trasparente";

ATTESTATO che il presente provvedimento a seguito dell'istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo, utile e proficuo per il servizio pubblico ai sensi e per gli effetti di quanto disposto dall'art. 1 della Legge n. 20/1994 e successive modifiche nonché alla stregua dei criteri di economicità e di efficacia di cui all'art. 1, comma 1, della Legge 241/1990 e successive modifiche ed integrazioni;

PROPONE

Per i motivi e le valutazioni sopra riportate, che formano parte integrante del presente atto:

di procedere all'affidamento in favore di Scudo Privacy srl, con sede in Roma, via di Valle Lupara n.10, P. IVA 14769431009, del servizio in oggetto per un importo complessivo di € 145.424,00 iva al 22% inclusa;

di far gravare la spesa complessiva derivante dall'adozione del presente atto graverà sul conto economico 502020189 "Altri servizi non sanitari da privato" dal 1.06.2026 al 31.05.2027 secondo la ripartizione di seguito specificata

CE 502020189 “Altri servizi non sanitari da privato”	
01.06.2026 – 31.12.2026	84.830,67 €
01.01.2027 -31.05.2027	60.593,33 €

di provvedere all’assolvimento degli obblighi di pubblicità legale, ai sensi della Delibera ANAC n.582 del 13.12.2023 ed in conformità degli obblighi fissati dal D.Lgs. n. 36/2023, nonché di pubblicare l’esito della procedura in oggetto sul portale istituzionale aziendale sezione “Amministrazione trasparente”;

di dare atto che, in forza di quanto disposto dall'Atto Aziendale e dalla deliberazione n. 176 del 13.02.2024, l'unità organizzativa responsabile del procedimento per la fase esecutiva è individuata nella UOC Logistica e che, salvo successiva formale assegnazione ad altro dipendente addetto all’unità, l'attuale responsabile, Ing. Paola Brazzoduro, è individuata quale Responsabile unico del procedimento per la fase esecutiva dell'appalto - RUP 2, ai sensi del D.Lgs. n. 36/2023;

di demandare ai RUP 2 e DEC ogni adempimento conseguenziale nel rispetto della normativa vigente:

Conto economico	RUP 2	DEC
502020189	Ing. Paola Brazzoduro	Dott. ssa Gloria Ciccarelli

di disporre che il presente atto venga pubblicato in versione integrale nell’Albo Pretorio on line aziendale ai sensi dell’art. 32 comma 1 della Legge 18/06/2009 n. 69, nel rispetto comunque della normativa sulla protezione dei dati personali e autorizzare il competente servizio aziendale ad oscurare eventuali dati ritenuti non necessari rispetto alle finalità di pubblicazione.

Il Responsabile del Procedimento	Il Direttore della U.O.C. Acquisizione Beni e Servizi	Il Direttore del Dipartimento Tecnico Patrimoniale
Barbara Gentile	Dott.ssa Cristina Franco	Ing. Paola Brazzoduro
Firmato digitalmente	*Firmato digitalmente*	*Firmato digitalmente*

IL DIRETTORE GENERALE

In virtù dei poteri previsti:
dall’art. 3 del D.Lgs. 502/1992 e ss.mm.ii.;
dall’art. 8 della L.R. 18/1994 e ss.mm.ii.;
nonché delle funzioni e dei poteri conferitigli dal Decreto del presidente della Regione Lazio T00006 del 10/01/2025;

Letta la proposta di delibera sopra riportata presentata dal Dirigente Responsabile dell’Unità nel frontespizio indicata;

Preso atto che il Direttore della Struttura proponente il presente provvedimento, sottoscrivendolo, attesta che lo stesso, a seguito dell’istruttoria effettuata, nella forma e nella sostanza è totalmente legittimo, utile e proficuo per il servizio pubblico ai sensi e per gli effetti di quanto disposto dall’art. 1 della Legge n. 20/1994 e successive modifiche nonché alla stregua dei criteri di economicità e di efficacia di cui all’art. 1, comma 1, della Legge n. 241/1990 e successive modifiche ed integrazioni;

Acquisiti i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario riportati nel frontespizio;

DELIBERA

di adottare la proposta di deliberazione avente per oggetto "Affidamento, ai sensi dell'art. 50 comma 1 lett. b) del D.Lgs. n. 36/2023, del servizio di Data Protection Officer (DPO) per la Asl Roma 1 per un importo pari ad € 119.200,00 IE - CIG BBDDBDCE14" e conseguentemente, per i motivi e le valutazioni sopra riportate, che formano parte integrante del presente atto;

di procedere all'affidamento in favore di Scudo Privacy srl, con sede in Roma, via di Valle Lupara n.10, P. IVA 14769431009, del servizio in oggetto per un importo complessivo di € 145.424,00 iva al 22% inclusa;

di far gravare la spesa complessiva derivante dall'adozione del presente atto graverà sul conto economico 502020189 "Altri servizi non sanitari da privato" dal 1.06.2026 al 31.05.2027 secondo la ripartizione di seguito specificata

CE 502020189 "Altri servizi non sanitari da privato"	
01.06.2026 – 31.12.2026	84.830,67 €
01.01.2027 -31.05.2027	60.593,33 €

di provvedere all'assolvimento degli obblighi di pubblicità legale, ai sensi della Delibera ANAC n.582 del 13.12.2023 ed in conformità degli obblighi fissati dal D.Lgs. n. 36/2023, nonché di pubblicare l'esito della procedura in oggetto sul portale istituzionale aziendale sezione "Amministrazione trasparente";

di dare atto che, in forza di quanto disposto dall'Atto Aziendale e dalla deliberazione n. 176 del 13.02.2024, l'unità organizzativa responsabile del procedimento per la fase esecutiva è individuata nella UOC Logistica e che, salvo successiva formale assegnazione ad altro dipendente addetto all'unità, l'attuale responsabile, Ing. Paola Brazzoduro, è individuata quale Responsabile unico del procedimento per la fase esecutiva dell'appalto - RUP 2, ai sensi del D.Lgs. n. 36/2023;

di demandare ai RUP 2 e DEC ogni adempimento conseguenziale nel rispetto della normativa vigente:

Conto economico	RUP 2	DEC
502020189	Ing. Paola Brazzoduro	Dott. ssa Gloria Ciccarelli

di disporre che il presente atto venga pubblicato in versione integrale nell'Albo Pretorio on line aziendale ai sensi dell'art. 32 comma 1 della Legge 18/06/2009 n. 69, nel rispetto comunque della normativa sulla protezione dei dati personali e autorizzare il competente servizio aziendale ad oscurare eventuali dati ritenuti non necessari rispetto alle finalità di pubblicazione
La struttura proponente provvederà all'attuazione della presente deliberazione curandone altresì la relativa trasmissione agli uffici/organi rispettivamente interessati.

IL DIRETTORE GENERALE
Dott. Giuseppe Quintavalle
Firmata digitalmente

ASL ROMA 1

Dipartimento Amministrativo e delle Risorse Umane
UOC Affari Generali

PROT. 98981
DEL 28/05/2026

Al Direttore
UOC Acquisizione e Beni e Servizi
Dott.ssa Cristina Franco

E p.c. Direttore Amministrativo
Dr Francesco Quagliariello

Oggetto: richiesta di affidamento diretto per rinnovo del contratto stipulato con la società Scudo Privacy s.r.l. relativo al servizio di Data Protection Officer (DPO) per la Asl Roma – Del. n. 514/2024

Con riferimento all'oggetto in vista dell'imminente scadenza del contratto per il servizio di Data Protection Officer (DPO), previsto per il 31/05/2026, come da Delibera n. 514/2024, si rappresenta la necessità di garantire la continuità di tale supporto.
Si propone, a tal fine, di procedere ad un affidamento diretto del servizio all'attuale fornitore per una durata di 12 mesi, non prorogabile.
La presente nota intende illustrare le motivazioni tecniche e giuridiche che giustificano tale richiesta, radicate nella profonda e rapida evoluzione del quadro normativo, con particolare riferimento all'introduzione di una disciplina organica sull'Intelligenza Artificiale (IA).
Il panorama giuridico che regola il trattamento dei dati personali, e in particolare dei dati sanitari, è in una fase di significativa trasformazione a causa dell'adozione di nuove normative a livello europeo e nazionale sull'Intelligenza Artificiale. Tale evoluzione impone un'analisi approfondita e complessa per adeguare i processi, le tecnologie e le procedure contrattuali dell'Azienda. La preparazione di un capitolato di gara esaustivo e tecnicamente adeguato richiede, pertanto, un tempo di elaborazione non compatibile con la scadenza contrattuale.

Il Regolamento (UE) 2024/1689, noto come AI Act, ha introdotto un quadro giuridico armonizzato per lo sviluppo, l'immissione sul mercato e l'uso dei sistemi di IA, adottando un approccio basato sul rischio, imponendo requisiti specifici e stringenti per i "sistemi di IA ad alto rischio". Molti sistemi di IA impiegati o impiegabili in ambito sanitario rientrano in tale categoria, data la loro potenziale incidenza sulla salute e sui diritti dei pazienti. Ciò comporta per l'Azienda la necessità di implementare e richiedere ai propri fornitori nuove e complesse misure di conformità che dovranno essere dettagliatamente recepite in un futuro capitolato di gara.

In ambito nazionale, la Legge 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", introduce una disciplina settoriale di grande rilevanza per l' Asl Roma 1.
Queste disposizioni, unitamente a quelle previste per la ricerca scientifica e per l'istituzione di una piattaforma nazionale di IA gestita da AGENAS (Parere su uno schema di disegno di legge recante disposizioni e deleghe in materia di intelligenza artificiale - 2 agosto 2024), introducono obblighi specifici che devono essere attentamente valutati e integrati nei requisiti tecnici e contrattuali per i futuri fornitori.

La complessità del quadro è accentuata dalla necessità di coordinare la normativa nazionale con quella europea. Il Garante per la Protezione dei Dati Personali, nel suo parere sullo schema del disegno di legge italiano, ha evidenziato la necessità di integrare le disposizioni nazionali (in particolare l'art. 7) con i requisiti "ben più stringenti" previsti dall'AI Act per il trattamento di dati appartenenti a categorie particolari, come quelli sanitari, nell'ambito di sistemi ad alto rischio [Parere su uno schema di disegno di legge recante disposizioni e deleghe in materia di intelligenza artificiale - 2 agosto 2024]. Questo rilievo conferma che la definizione dei requisiti di conformità per l'IA in sanità è un'attività delicata e ancora in via di consolidamento, che richiede un supporto consulenziale esperto e continuo, ma non ancora determinabili con certezza.

L'evoluzione normativa descritta ha un impatto diretto e sostanziale sulle responsabilità di questa Azienda in qualità di titolare del trattamento. L'obbligo di adottare misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, sancito dall'art. 32 del Regolamento (UE) 2016/679 (GDPR), deve essere ricalibrato alla luce dei nuovi rischi introdotti dai sistemi di IA
Inoltre il modello privacy dovrà tener conto anche dgegli obblighi previsti in tema di cybersicurezza dalla normativa NIS2, che disciplina il sistema nazionale di vigilanza controllo e applicazione dell'Intelligenza Artificiale.
La redazione di un capitolato di gara che tenga conto di tale complessa cornice normativa non può risolversi in un mero aggiornamento del precedente. È necessario condurre un'analisi approfondita per:
- Mappare i trattamenti di dati attuali e futuri che potrebbero avvalersi di sistemi di IA.
- Classificare i sistemi di IA secondo le categorie di rischio dell'AI Act.
- Definire i requisiti tecnici, di sicurezza e di governance conformi sia al GDPR sia all'AI Act e alla normativa nazionale.
- Stabilire chiare ripartizioni di responsabilità tra l'Azienda (titolare) e il fornitore (responsabile del trattamento o a sua volta titolare).
Questa attività richiede competenze multidisciplinari e un'analisi che non può essere completata in tempi brevi senza esporre l'Azienda a significativi rischi di non conformità e a possibili contenziosi.

L'affidamento diretto all'attuale fornitore per un periodo limitato di 12 mesi si configura, pertanto, come una scelta tecnicamente necessaria per garantire la continuità di un servizio essenziale, mitigando i rischi legali e operativi in una fase di transizione normativa. L'attuale società, la Scudo privacy s.r.l., possiede una conoscenza approfondita e consolidata del contesto organizzativo, tecnologico e dei flussi di dati dell'Azienda, elemento indispensabile per supportare l'ente in questo periodo di transizione, per gestire le problematiche correnti e armonizzare le diverse attività sinora poste in essere.

Per le ragioni sopra esposte, si chiede di propone di procedere ad affidamento diretto del servizio di di Data Protection Officer (DPO) all'attuale fornitore, la Scudo privacy srl per la durata di 12 mesi, non rinnovabili.
Questo periodo sarà impiegato per porre in essere tutte le attività di analisi e studio necessarie alla predisposizione di un nuovo e articolato capitolato tecnico, che sia pienamente rispondente al consolidato quadro normativo del GDPR, della normativa in materia di Cybersicurezza e alle nuove, complesse sfide poste dalla regolamentazione dell'Intelligenza Artificiale.

L'occasione è gradita per porgere distinti saluti.

Il Direttore UOC Affari Generali
Dott.ssa Gloria Ciccarelli

Firmato digitalmente da: GLORIA CICCARELLI
Data: 28/05/2026 12:54:43

Allegato: Capitolato tecnico

SCUDO PRIVACY S.r.l.

Spett.le A.S.L.RM1

Via Ariosto n. 3

00185 - ROMA

c.a. Dottoressa Cristina Franco UOC Acquisizione Beni e Servizi

Oggetto: offerta *servizio DPO* , regolamento UE 679/2016.

Descrizione dell'offerta

Il servizio, in favore dello Spett.le Istituto di cui all'indirizzo, prevede l'individuazione di un DATA PROTECTION OFFICER, figura prevista dall'art. 37 del regolamento europeo in oggetto e i cui compiti possono così brevemente riassumersi:

a) informare e fornire consulenza all'Istituto in merito agli obblighi derivanti dal citato regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del citato regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

c) fornire pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo.

f) TUTTO quanto meglio dettagliato nella relazione tecnica allegata.

La nostra migliore offerta per le prestazioni di servizio sopra specificata, per la durata di anni uno, è di:

La nostra migliore offerta per le prestazioni di servizio sopra specificate, **è di € 119.200 (centodicianovemiladuecento euro)** + IVA

In attesa di un Vs. gentile riscontro alla presente, inviamo i nostri migliori saluti.

Roma, 28-05-2026

Scudo Privacy srl

Allegata: Relazione Tecnica

Sede Legale:
00148 Roma - Via di Valle Lupara, 10
C.F./P.IVA 14769431009
Telefono: 06-3221675

scudoprivacy@legalmail.it
segreteria@scudoprivacysrl.com

OFFERTA TECNICA

Servizio di Data Protection Officer (DPO) per la ASL Roma 1

Durata: 12 mesi

Relazione tecnica allegata al preventivo di spesa,
in risposta alla Richiesta di Preventivo della UOC Acquisizione Beni e Servizi

SCUDO PRIVACY S.r.l.
Via Cesare Fracassini n. 25, 00196 Roma
segreteria@scudoprivacysrl.com — www.scudoprivacy.com

Roma, 28/05/2026

1. PREMESSA

La Scudo Privacy S.r.l. presenta la presente relazione tecnica, allegata al preventivo di spesa, in risposta alla richiesta di preventivo formulata dalla ASL Roma 1 — UOC Acquisizione Beni e Servizi (a firma del Direttore Dott.ssa Cristina Franco) ai fini dell'affidamento del Servizio di Data Protection Officer (DPO) e dei servizi aggiuntivi ad esso connessi, ai sensi degli articoli 37 e ss. del Regolamento (UE) 2016/679 (di seguito anche "GDPR") e secondo le specifiche del Capitolato Tecnico allegato alla procedura.

Il presente documento descrive le caratteristiche tecnico-organizzative del servizio che la Scudo Privacy S.r.l. si impegna a erogare in favore della ASL Roma 1 per l'intera durata contrattuale (12 mesi), con riferimento puntuale a tutte le prescrizioni del Capitolato Tecnico e, in particolare:

- la presentazione della Società affidataria e il quadro delle qualificazioni possedute;
- l'esperienza maturata dalla Scudo Privacy S.r.l. nel settore sanitario pubblico, anche con riferimento al servizio attualmente in erogazione presso la stessa ASL Roma 1;
- l'individuazione del Referente Unico per la commessa;
- il possesso, da parte del personale impegnato sulla commessa, dei requisiti specifici di cui al § 3 del Capitolato Tecnico e all'art. 37, comma 5, del GDPR;

- le modalità operative di svolgimento dei servizi di cui alle lettere a), b), c) ed ai n. 25 punti elencati al § 2 del Capitolato Tecnico;
- il dimensionamento dell'impegno orario annuo, il piano di presa in carico, il cronoprogramma delle attività e la rendicontazione;
- gli strumenti metodologici e operativi adottati per garantire la migliore compliance al GDPR e l'integrazione con il Team Cyber Security aziendale, il CIO, il Responsabile NIS, l'Incaricato e il Referente tecnico PSNC, il Responsabile della transizione digitale e i consulenti tecnici aziendali.

Le caratteristiche del servizio sono qui di seguito enucleate in conformità a quanto previsto dalla richiesta di preventivo, in modo da consentire alla Stazione appaltante la valutazione tecnica integrata della proposta.

2. PRESENTAZIONE DELLA SOCIETÀ

La Scudo Privacy S.r.l. è una società di consulenza specializzata nell'erogazione di servizi di Data Protection Officer / Responsabile della Protezione dei Dati Personali, di consulenza tecnico-giuridica in materia di privacy e protezione dei dati personali e di assistenza in tema di sicurezza delle informazioni, con particolare riferimento alle Pubbliche Amministrazioni e, in via prevalente, agli Enti del Servizio Sanitario Nazionale.

La Società nasce per dare risposta integrata al dettato del GDPR e alle ulteriori discipline europee e nazionali in tema di Data Governance, sicurezza cibernetica e nuove tecnologie (Direttiva NIS2, AI Act, normativa ACN/AgID), in un contesto in cui le potenzialità applicative delle tecnologie — inclusa l'intelligenza artificiale — devono essere coniugate con la piena tutela dei diritti e delle libertà degli interessati.

L'attività della Scudo Privacy S.r.l. soddisfa due esigenze tra loro complementari: (i) l'osservanza del dettato normativo a tutela del dato personale e delle informazioni, sotto il profilo legale; (ii) la tutela effettiva dei dati attraverso l'adozione di procedure, policy e strumenti tecnico-informatici dedicati alla protezione delle reti, degli archivi digitali e dei sistemi informativi.

Le competenze del Gruppo di lavoro proposto derivano da una pluriennale esperienza giuridica e tecnica, da qualificazioni internazionali in tema di sicurezza delle informazioni e protezione dei dati (CISA, CDPSE, Lead Auditor ISO/IEC 27001, Lead Auditor ISO 22301, Trainer accreditato BSI per ISO/IEC 27001:2022, ISO 22301:2019 e ISO/IEC 42001:2023, qualifica DPO ai sensi della norma UNI 11697:2017), nonché dalla collaborazione con organismi nazionali ed internazionali dedicati allo studio delle procedure di contrasto al cybercrime ed al fenomeno del Data Breach.

La Scudo Privacy S.r.l. è certificata ISO 9001:2015 per le attività di consulenza tecnico-giuridica, servizi di Data Protection Officer, servizi di formazione e attività connesse, ed è dotata di una struttura organizzativa stabile dedicata al settore sanitario, in grado di interfacciarsi efficacemente con le strutture organizzative, i Team Cyber Security, i Referenti NIS e i Responsabili della Transizione Digitale degli Enti committenti.

2.1 Dati identificativi

Denominazione sociale	Scudo Privacy S.r.l.
Sede legale e operativa	Via Cesare Fracassini n. 25, 00196 Roma
Contatti	segreteria@scudoprivacysrl.com — www.scudoprivacy.com

Certificazione di Sistema di Gestione per la Qualità	UNI EN ISO 9001:2015
Specializzazione	Servizi di DPO, consulenza tecnico-giuridica privacy, sicurezza delle informazioni, formazione — prevalentemente per Enti del SSN e Pubbliche Amministrazioni

3. ESPERIENZA SPECIFICA NEL SETTORE SANITARIO PUBBLICO

La Scudo Privacy S.r.l. ha maturato una significativa esperienza nell'erogazione del servizio di Data Protection Officer e di assistenza al DPO presso Aziende Sanitarie Locali, IRCCS, Aziende Ospedaliere ed Enti di ricerca del Servizio Sanitario Nazionale, integralmente prestata presso Enti pubblici.

La sintesi degli incarichi maturati è la seguente:

N.	Ente / Amministrazione	Natura	Periodo	Tipologia del servizio
1	ASL Roma 4	Ente pubblico	23/05/2018 – 31/12/2025	Servizio di RPD/DPO
2	ASL Roma 5	Ente pubblico	01/07/2019 – 31/07/2024	Servizio di RPD/DPO
3	ASL Napoli 3 Sud	Ente pubblico	01/04/2019 – 30/04/2021	Servizio di RPD/DPO
4	IFO IRCCS (IRE & ISG) – Roma	Ente pubblico	11/05/2018 – 31/12/2023	Servizio di RPD/DPO
5	ASP Cosenza	Ente pubblico	01/01/2020 – in corso	Servizio di RPD/DPO
6	ASL ROMA 1	Ente pubblico	01/06/2022 – in corso	Servizio di RPD/DPO
7	ASL Roma 3	Ente pubblico	01/08/2022 – 31/05/2025	Servizio di RPD/DPO
8	ASL Roma 6	Ente pubblico	01/06/2024 – 30/06/2025	Servizio di RPD/DPO
9	INMI Lazzaro Spallanzani – Roma	Ente pubblico	01/11/2024 – in corso	Servizio di RPD/DPO
10	Istituto Superiore di Sanità (ISS)	Ente pubblico	01/01/2020 – 30/06/2024	Servizio di RPD/DPO

N.	Ente / Amministrazione	Natura	Periodo	Tipologia del servizio
11	Ospedale San Giovanni Addolorata – Roma	Ente pubblico	01/03/2026 – in corso	Servizio di RPD/DPO
12	Polo Oncologico – Bari (IRCCS Giovanni Paolo II)	Ente pubblico	01/06/2024 – in corso	Assistenza al DPO
13	ASL Toscana Sud-Est	Ente pubblico	01/04/2022 – 31/03/2023	Assistenza al DPO
14	Policlinico Universitario di Messina "G. Martino"	Ente pubblico	01/04/2025 – in corso	Assistenza al DPO
15	IFO IRCCS (IRE & ISG) – Roma	Ente pubblico	01/07/2024 – in corso	Servizio di RPD/DPO
	TOTALE	**Enti pubblici**	—	**n. 15 incarichi**

3.1 Continuità del servizio presso la ASL Roma 1

Si segnala in particolare che la Scudo Privacy S.r.l. è attualmente affidataria del Servizio di Data Protection Officer presso la stessa ASL Roma 1, in continuità dal 1° giugno 2022. Tale circostanza determina un evidente vantaggio operativo a favore della Stazione appaltante in caso di affidamento del nuovo servizio.

Nel corso del servizio attualmente erogato, la Scudo Privacy S.r.l. ha maturato una conoscenza diretta:

- dell'organizzazione interna della ASL Roma 1 e dei flussi di trattamento dei dati personali svolti dalle singole strutture aziendali;
- del Gruppo di Coordinamento Privacy aziendale e del Team Cyber Security aziendale, con i quali la Società già collabora stabilmente;
- delle interfacce funzionali con il CIO, il Responsabile NIS, l'Incaricato e il Referente tecnico PSNC, il Responsabile della transizione digitale e i consulenti tecnici aziendali;
- degli strumenti documentali aziendali in uso, ivi compresi i Registri delle attività di trattamento del Titolare e del Responsabile (ex art. 30 GDPR), il Data Breach Inventory, le procedure di DPIA, la modulistica privacy e i provvedimenti del Garante che hanno interessato l'Ente;
- delle piattaforme aziendali — incluse la piattaforma FAD e quella web di pubblicazione dei dati di contatto del DPO — utilizzate ai fini dell'erogazione del servizio.

Tale conoscenza pregressa assicura, in caso di nuovo affidamento, la piena continuità operativa senza fasi di apprendimento organizzativo e senza alcun rischio di interruzione nella tutela degli interessati, conformemente agli obblighi di cooperazione previsti dall'art. 38 del GDPR e alle prescrizioni del § 4 del Capitolato Tecnico in tema di passaggio di consegne.

La Scudo Privacy S.r.l. attesta, ai fini del requisito specifico di cui al § 3 del Capitolato Tecnico ("partecipazione ad esperienze lavorative rese in ambito pubblico, per non meno di n. 2 incarichi da DPO nel settore sanitario"), il possesso

del relativo requisito in misura ampiamente superiore al minimo richiesto, avendo svolto e/o svolgendo n. 15 incarichi presso Enti pubblici del settore sanitario.

4. POSSESSO DEI REQUISITI SPECIFICI DEL PERSONALE

Il § 3 del Capitolato Tecnico prescrive, a pena di esclusione, il possesso da parte del personale impegnato sulla commessa di specifici requisiti di competenza ed esperienza in coerenza con l'art. 37, comma 5, del GDPR. La Scudo Privacy S.r.l. attesta il possesso integrale dei requisiti richiesti, come di seguito sinteticamente rappresentato.

Requisito di cui al § 3 del Capitolato	Modalità di adempimento da parte della Scudo Privacy S.r.l.
Conoscenza specialistica della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del GDPR	Il Gruppo di lavoro è costituito in prevalenza da avvocati specializzati in privacy e data protection, con consolidata esperienza nella redazione di pareri e nella consulenza giuridico-legale ex GDPR, D.Lgs. 196/2003 e ss.mm.ii. presso Enti del SSN.
Familiarità con le operazioni di trattamento svolte (settore sanitario)	La Scudo Privacy S.r.l. opera in via prevalente nel settore sanitario pubblico, con n. 15 incarichi maturati presso ASL, IRCCS, Aziende Ospedaliere ed Enti di ricerca, ivi inclusa la ASL Roma 1 (in continuità dal 2022).
Familiarità con tecnologie informatiche e misure di sicurezza dei dati	Il Gruppo di lavoro include esperti in sicurezza dei flussi delle informazioni e cybersecurity.
Conoscenza dello specifico settore di attività e dell'organizzazione del titolare/del responsabile	Conoscenza diretta dell'organizzazione della ASL Roma 1 derivante dai 48 mesi di servizio attualmente in erogazione presso la medesima Azienda.
Capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione	La Società dispone di un team con qualificate competenze di docenza e formazione (universitaria, accreditata BSI e in contesti convegnistici nazionali e internazionali) e di una metodologia consolidata per la diffusione della cultura della protezione dei dati.

Il DPO e il Referente Unico, così come tutti i componenti del Gruppo di lavoro, dichiarano di non svolgere o aver svolto incarichi, compiti o funzioni che diano luogo a conflitto di interessi con le attività ed i compiti previsti dal Capitolato Tecnico.

5. REFERENTE UNICO

Quale Referente Unico ai sensi del § 3 del Capitolato Tecnico — figura cui sono demandati il coordinamento del personale operante sulla commessa, l'interlocuzione costante con la ASL Roma 1, la disponibilità dei dati di contatto ai fini della pubblicazione sul sito istituzionale e nella sezione "Amministrazione trasparente", nonché la comunicazione al Garante per la Protezione dei Dati Personali — la Scudo Privacy S.r.l. propone il seguente nominativo:

Referente Unico	[CARLO VILLANACCI]
Qualifica professionale	[DPO certificato UNI 11697:2017]
Recapito postale dedicato	Via Cesare Fracassini n. 25, 00196 Roma
Telefono dedicato	[06/3221675]
Indirizzo PEC dedicato	[scudoprivacy@legalmail.com]
Indirizzo e-mail dedicato	[backoffice@scudoprivacysrl.com]

Il Referente Unico appartiene alla struttura organizzativa della Scudo Privacy S.r.l. fin dal momento della presentazione della presente offerta e possiede le caratteristiche di cui all'art. 37, comma 5, del GDPR, nonché i requisiti specifici previsti dal § 3 del Capitolato Tecnico.

Il Referente Unico esprime sin d'ora — in sede di avvio del contratto — il proprio consenso alla diffusione dei dati identificativi e al conseguente trattamento, qualora questo avvenga per espressa disposizione di legge, ai sensi del § 3 del Capitolato.

La Scudo Privacy S.r.l. garantisce che almeno il 40% delle 230 giornate annue di impegno previste dal Capitolato — pari ad almeno 92 giornate annue di 8 ore ciascuna — sarà svolto direttamente dal Referente Unico, in conformità al § 2 del Capitolato Tecnico.

In caso di forza maggiore che imponga, nel corso del periodo di validità del contratto, l'individuazione di un Referente Unico sostitutivo, la Scudo Privacy S.r.l. assicura che il sostituto possiederà competenza ed esperienza almeno pari a quelle del Referente Unico originariamente proposto, in conformità a quanto previsto dal § 3 del Capitolato.

6. SERVIZI OGGETTO DI AFFIDAMENTO

Conformemente al § 2 del Capitolato Tecnico, i servizi che la Scudo Privacy S.r.l. si impegna a erogare in favore della ASL Roma 1 ricomprendono le tre macro-aree di seguito declinate (lett. a, b, c), nell'ambito delle quali sono svolte le n. 25 attività specifiche dettagliate dal medesimo Capitolato, descritte al successivo § 7.

6.1 Attività di Data Protection Officer (lett. a)

La Scudo Privacy S.r.l. assicura l'integrale svolgimento dei compiti del Data Protection Officer previsti dall'art. 39 del GDPR, in coerenza con i principi e le prescrizioni di cui agli artt. 5, 6 (principi e liceità del trattamento), 12, 13, 14 (informazioni agli interessati), 7 c. 3 e da 15 a 23 (diritti degli interessati), 24 e 25 (responsabilità e principi di protezione, ivi inclusi privacy by design e by default), 28 (nomina dei responsabili), 30 (registri dei trattamenti), 32 (sicurezza dei trattamenti), 33 e 34 (violazioni dei dati personali), 35 e 36 (valutazioni di impatto e consultazione preventiva), da 40 a 43 (codici di condotta e certificazioni), da 44 a 49 (trasferimenti extra-UE), 83 e 84 (sanzioni) e da 86 a 90 (situazioni particolari di trattamento) del GDPR, in armonizzazione con le indicazioni del Comitato Europeo per la Protezione dei Dati (EDPB) e con i provvedimenti del Garante per la protezione dei dati personali.

6.2 Redazione e supporto in materia di sicurezza informatica e protezione dei dati (lett. b)

La Scudo Privacy S.r.l. supporta la ASL Roma 1 nella redazione, diffusione e formazione in merito alle procedure interne in materia di sicurezza informatica e protezione dei dati personali, in conformità a: D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e ss.mm.ii.; D.Lgs. 18 maggio 2018, n. 65 (attuazione della Direttiva NIS); Direttiva (UE) 2022/2555 (NIS2) e relativi atti di recepimento; Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015 "Misure minime di sicurezza ICT per le Pubbliche Amministrazioni"; Linee Guida e Misure Minime di sicurezza ICT adottate da AgID; provvedimenti dell'Agenzia per la Cybersicurezza Nazionale (ACN).

6.3 Partecipazione al Team Cyber Security aziendale (lett. c)

La Scudo Privacy S.r.l. garantisce la partecipazione costante, in qualità di membro permanente, alle riunioni programmate e straordinarie del Team Cyber Security aziendale e fornisce supporto alla redazione degli atti definiti nell'ambito del Team, in stretto coordinamento con il CIO, il Responsabile NIS, l'Incaricato e Referente tecnico PSNC, il Responsabile della transizione digitale e i consulenti tecnici aziendali, conformemente al § 2 del Capitolato Tecnico.

7. MODALITÀ OPERATIVE DI SVOLGIMENTO

Di seguito sono descritte le modalità operative con cui la Scudo Privacy S.r.l. assicura lo svolgimento delle attività di cui al § 2 del Capitolato Tecnico. Le attività sono raggruppate per macro-aree tematiche, con riferimento espresso ai punti numerati del Capitolato.

7.1 Analisi iniziale e relazione di gap analysis (punto 1)

Entro 30 giorni dall'affidamento del servizio, la Scudo Privacy S.r.l. consegnerà alla ASL Roma 1 una relazione che evidenzi il grado di conformità complessivo dell'Ente agli adempimenti in materia di trattamento e sicurezza dei dati personali e le azioni da intraprendere per garantire la protezione dei dati. In considerazione della continuità del servizio (vedi § 3.1), tale relazione potrà valorizzare l'analisi già condotta e gli aggiornamenti intervenuti nel corso del precedente affidamento, includendo una verifica integrata degli adempimenti, una mappatura delle azioni di rafforzamento in corso e l'individuazione delle priorità per i 12 mesi contrattuali.

7.2 Rilevazione e catalogazione dei trattamenti (punto 2)

La Società assicura la nuova rilevazione e catalogazione dei trattamenti di dati svolti dall'Ente attraverso l'esame della documentazione aziendale, l'accesso diretto agli uffici e il confronto con i Direttori e Responsabili di Struttura e con i Presidenti e Coordinatori di Organismi e Comitati dell'Ente.

7.3 Tenuta dei Registri delle attività di trattamento ex art. 30 GDPR (punto 3)

La Scudo Privacy S.r.l. cura la tenuta dei Registri delle attività di trattamento del Titolare e del Responsabile, previsti dall'art. 30 commi 1 e 2 del GDPR, sotto la responsabilità della ASL Roma 1 e sulla base delle informazioni fornite dalla stessa, attenendosi alle istruzioni impartite ed utilizzando gli strumenti messi a disposizione dall'Azienda.

7.4 Risk Assessment e valutazione d'impatto sulla protezione dei dati (DPIA) (punti 5 e 6)

La Società struttura, tenendo conto delle Linee Guida AgID, del DPCM 15 giugno 2021, di quanto già predisposto a livello aziendale per l'applicazione del D.Lgs. 65/2018 e delle ulteriori indicazioni della ASL Roma 1, un processo di analisi del rischio (risk assessment) per tutti i trattamenti, con particolare riferimento alla valutazione di probabilità di accadimento delle minacce e alla gravità (impatto) dei relativi eventi sui diritti e le libertà degli interessati. L'attività è svolta di concerto con la funzione di Risk Management aziendale e con le ulteriori funzioni indicate al § 2 del Capitolato.

In ambito DPIA (art. 35 GDPR), la Scudo Privacy S.r.l. supporta il Titolare nell'individuazione dei casi in cui sia necessario effettuare la valutazione d'impatto; fornisce indicazioni metodologiche per lo svolgimento delle DPIA ritenute necessarie e collabora con il Titolare ed il Referente NIS alla loro stesura; valuta le salvaguardie da applicare (incluse le misure tecniche ed organizzative) per attenuare i rischi; esamina la correttezza delle DPIA effettuate dal Titolare verificandone la conformità ai requisiti del Regolamento; riesamina periodicamente le DPIA effettuate e la necessità di effettuarne ulteriori.

7.5 Verifica dell'efficacia delle misure tecniche ed organizzative (punto 7)

La Società elabora procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento dei dati personali, in coerenza con i principi di accountability e con le best practice in materia di Information Security Management.

7.6 Trasferimenti dei dati in Paesi terzi (punto 8)

La Scudo Privacy S.r.l. definisce le procedure e le misure di sicurezza da adottare per il trasferimento dei dati in Paesi terzi (extra-UE), in conformità agli artt. 44-49 del GDPR e alle decisioni di adeguatezza, Clausole Contrattuali Standard e ulteriori meccanismi di trasferimento adottati dalla Commissione Europea e dal Garante.

7.7 Regolamentazione interna, policy, modulistica e gestione dei Responsabili del trattamento (punti 9, 10, 11, 12)

La Società fornisce assistenza e supporto operativo nella predisposizione e nell'adeguamento della regolamentazione aziendale, delle linee guida, delle disposizioni operative, della modulistica, delle informative e delle policy applicative in materia di protezione dei dati personali e sicurezza informatica. Definisce e supporta la redazione delle procedure e della modulistica per l'elaborazione e il controllo degli atti di nomina di responsabili del trattamento, delegati e autorizzati al trattamento e amministratori di sistema. Cura il monitoraggio e l'aggiornamento della procedura di gestione degli affidamenti che comportano un trattamento di dati personali a Responsabili del trattamento.

7.8 Pareristica e bilanciamento tra riservatezza e diritto di accesso (punto 13)

La Scudo Privacy S.r.l. formula pareri giuridici in tema di bilanciamento tra riservatezza e diritto di accesso, sia documentale che civico (ai sensi della L. 241/1990, del D.Lgs. 33/2013 e ss.mm.ii.), tenendo conto delle Linee Guida ANAC e dei provvedimenti del Garante.

7.9 Punto di contatto per gli interessati e con il Garante (punti 14 e 15)

La Società garantisce la possibilità per gli interessati di contattare il DPO per tutte le questioni relative al trattamento dei dati e all'esercizio dei diritti derivanti dal GDPR, anche tramite apposito servizio di assistenza remota. Funge da punto di

contatto con il Garante per la protezione dei dati personali per le questioni connesse al trattamento, ivi inclusa la consultazione preventiva di cui all'art. 36 GDPR, ed effettua, se del caso, le ulteriori consultazioni.

7.10 Gestione e analisi dei Data Breach (punti 4, 16, 24)

La Scudo Privacy S.r.l. cura: la tenuta della documentazione sulle violazioni dei dati personali prevista dall'art. 33 c. 5 del GDPR; la revisione del processo di rilevazione e notificazione delle violazioni (data breach) ai sensi degli artt. 33 e 34 del GDPR; la collaborazione con i DPO di eventuali Contitolari o Responsabili del trattamento nella gestione del breach; la predisposizione della notifica del Data Breach all'Autorità di Controllo e agli interessati nei termini previsti dal GDPR; il monitoraggio del processo di gestione del breach in ottica di continuous improvement; il monitoraggio e controllo della tenuta del Data Breach Inventory.

7.11 Privacy by Design / by Default e Security by Design (punto 25)

La Società supporta il Titolare e il CIO nell'integrazione, nei processi interni, dei principi di Privacy by Design e Privacy by Default ex art. 25 GDPR, nonché del principio di Security by Design in fase di progettazione, evoluzione o verifica degli applicativi utilizzati nell'ambito del trattamento di dati personali, monitorando l'effettiva implementazione degli stessi.

7.12 Formazione e sensibilizzazione (punti 17 e 18)

La Scudo Privacy S.r.l. progetta e gestisce il piano di formazione delle persone delegate e autorizzate al trattamento, assumendo in proprio la gestione di sessioni formative svolte presso la sede aziendale per un ammontare pari ad almeno 40 ore annue, anche tramite l'utilizzo della piattaforma FAD aziendale. Le attività formative ricomprendono: aggiornamenti su obblighi derivanti dal GDPR e dalla disciplina nazionale; novità normative e provvedimenti del Garante; profili specifici della protezione dei dati nel settore sanitario; tematiche di sicurezza ICT e cyber awareness.

7.13 Rendicontazione trimestrale e relazione annuale (punti 20 e 21)

La Società redige una relazione annuale, da consegnare entro la fine di ogni anno solare, contenente le proprie valutazioni sullo stato del sistema di protezione dei dati personali, sul rispetto dei diritti degli interessati e sull'efficacia delle procedure di informazione e controllo, con eventuali rilievi e suggerimenti operativi. Compila inoltre, entro il 15 del mese successivo alla fine di ciascun trimestre dell'anno solare, un rendiconto che documenti adeguatamente lo svolgimento dei compiti del DPO previsti dall'art. 39 GDPR nel periodo di riferimento, con particolare riferimento ai compiti di cui all'art. 39 c. 1 lett. b).

7.14 Supporto in controversie e collaborazione interfunzionale (punti 19, 22, 23)

La Scudo Privacy S.r.l. assiste e supporta la ASL Roma 1 nei rapporti e nelle eventuali controversie con Contitolari, Titolari autonomi, Responsabili nominati, Titolari che hanno nominato la ASL Roma 1 quale Responsabile del trattamento e, quando richiesto, con l'Autorità di controllo. Collabora proattivamente con le strutture organizzative dell'Ente per la risoluzione dei problemi relativi alla protezione dei dati personali e, quando necessario, con le altre Società incaricate di fornire supporto in ambito tecnico, organizzativo, formativo e legale. Partecipa, ove richiesto dall'Ente, ad incontri con altri soggetti per attività correlate alle precedenti.

8. IMPEGNO ORARIO E DIMENSIONAMENTO DEL SERVIZIO

La Scudo Privacy S.r.l. si impegna a garantire, per tutta la durata dell'incarico, l'impegno orario minimo prescritto dal § 2 del Capitolato Tecnico, secondo il seguente dimensionamento:

La Scudo Privacy S.r.l. garantisce la continuità del servizio per tutta la durata dell'incarico, anche durante eventuali periodi di indisponibilità del Referente Unico, attraverso il Team di supporto. I dati di contatto del Referente Unico saranno tempestivamente forniti ed aggiornati ai fini dell'inserimento negli atti e nei documenti della ASL Roma 1, della pubblicazione sul sito istituzionale e nella sezione "Amministrazione trasparente" e della comunicazione al Garante.

9. PIANO DI PRESA IN CARICO E CRONOPROGRAMMA

La presa in carico del servizio è progettata in coerenza con il § 2 del Capitolato Tecnico e con il contesto operativo già consolidato con la ASL Roma 1. Si articola nelle seguenti fasi temporali.

Fase	Tempistica	Attività principali
Fase 1 — Avvio	T0 — entro 15 gg	Formalizzazione del Referente Unico e dei componenti del Gruppo di lavoro; comunicazione dei recapiti dedicati; allineamento con il Gruppo di Coordinamento Privacy aziendale, il Team Cyber Security, il CIO, il Responsabile NIS, il Referente PSNC e il RTD.
Fase 2 — Gap analysis	Entro T0 + 30 gg	Consegna della relazione di analisi sullo stato di conformità (punto 1 del Capitolato), con piano di azioni e priorità per i 12 mesi contrattuali.
Fase 3 — Operatività ordinaria	Da T0 + 30 gg al termine	Erogazione delle attività di DPO (artt. 37-39 GDPR) e dei servizi di cui ai punti 2-19 e 22-25 del Capitolato; partecipazione costante al Team Cyber Security; formazione annuale (≥ 40 ore); pareristica; supporto a DPIA, risk assessment e gestione data breach.
Fase 4 — Rendicontazione	Trimestrale + annuale	Rendiconti trimestrali entro il 15 del mese successivo a ciascun trimestre solare (punto 21); relazione annuale entro fine anno solare (punto 20); approvazione preventiva dei rendiconti ai fini della fatturazione.

Fase	Tempistica	Attività principali
Fase 5 — Eventuale prosecuzione	Fino a +6 mesi post-scadenza	Garanzia di prosecuzione del servizio per il tempo strettamente necessario all'individuazione del nuovo DPO (§ 4 Capitolato), con presidio del passaggio di consegne.

10. METODOLOGIA OPERATIVA E STRUMENTI

La Scudo Privacy S.r.l. eroga il servizio avvalendosi di un set strutturato di strumenti metodologici e operativi, mutuati dalle migliori prassi nazionali ed internazionali e già consolidato nel corso degli incarichi pregressi nel settore sanitario.

- Metodologia di Risk Assessment conforme alle Linee Guida AgID, al DPCM 15 giugno 2021, alla norma ISO/IEC 27005 e al framework ENISA, con scoring di probabilità e impatto e valutazione dei rischi sui diritti e libertà degli interessati.
- Metodologia DPIA conforme alle Linee Guida WP248 dell'ex Gruppo "Art. 29" e ai criteri del Garante, con modulistica strutturata per soglie di valutazione, mappatura degli stakeholder, individuazione delle misure di mitigazione e tracciamento del processo decisionale.
- Strumenti documentali per la tenuta dei Registri ex art. 30 GDPR (Registro del Titolare e Registro del Responsabile), con versioning, audit-trail e mappatura tra trattamenti, basi giuridiche, dati, soggetti coinvolti e misure tecniche/organizzative.
- Procedura di gestione del Data Breach (artt. 33-34 GDPR) con flow di rilevazione, contenimento, valutazione del rischio per gli interessati, notifica al Garante entro 72 ore, comunicazione agli interessati ove richiesto, tenuta del Data Breach Inventory e attività di lessons learned.
- Sistema strutturato di gestione delle richieste di esercizio dei diritti degli interessati (artt. 15-22 GDPR), con tracciatura e rispetto dei termini di riscontro.
- Procedura di due diligence sui Responsabili del trattamento (art. 28 GDPR) e relativi accordi (DPA), con monitoraggio periodico della conformità dei fornitori.
- Sistema strutturato di pareristica giuridica per quesiti formali ed informali, con archiviazione e ricerca per materia.
- Sistema integrato di formazione (presenza + FAD aziendale) con valutazione di efficacia dell'apprendimento.

11. AGGIORNAMENTO PROFESSIONALE CONTINUO DEL TEAM

In conformità all'obbligo prescritto dal § 3 del Capitolato Tecnico, la Scudo Privacy S.r.l. assicura l'aggiornamento professionale continuo del personale impegnato sulla commessa, sotto i seguenti profili:

- aggiornamento normativo e regolamentare: monitoraggio continuo dei provvedimenti del Garante, delle Linee Guida EDPB, delle pronunce della Corte di Giustizia UE, della normativa europea e nazionale di settore (GDPR, NIS2, AI Act, normativa di settore sanitario);

- aggiornamento settoriale: confronto con le prassi e i codici di condotta in uso nel settore sanitario, monitoraggio delle direttive AgID e ACN e dei provvedimenti del Dipartimento per la Trasformazione Digitale rilevanti per le Aziende Sanitarie.

La Scudo Privacy S.r.l. assicura che il Referente Unico e i componenti del Team di supporto siano sempre adeguatamente istruiti e informati sulla legislazione vigente, sulle direttive dell'Autorità di controllo, sull'approvazione dei codici di condotta di cui all'art. 40 del GDPR, sull'evoluzione tecnologica degli strumenti di sicurezza informatici e sulle pratiche di protezione dei dati in uso nel settore sanitario.

12. TAVOLA DI RISPONDENZA AL CAPITOLATO TECNICO

La tavola che segue riepiloga, per ciascun punto numerato del § 2 del Capitolato Tecnico (n. 25 attività), il riferimento alla sezione della presente relazione tecnica in cui ne sono descritte le modalità di adempimento da parte della Scudo Privacy S.r.l.

Punto	Attività richiesta dal Capitolato (sintesi)	Sezione della presente relazione
1	Analisi assetto complessivo e relazione di conformità entro 30 gg	§ 7.1
2	Rilevazione e catalogazione dei trattamenti	§ 7.2
3	Tenuta dei Registri ex art. 30 GDPR (Titolare e Responsabile)	§ 7.3
4	Documentazione sulle violazioni dei dati ex art. 33 c. 5 GDPR	§ 7.10
5	Processo di analisi del rischio (risk assessment)	§ 7.4
6	DPIA ex art. 35 GDPR (parere e sorveglianza)	§ 7.4
7	Verifica efficacia misure tecniche ed organizzative	§ 7.5
8	Procedure per il trasferimento dati extra-UE	§ 7.6
9	Adeguamento regolamentazione interna alla normativa privacy	§ 7.7
10	Linee guida, modulistica, informative e policy applicative	§ 7.7
11	Procedure di nomina responsabili, delegati, autorizzati, AdS	§ 7.7
12	Gestione affidamenti a Responsabili del trattamento	§ 7.7
13	Pareri su bilanciamento riservatezza / diritto di accesso	§ 7.8
14	Punto di contatto per gli interessati (anche da remoto)	§ 7.9
15	Punto di contatto con il Garante; consultazione preventiva ex art. 36	§ 7.9
16	Revisione processo rilevazione/notificazione data breach (artt. 33-34)	§ 7.10

Punto	Attività richiesta dal Capitolato (sintesi)	Sezione della presente relazione
17	Piano di formazione (≥ 40 ore annue; anche FAD)	§ 7.12 — § 8
18	Informazione/sensibilizzazione su obblighi GDPR e novità normative	§ 7.12
19	Attività correlate / partecipazione ad incontri	§ 7.14
20	Relazione annuale entro fine anno solare	§ 7.13 — § 8
21	Rendiconto trimestrale entro il 15 del mese successivo	§ 7.13 — § 8
22	Supporto in rapporti/controversie con Contitolari, Responsabili, ecc.	§ 7.14
23	Collaborazione interfunzionale con strutture aziendali e altre Società	§ 7.14
24	Gestione e analisi data breach (notifica Autorità e interessati)	§ 7.10
25	Privacy by Design / by Default e Security by Design (art. 25 GDPR)	§ 7.11

La Scudo Privacy S.r.l. si impegna ad eseguire le prestazioni oggetto dell'incarico a regola d'arte, nel rispetto delle norme vigenti e secondo le condizioni, le modalità, i termini e le prescrizioni contenute nel Capitolato Tecnico e negli ulteriori atti della procedura, ivi inclusi gli obblighi in materia di tracciabilità dei flussi finanziari ai sensi della Legge 13 agosto 2010, n. 136 e ss.mm.ii. (§ 6 Capitolato), nonché gli ulteriori obblighi reciproci di cui ai §§ 5 e seguenti del Capitolato medesimo.

Roma, [28/05/2026]

Per la SCUDO PRIVACY S.r.l.

Il Legale Rappresentante

[firmato digitalmente]