



AZIENDA SANITARIA LOCALE DI PESCARA
Via Renato Paolini, 47 – 65124 Pescara (PE)

**DELIBERAZIONE DEL DIRETTORE GENERALE
AZIENDA SANITARIA LOCALE DI PESCARA**

ANNO: 2026

N. 1555

Data 05/10/2026

OGGETTO: APPROVAZIONE SCHEMA DI ACCORDO DI COLLABORAZIONE PER LO SVILUPPO DEL PROGETTO “ CAROVANA DELLA PREVENZIONE” E DETERMINAZIONI CONSEGUENTI.

IL DIRETTORE GENERALE

OGGETTO: approvazione schema di accordo di collaborazione per lo sviluppo del progetto “**Carovana della Prevenzione**” e determinazioni conseguenti.

LETTA la relazione del Direttore Sanitario;

PREMESSO che la ASR Regione Abruzzo proponeva alla ASL di Pescara di aderire all’accordo di collaborazione tra la Regione Abruzzo, l’Azienda Sanitaria Regionale Abruzzo, la Think Pink Italy ETS (già Komen Italia), l’Azienda ASL di Teramo, l’Azienda ASL di Pescara, l’Azienda ASL di Avezzano Sulmona L’Aquila, l’Azienda ASL di Lanciano Vasto Chieti per la realizzazione del progetto “**CAROVANA DELLA PREVENZIONE**” , giusta versione definitiva inviata in data 17.09.2026 dalla stessa ASR;

CONSIDERATO che la Think Pink Italy ETS (già Komen Italia):

- da anni organizza un Programma Nazionale Itinerante di Promozione della Salute finalizzato alla promozione della salute, della prevenzione oncologica e della diffusione della cultura della Prevenzione;
- è un’organizzazione priva di finalità di lucro, basata sul volontariato, in prima linea nella lotta ai tumori al seno e nella promozione della salute femminile su tutto il territorio nazionale;
- manifesta la propria disponibilità a collaborare per i programmi di sensibilizzazione e comunicazione per la prevenzione dei tumori che saranno organizzati dalle singole ASL della Regione Abruzzo;
- propone un progetto che prevede il coinvolgimento istituzionale (l’Alto Patronato del Presidente della Repubblica, il Patrocinio del Ministero della Salute e dell’Istituto Superiore di Sanità), con la collaborazione di istituzioni sanitarie e organizzazioni no-profit delle diverse regioni italiane e con il supporto di partner pubblici e privati;

CONSIDERATO, ALTRESI’, che la ASL di Pescara:

- in coerenza con la propria mission istituzionale, promuove iniziative finalizzate alla tutela della salute e della prevenzione dei tumori femminili;
- intende partecipare al progetto “Carovana della Prevenzione” promosso da Think Pink Italy ETS, che prevede screening offerti dalle unità mobili che si integrano con i programmi di screening regionali (es. offrendo esami a donne fuori dalle fasce d’età standard);
- stabilisce che, in caso di esito positivo o sospetto agli esami diagnostici (mammografie ed ecografie), la paziente venga inserita in un proprio percorso di cura e approfondimento, in conformità con le modalità stabilite dal S.S.N., assicurando continuità assistenziale;

- intende definire le modalità operative con le quali garantirà il proprio supporto di personale, accanto e in raccordo con il personale della Think Pink Italy ETS;

RITENUTO che tali iniziative, realizzate in modalità integrata e in rete, favoriscono l'adesione attiva degli operatori sanitari e lo scambio di esperienze e buone pratiche professionali;

LETTO il citato accordo di collaborazione tra la Regione Abruzzo, l'Agenzia Regionale Abruzzo, la Think Pink Italy ETS (già Komen Italia) e le ASL della Regione Abruzzo e di condividerne i contenuti;

RILEVATO che l'adesione a tale progetto implica, per la Asl di Pescara, impiego di risorse legate alle prestazioni lavorative di operatori sanitari che verranno coinvolti nelle attività dell'Unità Mobile della Think Pink Italy allorquando stazionerà all'interno del territorio di competenza della Asl di Pescara, ed alcun'altra forma di esborso finanziario;

CONSIDERATO che, il citato documento, prevede, ai fini del coordinamento tra i diversi Enti coinvolti per la realizzazione delle diverse attività, le funzioni della “ Cabina di Regia” che, tra gli altri, è altresì composta da n. 4 responsabili dei Centri Gestionali Screening delle Aziende Sanitarie Locali coadiuvati dai Responsabili delle UU.OO. di Screening mammografico delle singole ASL;

RITENUTO di individuare, ai fini della partecipazione alla citata “cabina di regia” in rappresentanza della Asl di Pescara, rispettivamente la Dr.ssa Graziella Soldato, Direttore f.f. del Dipartimento di Prevenzione e la Dr.ssa Maria Carmela Minna, Responsabile UOSD Assistenza Consultoriale;

PRECISATO che, la Dr.ssa Soldato e la Dr.ssa Minna, ciascuno per quanto di propria competenza e nell'esercizio delle rispettive funzioni, dovranno assicurare, durante il periodo di permanenza dell'Unità Mobile nel territorio di competenza della Asl di Pescara, l'organizzazione e gestione degli operatori, così come dettagliato nell'accordo, stilando un documento operativo sulle modalità organizzative e sugli operatori coinvolti;

SENTITO il DPO aziendale che ha espresso parere favorevole all'accordo di collaborazione, prescrivendo la sottoscrizione, da parte della Think Pink Italy ETS, dell' ”Accordo per il trattamento di dati personali con il Responsabile del Trattamento”;

PRESO ATTO dell'attestazione dei competenti Responsabili in ordine alla regolarità amministrativo-contabile e tecnica del presente provvedimento;

ACQUISITI per quanto di competenza i pareri favorevoli espressi in merito dal Direttore Amministrativo Aziendale e dal Direttore Sanitario Aziendale;

D E L I B E R A

Per tutto quanto sopra indicato, che qui si intende integralmente richiamato

- 1) **DI PRENDERE ATTO E DI APPROVARE** l'accordo di collaborazione tra la Regione

Abruzzo, l'Agenzia Regionale Abruzzo, la Think Pink Italy ETS (già Komen Italia) e le ASL della Regione Abruzzo per lo sviluppo del progetto “ Carovana della Prevenzione”, che in questa sede si approva e che costituisce parte integrante e sostanziale del presente atto deliberativo unitamente all'accordo per il trattamento di dati personali con il Responsabile del Trattamento a firma del l.r.p.t. della Think Pink Italy ETS;

- 2) **DI AUTORIZZARE** la sottoscrizione dell'accordo di collaborazione tra la Regione Abruzzo, l'Agenzia Regionale Abruzzo, la Think Pink Italy ETS (già Komen Italia) e le ASL della Regione Abruzzo e l'accordo per il trattamento di dati personali con il Responsabile del Trattamento a firma del l.r.p.t. della Think Pink Italy ETS;
- 3) **DI PRECISARE** che la ASL di Pescara garantirà le risorse sanitarie necessarie, in conformità agli standard organizzativi indicati nel citato accordo, durante la permanenza dell'Unità Mobile nel proprio territorio di competenza;
- 4) **DI INDIVIDUARE** ai fini della partecipazione alla citata “cabina di regia” in rappresentanza della Asl di Pescara, rispettivamente la Dr.ssa Graziella Soldato, Direttore del Dipartimento di Prevenzione e la Dr.ssa Maria Carmela Minna, Responsabile UOSD Assistenza Consultoriale;
- 5) **DI STABILIRE** che la Dr.ssa Soldato e la Dr.ssa Minna, ciascuno per quanto di propria competenza e nell'esercizio delle rispettive funzioni, dovranno stilare un documento operativo sulle modalità organizzative al fine di assicurare, durante la permanenza dell'Unità Mobile nel territorio di competenza della Asl di Pescara, la partecipazione di operatori sanitari, per prestare operato a bordo della Unità Mobile;
- 6) **DI TRASMETTERE** copia del presente atto al Direttore Sanitario Aziendale, al Dipartimento di Prevenzione, alla UOSD Assistenza Consultoriale, all'Ufficio Affari Generali e Legali, all'Ufficio Privacy;
- 7) **DI DARE ATTO** il presente provvedimento deve essere pubblicato nell'albo pretorio online della ASL ai sensi della legge n. 69/2009 e del D.Lgs. 33/2013 s.m.i. e che, ai sensi della L.R. n. 10/2022, il presente provvedimento sarà soggetto a pubblicazione integrale;
- 8) **DI CONFERIRE** al presente atto la clausola di immediata esecutività.



ACCORDO DI COLLABORAZIONE

TRA

La Regione Abruzzo, Codice Fiscale 80003170661, in persona dell'Assessore della Salute Dott.ssa Nicoletta Veri, domiciliata per la carica presso la sede in Via Leonardo da Vinci, 6, 67100 L'Aquila (AQ) – (di seguito denominato Assessorato)

E

L'Agenzia Sanitaria Regionale Abruzzo, Codice Fiscale 01780030688, in persona del Direttore dell'Agenzia Sanitaria Regionale Dott. Maurizio Brucchi, con sede in Via Attilio Monti, 9 in Pescara (di seguito denominata ASR Abruzzo),

E

La Think Pink Italy ETS (già Komen Italia), Codice Fiscale 06073831007, con sede in Roma, con sede legale in Largo Agostino Gemelli 8, 00168 Roma (RM) e sede operativa in Circ.ne Clodia 78/A, 00195 Roma (RM), in persona del legale rappresentante Prof.ssa Alba Di Leone (di seguito denominato "Think Pink Italy ETS")

E

AZIENDA ASL DI TERAMO con sede legale in Teramo, CF 00115590671 in persona del legale rappresentante Dott. Di Giosia Maurizio.

E

AZIENDA ASL DI PESCARA con sede legale in Pescara, CF 01397530682 in persona del legale rappresentante Dott. Vero Michitelli.

E

AZIENDA ASL DI AVEZZANO SULMONA L'AQUILA con sede legale in L'Aquila, CF 01792410662 in persona del legale rappresentante Dott. Paolo Costanzi.

E

AZIENDA ASL DI LANCIANO VASTO CHIETI con sede legale in Chieti, CF 02307130696 in persona del legale rappresentante Dott. Mauro Palmieri.

PREMESSO CHE

- L'Assessorato, con le competenze attribuite all'Agenzia Sanitaria Regionale (di seguito ASR Abruzzo) svolge attività in materia di politiche per la salute, la pianificazione e programmazione strategica sanitaria per la Regione Abruzzo,
- In particolare, l'ASR è la "tecnostruttura" del sistema sanitario regionale che concorre, a livello centrale, alla definizione delle politiche per la salute e alla pianificazione e programmazione strategica sanitaria e, a livello periferico, contribuisce al perseguimento degli obiettivi strategici regionali garantendo il supporto tecnico-metodologico e formativo alle Aziende Sanitarie Locali e alle altre componenti "sistema salute" (Istituzioni, Enti pubblici e privati, espressioni organizzate della comunità);
- L'Agenzia Sanitaria Regionale Abruzzo concorre al perseguimento degli obiettivi di politica sanitaria regionale assicurando supporto tecnico-scientifico alla Regione Abruzzo per l'osservazione epidemiologica e il monitoraggio dei "livelli essenziali di assistenza", il supporto tecnico alla Direzione "Sanità" per la programmazione sanitaria e controllo direzionale, la ricerca e sviluppo di metodologie e strumenti per il governo clinico, per il miglioramento continuo della qualità e per lo sviluppo dell'integrazione socio-sanitaria;
- L'Agenzia Sanitaria Regionale Abruzzo svolge le attività d'intesa con il Dipartimento per la Salute della Regione Abruzzo e in sinergia con le Aziende Sanitarie Locali della Regione;
- La Think Pink Italy ETS è un'organizzazione priva di finalità lucrative, basata sul volontariato, in prima linea nella lotta ai tumori del seno e nella promozione della salute femminile su tutto il territorio nazionale;
- L'organizzazione opera in maniera specifica con prestazioni non occasionali perseguendo esclusivamente finalità di solidarietà sociale;
- L'organizzazione svolge regolarmente da più di vent'anni – in base al proprio Statuto – attività di sensibilizzazione dell'opinione pubblica sulla salute del seno anche attraverso l'attuazione di programmi di prevenzione secondaria, di diagnosi e di trattamento dei tumori alla mammella;

CONSIDERATO

che la suddetta organizzazione ha avviato, a partire dal 2017, un progetto dal titolo “CAROVANA DELLA PREVENZIONE” con l'obiettivo di ampliare le attività di promozione della prevenzione offerte su tutto il territorio nazionale, estendendo alle aree meno servite o disagiate l'offerta di aderire alle attività di prevenzione secondaria dei tumori femminili.

- che il progetto è svolto sotto il più alto coinvolgimento istituzionale (l'Alto Patronato del Presidente della Repubblica, il Patrocinio del Ministero della Salute e dell'Istituto Superiore di Sanità), con la collaborazione di istituzioni sanitarie e organizzazioni no-profit delle diverse regioni italiane e con il supporto di partner pubblici e privati;
- che il progetto ha già raggiunto 17 Regioni italiane con l'organizzazione di oltre 2.500 “Giornate di Promozione della Salute Femminile”;
- che in data 10 settembre 2021 è stato sottoscritto un accordo di collaborazione biennale tra le parti, attraverso il quale la Think Pink Italy ETS (già Komen Italia) ha messo a disposizione, con costi a proprio carico, una Unità mobile per la realizzazione su tutto il

territorio della Regione Abruzzo di “Giornate di Promozione della Prevenzione e della Salute Femminile”, con l’obiettivo prioritario di coinvolgere fasce di popolazione in condizioni di disagio sociale od economico o residenti in aree territorialmente disagiate;

Preso atto

delle comuni finalità e riscontrando l’interesse delle parti di rinnovare la virtuosa collaborazione per incidere positivamente sulla salute delle donne residenti nella Regione Abruzzo.

Tutto ciò premesso, si conviene e si stipula quanto segue

Art. 1 (Oggetto)

a) Le parti riconoscono l’interesse a una reciproca collaborazione volta allo sviluppo del progetto “Carovana della Prevenzione”, attraverso la realizzazione su tutto il territorio della Regione Abruzzo di “Giornate di Promozione della Prevenzione e della Salute Femminile” con l’obiettivo prioritario di coinvolgere fasce di popolazione in condizioni di disagio sociale od economico o residenti in aree territorialmente disagiate.

Le attività di prevenzione oncologica potranno anche essere orientate alla popolazione appartenente alla fascia di età target prevista dai programmi di screening oncologico organizzato del SSN, in coerenza con il vigente Piano Regionale della Prevenzione e su indicazione e stretta collaborazione operativa con i Centri Gestionali Screening e le UU.OO. di Screening Mammografico delle ASL. In questo caso le attività potranno essere condotte con l’intervento attivo del personale già impegnato nei programmi di screening delle singole ASL.

b) la popolazione attualmente non compresa nella fascia d’età dello screening (<50 e >69 anni) potrà effettuare gli esami diagnostici di I livello a cura di Think Pink Italy ETS, con modalità organizzative e gestionali dalla stessa definite: per evitare che intervengano elementi confondenti e sovrapposizioni organizzative, tale attività sarà realizzata in momenti diversi da quelli destinati ad utenti in fascia di età di screening. La Think Pink Italy ETS provvederà all’organizzazione ed alla gestione di tali attività con risorse umane e strumentali appositamente identificate.

c) In ciascuna tappa del progetto potranno essere organizzati anche eventi educativi e laboratori teorico-pratici di promozione dell’attività fisica, del benessere e della corretta alimentazione e momenti educativi sull’importanza della prevenzione e dell’attenzione alla propria salute.

d) Think Pink Italy ETS manifesta la propria disponibilità a collaborare per i programmi di sensibilizzazione e comunicazione per la prevenzione dei tumori che saranno organizzati dalle singole Aziende Sanitarie Provinciali.

Art. 2 (Durata)

La presente collaborazione avrà la durata di ventiquattro mesi, a decorrere dalla data di pubblicazione della Delibera di approvazione del presente dell’Accordo e potrà essere rinnovata, previo accordo congiunto tra le parti.

Art.3 (Compiti)

Ciascuna Parte si impegna in esecuzione del presente Accordo a svolgere le attività di propria competenza con la massima cura e diligenza, nonché a tenere informata l'altra parte sulle attività effettuate.

In particolare:

a. L'Assessorato attraverso l'ASR si impegna a:

- agevolare le iniziative virtuose di prevenzione previste nel presente Accordo, garantendo che esse vengano realizzate in pieno coordinamento con le singole Aziende Sanitarie Locali;
- confermare le funzioni della "Cabina di Regia" costituita da:

n. 1 rappresentante dell'ASR individuato in: Direttore dell'ASR Abruzzo, Dott. Maurizio Brucchi

n. 3 rappresentanti della Think Pink Italy ETS individuati in:

- Prof.ssa Alba Di Leone, Presidente Komen Italia
- Isabella Marianacci, Presidente Comitato Regionale Abruzzo
- Giustiniana Vecchiotti, Head Programmi Istituzionali e Mission

n. 4 responsabili dei Centri Gestionali Screening delle Aziende Sanitarie Locali coadiuvati dai Responsabili delle UU.OO. di Screening mammografico delle singole ASL

La Cabina di Regia avrà il compito di assicurare al meglio lo svolgimento del progetto, provvedendo a pianificare le attività previste dall'Accordo secondo i tempi e il fabbisogno territoriale espresso da ogni singola Azienda Sanitaria Locale.

- assicurare che ogni ASL, durante la permanenza dell'Unità Mobile nel proprio territorio di competenza favorisca la partecipazione di propri operatori sanitari, per prestare il proprio operato a bordo della Unità Mobile, assumendo altresì tutti gli oneri legali, assicurativi e amministrativi necessari per la partecipazione del proprio personale medico, tecnico e infermieristico coinvolto. Anche a tal fine, le singole ASL potranno definire un documento operativo sulle modalità organizzative e sugli operatori coinvolti;

b. la Think Pink Italy ETS si impegna a:

- mettere a disposizione, con costi a proprio carico, n.1 (una) Unità Mobile FIAT Ducato dotata di mammografo digitale conforme alle specifiche di screening, comprensiva dell'ingaggio degli autisti necessari, che provvederanno a condurre e posizionare il mezzo nelle aree di volta in volta individuate e a riportarlo nelle aree di parcheggio/custodia preventivamente individuate da Think Pink Italy ETS;
- mettere a disposizione gli strumenti tecnologici di ultima generazione (mammografo digitale, ecografo portatile, workstation di refertazione e strumenti di teleradiologia), valutati idonei e conformi in base alla normativa vigente;
- fornire copia delle certificazioni di idoneità e conformità, in base alla normativa vigente, degli impianti radiologici, sentito lo Specialista in Fisica Medica dell'ambulatorio;

- fornire tutte le documentazioni tecniche e radioprotezionistiche all'Esperto di Radioprotezione dell'ambulatorio, al fine di emettere il proprio benestare all'utilizzo dell'impianto, a protezione dei lavoratori e della popolazione;
- sostenere i costi relativi all'ingaggio degli autisti necessari per gli spostamenti delle Unità Mobili;
- prevedere l'ottimale trasferimento e archiviazione delle immagini prodotte in screening e l'integrazione con i sistemi RIS-PACS aziendali;
- assicurare la presenza di un punto rete, per consentire i necessari collegamenti con le piattaforme gestionali screening delle singole ASL;
- provvedere all'interfaccia operativa con gli Enti, le Istituzioni e le Associazioni territoriali coinvolte per le autorizzazioni necessarie alla realizzazione di ogni tappa.
Tale azione sarà svolta in sinergia con l'ASR Abruzzo e con le ASL al fine di definire un calendario per lo svolgimento delle giornate di attività;
- supportare con i propri volontari il personale in servizio delle singole ASL e le attività organizzative e realizzative di ogni Giornata.

c. Entrambe le Parti si impegnano a collaborare insieme nella ideazione e realizzazione di:

- seminari educativi su tematiche di sana alimentazione, sport e attività fisica, da svolgere – con il coordinamento delle singole Aziende Sanitarie Locali che partecipano al progetto – durante le Giornate di prevenzione previste dal presente accordo;
- progetti di ricerca epidemiologica.

Art.4

(Comunicazione)

Le Parti si impegnano congiuntamente a:

- dare visibilità al progetto e alla partnership su tutti i canali di comunicazione a propria disposizione;
- dare visibilità agli eventi e alle iniziative su tutti i canali di comunicazione a propria disposizione (Sito web, Social network, ufficio stampa, etc.);

Art.5

(Pubblicazioni)

La pubblicazione di dati e materiali elaborati durante lo svolgimento del progetto dovrà ottenere il consenso concordato tra le Parti

Art.6

(Privacy)

Le Parti acconsentono, nel rispetto del decreto legislativo 30 giugno 2003, n.196 (e successive modifiche e integrazioni) che:

- i dati personali e sulla salute relativi alle attività di screening di cui all'art.1 punto a) siano trattati nelle modalità previste dalla normativa vigente e archiviati presso le singole ASL Abruzzesi, per come già avviene nell'ambito delle attività ordinarie. Le immagini diagnostiche relative agli accertamenti medici realizzate nell'ambito di tale attività ed i

relativi referti verranno trasferite negli archivi dell'azienda sanitaria territoriale e custoditi nei termini e nelle condizioni di legge vigenti. Le Aziende Sanitarie Locali provvederanno a nominare l'Associazione Think Pink Italy ETS quale Responsabile del trattamento limitatamente alle attività di competenza.

- i dati personali e sulla salute relativi alle attività di cui all'art.1 punto b) siano trattati, gestiti e archiviati secondo le modalità previste dalla normativa vigente a cura della Think Pink Italy ETS. In tale fattispecie le immagini diagnostiche relative agli accertamenti medici realizzate ed i relativi referti verranno archiviati e custoditi a cura della Think Pink Italy ETS nei termini e nelle condizioni delle leggi vigenti.

Art.7 (Modifiche)

Ogni modifica del presente Accordo dovrà rivestire, a pena di nullità, la forma scritta ed essere sottoscritta dalle Parti.

Art.8 (Registrazione)

La registrazione del presente accordo verrà effettuata dalla parte che ne abbia interesse solo in caso d'uso, ai sensi della vigente normativa. Le spese, compreso il bollo, sono a carico della parte medesima.

Letto, approvato e sottoscritto

L'Aquila, lì

Direttore ASR Abruzzo
Agenzia Sanitaria Regionale Abruzzo
Dott. Maurizio Brucchi _____

Presidente della Think Pink Italy ETS (già Komen Italia)
Prof.ssa Alba Leone _____

Il Direttore Generale ASL di Teramo
Dott. Maurizio Di Giosia _____

Il Direttore Generale ASL di Pescara
Dott. Vero Michitelli _____

Il Direttore Generale ASL di Avezzano Sulmona L'aquila
Dott. Paolo Costanzi _____

Il Direttore Generale ASL di Lanciano Vasto Chieti
Dott. Mauro Palmieri _____

Assessore alla Sanità della Regione Abruzzo

Dott.ssa Nicoletta Veri _____

 asl pescara www.asl.pe.it	Regione Abruzzo – ASL 03 Pescara	Accordo per il trattamento ex art. 28 GDPR
	ACCORDO PER IL TRATTAMENTO DEI DATI Art. 28 Regolamento UE 2016/679	PRY-RT-001 Rev. 4 Del 12/08/2026

Sede Legale:
Via Renato Paolini, 45
65124 Pescara
P. IVA 01397530982

Accordo per il trattamento di dati personali con il Responsabile del Trattamento

Prot. n. _____

Pescara, lì _____

Spett.le	Think Pink Italy ETS (già Komen Italia)
Via	Largo Agostino Gemelli 8
Località	Roma
P.IVA	06073831007
p.c.	_____

Oggetto: Accordo per il trattamento dei dati personali con il Responsabile del trattamento ai sensi dell'Art. 28 del Regolamento UE Generale sulla Protezione dei Dati n. 2016/679 (GDPR – General Data Protection Regulation) e della vigente normativa di settore.

Il sottoscritto Dr. Vero Michitelli, in qualità di Legale Rappresentante della ASL di Pescara – Titolare del trattamento dei dati personali - considerato che:

- La ASL di Pescara – in qualità di TITOLARE del Trattamento di Dati Personali – è tenuta a tutti gli adempimenti di legge;
- La designazione a Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento Generale sulla Protezione dei Dati n. 2016/679 (di seguito GDPR – General Data Protection Regulation – o Regolamento) viene intesa essere rivolta a soggetti esterni alla struttura del Titolare;

Il presente accordo, ai sensi dell'art. 28 del Regolamento (UE) 2016/679, integra e specifica gli obblighi derivanti dalla Delibera e dai relativi documenti contrattuali tra la ASL di Pescara (di seguito "ASL PE" o "Titolare") e l'impresa (di seguito "Fornitore" o "Responsabile"), con particolare riferimento alla protezione dei dati personali.

Il presente Accordo sulla protezione dei dati (di seguito anche "ATD") si applica alle attività nelle quali il Responsabile tratta dati personali per conto del Titolare, comprese quelle svolte da persone autorizzate e, ove autorizzati ai sensi dell'art. 11, da sub-responsabili. Restano ferme le disposizioni del Regolamento (UE) 2016/679, del d.lgs. 196/2003, come modificato dal d.lgs. 101/2018, e della normativa di settore applicabile.

Il Responsabile e la ASL di Pescara sono di seguito congiuntamente le “**Parti**” e singolarmente la “**Parte**”. Ogni riferimento al “**Titolare**” indica esclusivamente la ASL di Pescara.

Le comunicazioni al Titolare sono trasmesse alla PEC protocollo.aslpe@pec.it, all’attenzione del Direttore generale, e per conoscenza all’Ufficio Privacy e Sicurezza delle Informazioni, fatti salvi i canali di emergenza previsti dall’art. 8.

Articolo 1 – Oggetto, natura, finalità e durata del trattamento

- 1) Il presente ATD si applica esclusivamente alle attività nelle quali il Fornitore tratta dati personali per conto della ASL di Pescara. La qualificazione delle Parti dipende dalle attività effettivamente svolte: il presente modello non si applica automaticamente quando il Fornitore non tratta dati personali o agisce, per una specifica attività, quale titolare autonomo.
- 2) Natura, oggetto, finalità, durata, categorie di dati personali, categorie di Interessati e operazioni autorizzate sono definiti nei documenti contrattuali e nell’art. 15. Gli artt. 15 e, ove applicabili, 17, 18 e 19 devono essere completati, verificati e approvati prima della sottoscrizione e, in ogni caso, prima dell’accesso ai dati o dell’avvio del servizio.
- 3) Il Titolare determina finalità e mezzi essenziali del trattamento e ne individua i presupposti di liceità; il Responsabile adempie agli obblighi propri del ruolo e tratta i dati esclusivamente secondo istruzioni documentate. La ripartizione dei compiti non limita gli obblighi di assistenza, cooperazione e responsabilità previsti dalla legge e dal presente ATD.
- 4) Il Responsabile è tenuto al rispetto delle istruzioni impartite dal Titolare in materia di protezione dei dati personali.
- 5) La durata del trattamento da parte del Responsabile corrisponde alla durata del rapporto contrattuale e agli eventuali periodi di uscita, restituzione, cancellazione o conservazione legale specificamente indicati negli artt. 7 e 15.
- 6) Nell’Ambito di Trattamento definito, il Titolare chiede al Responsabile di trattare i dati nel rispetto dei seguenti principi:
 - a) trattati in modo lecito, corretto e trasparente nei confronti dell’interessato («liceità, correttezza e trasparenza»);
 - b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
 - c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
 - d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
 - e) conservati in una forma che consenta l’identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»);
 - f) trattati in maniera da garantire un’adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Articolo 2 – Tipologie di dati personali e categorie di interessati

- 1) Le categorie di persone interessate dal trattamento da parte del Responsabile sono indicate nell’art. 15 e sono di seguito definite “**Interessati**”.
- 2) Le categorie di dati personali trattati sono indicate nell’art. 15.

Articolo 3 – Istruzioni

- 1) Il Responsabile tratta i dati personali soltanto sulla base delle istruzioni documentate del Titolare, comprese quelle risultanti dal presente ATD, dalla Delibera, dal contratto e dall’art. 15. È vietato utilizzare

i dati per finalità proprie, analisi commerciali, addestramento di sistemi di intelligenza artificiale, miglioramento di prodotti o telemetria contenente dati personali, salvo preventiva istruzione documentata e verifica della corretta qualificazione dei ruoli e della liceità. Il Responsabile informa immediatamente il Titolare qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni applicabili in materia di protezione dei dati.

- 2) Le istruzioni aggiuntive o modificate sono trasmesse per iscritto, anche tramite PEC o altro canale concordato che ne assicuri tracciabilità e integrità. Sono efficaci dal ricevimento; le Parti documentano un termine tecnico proporzionato per l'attuazione, fermo l'adempimento immediato delle istruzioni urgenti necessarie a interrompere o contenere un rischio o una violazione.
- 3) Si intendono istruzioni in forma scritta documenti quali (a titolo esemplificativo e non esaustivo): Procedure, Circolari, Comunicazioni, Regolamenti, Disciplinari, Materiale didattico per la formazione, ecc...
- 4) È fatto obbligo al Responsabile di:
 - a) Impegnarsi alla riservatezza secondo quanto previsto dall'art. 4 del presente ATD;
 - b) adottare le misure di sicurezza richieste ai sensi dell'Art. 32 del GDPR, come previsto dall'art. 5 del presente ATD;
 - c) fornire assistenza al Titolare del Trattamento secondo quanto previsto dall'art. 6 del presente ATD;
 - d) rispettare gli obblighi di conservazione, riconsegna e cancellazione dei dati secondo quanto previsto dall'Art. 7 del presente ATD;
 - e) impegnarsi a supportare il Titolare nella segnalazione e gestione di eventuali Violazioni di Dati Personali secondo quanto previsto dall'art.8 del presente ATD;
 - f) impegnarsi a supportare il Titolare nell'esecuzione della Valutazione di Impatto secondo quanto previsto dall'art.9 del presente ATD;
 - g) nominare i Soggetti Autorizzati al Trattamento dei dati (ex Incaricati al Trattamento dei Dati) ai sensi dell'art. 28, par. 3, lett. b) del Reg. UE 2016/679 e dell'art. 2-quaterdecies del Codice, conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione come previsto dall'art. 10 del presente ATD;
 - h) ove necessario designare i sub-Responsabili del Trattamento dei dati ai sensi dell'art. 28 del Reg. UE 2016/679, conferendo loro apposite istruzioni sulle norme e le procedure da osservare, secondo quanto previsto dall'art. 11 del presente ATD;
 - i) ove applicabile assolvere agli adempimenti per gli Amministratori di Sistema secondo quanto previsto dall'art. 12 del presente ATD;
 - j) coadiuvare il Titolare nei rapporti con le autorità come previsto dall'Art. 13 del presente ATD;
 - k) rispettare gli ulteriori obblighi e responsabilità di cui all'art. 14 e le disposizioni finali di cui all'art. 20;
 - l) redigere e aggiornare l'elenco interno delle persone autorizzate e l'elenco dei sub-responsabili di cui all'art. 17; rendere disponibili al Titolare, su richiesta, l'elenco o evidenze equivalenti, comunicando dati nominativi soltanto quando necessari e proporzionati, fermo quanto previsto per gli Amministratori di sistema;
 - m) controllare le operazioni di trattamento svolte dai soggetti autorizzati al trattamento ed eventualmente dai sub-Responsabili e la conformità nell'ambito di trattamento consentito;
 - n) comunicare immediatamente al Titolare, salvo un divieto legale di informazione, ogni richiesta, ordine o attività di controllo dell'autorità di controllo o dell'autorità giudiziaria relativa ai dati trattati per conto della ASL, e cooperare preservando la riservatezza e le evidenze pertinenti. Le comunicazioni di violazioni e incidenti restano disciplinate separatamente dall'art. 8;
 - o) organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali oggetto del presente ATD affinché esse vengano effettuate nel rispetto delle disposizioni normative in materia di protezione di dati personali e predisporre tutti i documenti richiesti dai relativi adempimenti;
 - p) rispettare tutto quanto ulteriormente disciplinato dal presente ATD.

Articolo 4 – Riservatezza

- 1) Il Responsabile si impegna a mantenere la riservatezza dei dati a cui ha accesso ed è soggetto a tale obbligo;
- 2) Il Responsabile garantisce che le persone da esso autorizzate siano vincolate alla riservatezza o soggette a un adeguato obbligo legale di riservatezza. I sub-responsabili sono distintamente vincolati mediante l'atto scritto previsto dall'art. 11.

Articolo 5 – Sicurezza del trattamento

- 1) Il Responsabile si impegna ad adottare tutte le misure richieste dall'art. 32 del GDPR e le procedure tecniche e organizzative in materia stabilite dal Titolare all'interno del presente accordo.
- 2) In particolare - in considerazione dello stato dell'arte, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, il Responsabile si impegna a mettere in atto le misure tecniche e organizzative indicate dal Titolare e indicate nell'art.19 del presente ATD.
- 3) Le misure essenziali e applicabili dell'art. 19 devono essere operative e comprovate prima di qualsiasi accesso ai dati o avvio del servizio. Eventuali scostamenti residui non critici sono ammessi soltanto previa valutazione del rischio, accettazione scritta del Titolare e piano con responsabilità, misure compensative e scadenze, sentiti il DPO e le funzioni di sicurezza competenti. Nessun piano successivo alla sottoscrizione sana l'assenza di una garanzia richiesta per l'avvio.
- 4) L'art. 19, ai sensi dell'art. 28, par. 3, lett. h), costituisce riferimento per le verifiche, le ispezioni e gli audit eseguiti dal Titolare o da un soggetto da questi incaricato.
- 5) Qualora il Responsabile intendesse apportare modifiche alle misure tecniche e organizzative previste nell'art.19 del presente ATD, in considerazione del progresso e sviluppo tecnologico, tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto dalle misure di cui all'art.19 del presente accordo.

Articolo 6 – Assistenza

- 1) Tenendo conto della natura del trattamento e mediante misure tecniche e organizzative adeguate, il Responsabile assiste il Titolare, per quanto possibile, nel dare seguito alle richieste di esercizio dei diritti degli Interessati di cui agli artt. 15-22 GDPR.
- 2) Il Responsabile dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Interessato eserciti nei suoi confronti o di uno dei sub-responsabili (ved. Art. 11 del presente ATD) uno dei diritti di cui agli artt. da 15 a 22 del GDPR.
- 3) Tenendo conto della natura del trattamento e delle informazioni di volta in volta messe a disposizione, il Responsabile si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 del GDPR.

Articolo 7 – Conservazione, Riconsegna e Cancellazione

- 1) Alla cessazione dei servizi, su scelta documentata del Titolare, il Responsabile restituisce i dati personali e cancella le copie residue oppure cancella tutti i dati, entro il termine massimo di 30 giorni per le copie attive, salvo un diverso termine indicato nell'art. 15 o un obbligo di legge debitamente identificato.
- 2) Il Responsabile attesta per iscritto l'avvenuta restituzione e/o cancellazione e impone il medesimo obbligo ai sub-responsabili. Backup, cache, log e supporti non immediatamente sovrascrivibili sono isolati dall'uso ordinario, protetti e cancellati secondo il ciclo documentato nell'art. 15. Se una norma impone la conservazione, il Responsabile ne comunica fonte, categorie di dati, durata e decorrenza, limita il trattamento alla sola conservazione e mantiene le misure di sicurezza.
- 3) In mancanza di diverse istruzioni successive, il Titolare chiede sin d'ora al Responsabile (e questi agli eventuali sub-responsabili) di procedere con la cancellazione di tutte le copie di dati personali in proprio possesso a seguito della cessazione, da parte del Responsabile o del sub-responsabile, dei servizi in

relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Responsabile (o il sub-responsabile) alla conservazione dei dati personali trattati.

Articolo 8 – Violazioni di Dati Personali (cd. “Data Breach”)

- 1) Il Responsabile informa il Titolare senza ingiustificato ritardo e comunque entro 24 ore da quando viene a conoscenza di una violazione dei dati personali, ai sensi degli artt. 28, par. 3, lett. f), e 33, par. 2, GDPR, senza attendere una propria valutazione conclusiva del rischio. La prima comunicazione indica almeno natura e momento dell'evento, sistemi e trattamenti coinvolti, categorie e stima di dati e Interessati, conseguenze probabili, misure adottate o proposte, referenti ed elementi ancora da accertare; seguono aggiornamenti progressivi e una relazione conclusiva. Il Responsabile preserva le evidenze e collabora alla registrazione, notifica e comunicazione dell'evento.
- 2) Il Responsabile si impegna inoltre, ai sensi dell'art. 28, par. 3, lett. f), tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.
- 3) La comunicazione è inviata alla PEC protocollo.aslpe@pec.it e, per conoscenza, al DPO (dpo@asl.pe.it), all'Ufficio Privacy e Sicurezza delle Informazioni e ai contatti di emergenza indicati nell'art. 16. Gli incidenti informatici potenzialmente rilevanti per gli obblighi della ASL ai sensi della legge n. 90/2024 o del d.lgs. 138/2024 sono segnalati separatamente, immediatamente, quale SLA contrattuale di cooperazione da validare con la funzione di sicurezza.

Articolo 9 – Valutazione D’impatto (CD. “DATA PROTECTION IMPACT ASSESSMENT”)

- 1) Il Responsabile, ai sensi dell'art. 28, par. 3, lett. f), s'impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a propria disposizione, a fornire al Titolare ogni elemento utile all'effettuazione della valutazione di impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment), qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante ai sensi dell'art. 36 del Regolamento stesso.

Articolo 10 – Soggetti Autorizzati al Trattamento

- 1) Il Responsabile garantisce che l'accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto e formalmente autorizzati (ex art. 2-*quaterdecies* del Codice), il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi previsti dal Contratto allegato alla Delibera.
- 2) Il Responsabile si impegna a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali del Titolare, le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro.

Articolo 11 – Sub-responsabili del Trattamento

- 1) Per l'esecuzione di specifiche attività per conto della ASL nell'ambito del Contratto, il Responsabile potrà avvalersi di sub-responsabili del trattamento (ciascuno un "Sub-responsabile del Trattamento") ai sensi del GDPR (art. 28, parr. 2 e 4). I Sub-responsabili del Trattamento sono autorizzati a trattare dati personali degli Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti al Responsabile ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Responsabile ricorrerà a Sub-responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, ad obblighi analoghi in materia di protezione dei dati e comunque non meno tutelanti per gli Interessati di quelli previsti nel presente ATD tra il Titolare del trattamento e il Responsabile, prevedendo in particolare garanzie sufficienti per mettere

in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento. Qualora il Sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile.

- 2) Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzo PEC indicato nelle premesse e nell'art. 8 del presente ATD), laddove intenda designare o sostituire un Sub-responsabile del Trattamento. La comunicazione al Titolare dovrà contenere l'elencazione dettagliata delle attività, previste dal Contratto, affidate al sub-Responsabile e dovrà essere effettuata 15 giorni prima dell'operazione di designazione o sostituzione; tale operazione si intenderà accettata laddove il Titolare non sollevi obiezioni per iscritto entro 15 giorni dalla ricezione della comunicazione da parte del Responsabile.
- 3) Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzo PEC indicato nelle premesse e nell'art. 8 del presente ATD), laddove intenda cessare il rapporto esistente con un sub-Responsabile del Trattamento senza procedere ad una sua sostituzione. Questa operazione prevede che le attività affidate al sub-Responsabile vengano riprese in carico da parte del Responsabile o riassegnate ad uno degli altri sub-Responsabili già designati. La comunicazione della cessazione al Titolare, comprensiva del dettaglio delle attività e della relativa riassegnazione, dovrà essere effettuata 15 giorni prima dell'operazione di cessazione.
- 4) Qualora il Titolare sollevi obiezioni su uno o più Sub-responsabili del Trattamento, darà indicazioni al Responsabile sulle relative motivazioni. In tal caso, quest'ultimo potrà:
 1. proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale il Titolare abbia sollevato obiezioni; o
 2. adottare misure tese a superare le obiezioni del Titolare (qualora le obiezioni fossero superabili).
- 5) L'elenco completo e aggiornato dei sub-responsabili è riportato nell'art. 17 e deve essere comunicato e approvato prima della sottoscrizione e prima dell'avvio del relativo trattamento. In assenza di sub-responsabili deve essere selezionata l'apposita dichiarazione. L'elenco è mantenuto aggiornato per l'intera durata del rapporto e comunicato alla PEC protocollo.aslpe@pec.it e all'Ufficio Privacy e Sicurezza delle Informazioni.
- 6) Il Fornitore è responsabile nei confronti del Titolare per l'adempimento del Sub-responsabile del Trattamento ai propri obblighi previsti dalla normativa vigente in materia di Protezione dei Dati Personali e dal presente ATD.
- 7) Qualunque trattamento o accesso da un Paese esterno allo Spazio economico europeo, anche da remoto o tramite un sub-responsabile, richiede preventiva informazione e autorizzazione del Titolare e l'indicazione nell'art. 17 dei Paesi, delle attività, dello strumento del capo V GDPR, della valutazione sul trasferimento e delle misure supplementari. Il trasferimento non può iniziare prima della verifica documentata della conformità agli artt. 44 e seguenti GDPR.

Articolo 12 – Amministratori di Sistema

- 1) Ove applicabile in relazione ai prodotti e servizi forniti, il Responsabile si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità.
- 2) In riferimento ai sistemi informatici (interni o esterni alle strutture dell'Azienda Sanitaria) di trattamento dei dati del Titolare, per i quali il Responsabile (o un suo Sub-responsabile) nomina uno o più Amministratori di Sistema (di seguito anche "AdS"), il Responsabile si impegna a:
 1. designare quali Amministratori di Sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;

2. effettuare un'elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;
3. predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali Amministratori di Sistema e le funzioni ad essi attribuite;
4. comunicare periodicamente (almeno una volta l'anno, entro il 31/12) al Titolare l'elenco aggiornato degli Amministratori di Sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.) ed i dati di contatto per l'attivazione di eventuali procedure di emergenza;
5. comunicare tempestivamente, entro 3 giorni dall'ingresso, sostituzione o cessazione degli AdS, le variazioni dell'elenco, specificando l'ambito di responsabilità, gli identificativi degli account attivati o dismessi e i contatti di emergenza dei nuovi AdS. Non devono essere mai comunicati password, token, chiavi o altri segreti di autenticazione;
6. verificare annualmente l'operato degli Amministratori di Sistema, informando il Titolare circa le risultanze di tale verifica;
7. registrare gli accessi logici degli Amministratori di sistema con caratteristiche di completezza, inalterabilità e verificabilità e conservarli per un periodo non inferiore a sei mesi, rendendoli disponibili al Titolare. I diversi log applicativi, di sicurezza e di audit seguono le finalità e i tempi documentati nell'art. 15;
8. garantire una rigida separazione dei compiti tra chi autorizza e/o assegna i privilegi di accesso (credenziali di Amministratore) e chi effettua le attività tecnico-sistemistiche sui medesimi sistemi.

Articolo 13 – Rapporti con le Autorità

- 1) Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali di propria competenza.

Articolo 14 – Ulteriori Obblighi e Responsabilità

- 1) Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente atto di designazione e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente ATD.
- 2) Il Titolare verifica le dichiarazioni rese dal Responsabile per l'intera vigenza contrattuale e, quando opportuno, prima dell'avvio del servizio. L'inosservanza delle prescrizioni può comportare sospensione degli accessi, misure correttive e, nei casi previsti dal contratto o dalla legge, risoluzione e ulteriori conseguenze.
- 3) Il Titolare comunica oggetto, tempistica e durata dell'audit con un preavviso ragionevole, salvo verifiche urgenti, incidenti, richieste dell'autorità o rischio concreto, per i quali il preavviso può essere ridotto o omissso nel rispetto di proporzionalità e riservatezza.
- 4) Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.
- 5) Il Responsabile si impegna altresì a:
 1. effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e relativi adempimenti eseguiti) ed alle conseguenti risultanze;
 2. collaborare, se richiesto dal Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;
 3. realizzare quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati con il presente atto di designazione;
 4. informare prontamente il Titolare di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia o ritenga a suo parere che il

trattamento dei Dati Personali violi la normativa vigente o presenti, comunque, rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato.

- 6) Resta inteso che, qualora il Responsabile o un sub-responsabile determini finalità e mezzi del trattamento in violazione del presente ATD e delle istruzioni lecite, esso è considerato titolare per quel trattamento ai sensi dell'art. 28, par. 10, GDPR, con i conseguenti obblighi e responsabilità.

Articolo 15 – Descrizione dettagliata dell'attività

Il Titolare e l'unità organizzativa richiedente descrivono e disciplinano nell'art. 15 il trattamento affidato, verificando la coerenza con contratto, flussi reali, Registro del Titolare, informativa e, ove necessaria, DPIA. Le procedure interne richiamate devono essere verificate nella versione vigente al momento dell'uso. Riferimento normativo ufficiale: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/?locale=it>. L'art. 15 e le sezioni applicabili degli artt. 17-19 sono condizioni essenziali e devono essere compilati prima della firma. I documenti di riferimento sono la Procedura per la Gestione di Accordi, Nomine e Designazioni rev. 1.1 - marzo 2019 (Del. 427 del 4/4/2019), Procedura per la gestione della conformità in materia di protezione dei dati personali nelle procedure di acquisizione di lavori, servizi e forniture rev. 1.0 - marzo 2020 (Circolare 1/2020), disponibili su asl.pe.it/datipersonali.

Cod.	Voce	Descrizione
1	AMBITO DI TRATTAMENTO	
1.1	Descrivere l'attività e il ciclo di vita completo del trattamento Art. 28, par. 3, GDPR	Progetto "La Carovana della Prevenzione" un tour itinerante che porta la prevenzione oncologica direttamente nelle comunità locali. In ogni tappa vengono organizzate Giornate di Prevenzione gratuite aperte alla popolazione femminile, che prevedono l'utilizzo di un'unità mobile attrezzata dotata di mammografo digitale per l'erogazione gratuita di prestazioni cliniche e diagnostiche nell'ambito della prevenzione oncologica femminile, in sinergia con il personale e le strutture dell'Azienda Sanitaria. Think Pink Italy ETS non raccoglie direttamente le prenotazioni degli utenti. La Asl di Pescara trasmette alla Think Pink Italy ETS l'agenda delle donne già prenotate nel proprio Sistema, contenente i seguenti dati personali: nome, cognome, data di nascita, codice fiscale, numero di telefono ed eventuale e-mail. Tali dati vengono utilizzati per le seguenti finalità operative strettamente connesse allo svolgimento degli eventi: - Invio di reminder per promuovere e confermare la partecipazione alla Giornata di Prevenzione. - Gestione delle comunicazioni relative a cambi di appuntamento e annullamenti. - Raccolta in forma cartacea in loco delle schede anagrafiche delle utenti partecipanti, i volontari di Think Pink Italy ETS che raccolgono materialmente le schede verranno nominate soggetti autorizzati al Trattamento (SAT) dalla Asl di Pescara. Prima dell'avvio delle attività diagnostiche (immagini diagnostiche e referti) viene predisposta una connessione VPN dedicata tra l'Unità Mobile di Think Pink Italy ETS e l'archivio digitale dell'Azienda Sanitaria di Pescara. Le immagini diagnostiche acquisite tramite il mammografo a bordo dell'Unità Mobile transitano direttamente sull'archivio Informatico della Asl di Pescara. (non transitano mai negli archivi di Think Pink Italy ETS e non vengono salvate o conservate in alcun modo sui sistemi di Think Pink Italy ETS) la conservazione delle immagini diagnostiche e dei referti è gestita integralmente dalla Asl di Pescara.
1.2	Indicare tutte le operazioni autorizzate Artt. 4, par. 2, e 28, par. 3, GDPR	☒ Raccolta ☐ Registrazione ☐ Organizzazione/strutturazione ☐ Conservazione

		☒ Consultazione/uso ☐ Modifica ☐ Estrazione ☐ Comunicazione/messa a disposizione ☐ Raffronto/interconnessione ☐ Limitazione ☒ Cancellazione/distruzione esclusivamente secondo le istruzioni del Titolare ☐ Trasferimento extra SEE o accesso remoto da Paese terzo
1.3	Finalità determinate del trattamento per conto del Titolare Artt. 28, par. 3, e 30, par. 1, lett. b), GDPR	☒ Prevenzione, diagnosi, cura o riabilitazione ☐ Gestione amministrativa connessa ☐ Governo clinico, qualità o sicurezza delle cure ☐ Gestione del personale ☐ Obbligo legale (indicare la legge): _____ ☐ Ricerca (indicare protocollo e presupposti) _____ ☐ Altro: _____ Descrivere separatamente ciascuna finalità; nessuna finalità propria del Responsabile è autorizzata.
1.4	Categorie di Interessati Artt. 28, par. 3, e 30, par. 1, lett. c), GDPR	☒ a) Dipendenti/Consulenti ☐ b) Utenti/Contraenti/Abbonati/Cienti (attuali o potenziali) ☐ c) Associati, soci, aderenti, simpatizzanti, sostenitori ☐ d) Soggetti che ricoprono cariche sociali ☐ e) Beneficiari o assistiti ☒ f) Assistiti ☐ g) Minori ☒ h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo) ☐ Altro: _____
1.5	Categorie di dati personali Artt. 28, par. 3, e 30, par. 1, lett. c), GDPR	☒ a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale) ☒ b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile) ☐ c) Dati di accesso e di identificazione (username, password, customer ID, altro...) ☐ d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...) ☐ e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro...) ☐ f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza ☐ g) Dati di profilazione ☐ h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro...) ☐ i) Dati relativi all'ubicazione ☐ l) Dati che rivelano l'origine razziale o etnica ☐ m) Dati che rivelano le opinioni politiche ☐ n) Dati che rivelano le convinzioni religiose o filosofiche ☐ o) Dati che rivelano l'appartenenza sindacale ☐ p) Dati relativi alla vita sessuale o all'orientamento sessuale ☒ q) Dati relativi alla salute ☐ r) Dati genetici ☐ s) Dati biometrici ☐ t) Altro. Indicare: _____
1.6	Destinatari, soggetti coinvolti e sub-responsabili Artt. 28, parr. 2-4, e 30, par. 1, lett. d), GDPR	Unità/ruoli interni ASL: SATD e SAT UO Screening Mammografico Personale/ruoli del Responsabile: Personale autorizzato del Responsabile Sub-responsabili (coerenti con art. 17): _____ Altri destinatari o enti e relativa funzione: _____

1.7	Durata e criteri di conservazione/cancellazione Artt. 5, par. 1, lett. e), 28, par. 3, lett. g), e 30, par. 1, lett. f), GDPR	Compilare separatamente per: dati operativi/documenti; log applicativi e di sicurezza; log AdS; backup e copie di disaster recovery; eventuale cartaceo. Per ciascuno indicare durata o criterio, evento iniziale (dies a quo), fonte normativa/contrattuale o valutazione, modalità di cancellazione e gestione delle eccezioni. Non applicare termini generici. - La durata della collaborazione è di 24 mesi dalla data di pubblicazione della delibera di approvazione dell'accordo. - I dati personali ricevuti dall'Azienda Sanitaria saranno conservati da Think Pink Italy ETS per un periodo massimo di 30 giorni dalla data di svolgimento dell'evento, decorsi i quali si procederà alla loro cancellazione definitiva e irreversibile. I dati non saranno utilizzati per alcuna finalità ulteriore rispetto alla gestione operativa dell'evento.
1.8	Luoghi di trattamento, archiviazione e accesso Artt. 28, par. 3, lett. a), 30, par. 1, lett. e), e 44 ss. GDPR	Indicare Paese/regione e soggetto per: produzione, replica, backup/DR, assistenza, telemetria/control plane e accesso remoto. [x] Solo SEE: _____ [] Paesi terzi: _____ Strumento di trasferimento, TIA e misure supplementari: _____
1.9	Natura e modalità del trattamento Artt. 24, 25, 28 e 32 GDPR	[] Cartaceo [x] Informatizzato locale [] Cloud/SaaS [] Hosting [] Assistenza remota [] Dispositivi o apparecchiature [] Altro: _____
1.10	Fonte dei dati, se non raccolti presso l'Interessato Art. 14, par. 2, lett. f), GDPR	[x] Interessato [] Professionista/struttura sanitaria: _____ [] Altra fonte: _____ [] Fonte pubblica: _____
1.11	Strumenti e componenti utilizzati Artt. 24, 25 e 32 GDPR	[x] a) Dispositivo/Apparecchiatura (indicare la denominazione) mammografo digitale [] b) Sistema (indicare la denominazione) _____ [] c) Software (indicare la denominazione) _____ [] d) Altro (indicare la denominazione) _____
1.12	Misure tecniche e organizzative ed evidenze Artt. 25, 28, par. 3, lett. c), e 32 GDPR	[x] a) I dati sono trattati in misura minima [x] b) La comunicazione dei dati avviene in modo protetto [] c) I fornitori hanno fornito una DPIA – Valutazione d'impatto [] d) I fornitori hanno la certificazione ISO27001 [x] e) I fornitori hanno designato il Responsabile della Protezione dei Dati [] f) Altro (indicare quali) _____

Articolo 16 – Recapiti della persona referente privacy e del Responsabile della Protezione dei Dati (DPO) del fornitore

Referente contrattuale: nome, ruolo, telefono	ELIANA NASO Direttore Generale enaso@komen.it - 0635405532
--	--

Referente privacy/incidenti: nome, e-mail, telefono	GIUSTINIANA VECCHIOTTI Direttrice Programmi Mission gvecchiotti@komen.it - 0635405533
PEC	slcdpo@pec.it ; postacertificata@pec.komenitalia.it
DPO, se designato: contatti (nome e cognome, numero telefonico, email)	Monica Arbitrio (SLCDPO srls) , 0686327973, info@slcdpo.it

⁽¹⁾ Se il DPO non è stato designato ai sensi dell'art. 37 GDPR, il Responsabile rende disponibile, su richiesta, una dichiarazione motivata e sottoscritta che documenti la valutazione effettuata. Indicare inoltre i canali di reperibilità per incidenti e violazioni, inclusa l'eventuale reperibilità H24.

Articolo 17 – Soggetti sub-responsabili (sub-fornitori)

ID	Ragione sociale	Sede e contatti email e PEC	Servizio/attività	Paesi di trattamento/accesso e capo V	Dati, Interessati e durata
1					
2					
3					
Ultimo aggiornamento dell'elenco			____/____/____		

☒ Il responsabile del trattamento NON affida a sub-fornitori attività che implicino trattamento di dati personali

Articolo 18 – Amministratori di sistema

ID	Nome e Cognome ⁽¹⁾	Ragione Sociale ⁽²⁾	Identificativo account e recapito (mai credenziali/segreti)	Sistemi Amministrati
1				
2				
3				
4				
Ultimo aggiornamento dell'elenco			____/____/____	

⁽¹⁾ se soggetti autorizzati ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/03 e dell'art. 29 del Reg. UE 2016/679

⁽²⁾ se soggetti individuati quali sub-responsabili ai sensi dell'art. 28, parr. 2 e 4, del Regolamento UE 2016/679

[x] Il Responsabile del trattamento NON svolge attività che implicino il ruolo di Amministratore di sistema

Articolo 19 – Principi, Diritti e Misure Tecniche e Organizzative – Requisiti/Schede di Audit

Si indicano, in base alla loro applicabilità in relazione al servizio erogato per conto del Titolare, i principi di trattamento, le misure di sicurezza e i diritti degli interessati, secondo le indicazioni del Regolamento UE 2016/679, del D.Lgs. 196/2003 (così come modificato dal D.Lgs. 101/2018) unitamente alle misure di sicurezza previste, per i quali il responsabile si impegna con la sottoscrizione del presente atto.

Le misure che seguono costituiscono requisiti contrattuali da applicare in funzione dei rischi e del servizio. Eventuali riferimenti ENISA hanno valore di orientamento tecnico e non sostituiscono la valutazione prevista dall'art. 32 GDPR. Il Responsabile ne documenta applicabilità, configurazione ed evidenze e mantiene coerente il proprio registro dei trattamenti.

1) Principi di Trattamento e Diritti degli Interessati

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

2) Misure di Sicurezza

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

Prima dell'avvio, il Responsabile compila una matrice che, per ciascuna misura, riporti: applicabile/non applicabile con motivazione; controllo o misura equivalente; configurazione; responsabile; evidenza e data di verifica. La matrice è parte delle informazioni disponibili per audit ordinari o urgenti.

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

CATEGORIA DI CONTROLLO	ID MISURA	DESCRIZIONE DELLA MISURA
Politiche di sicurezza e procedure per la protezione dei dati personali	1.2	La regolamentazione di cui al punto precedente deve essere riesaminata e aggiornata almeno su base annuale.
	1.3	La regolamentazione deve essere approvata dalla Direzione e comunicata a tutti i dipendenti e alle parti esterne interessate.
	1.4	La regolamentazione deve disciplinare almeno i seguenti punti: ruoli e responsabilità del personale, misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, per i responsabili e sub-responsabili del trattamento dei dati e per le altre terze parti coinvolte nel trattamento dei dati personali.
Ruoli e responsabilità	2.1	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con la politica di sicurezza.
	2.2	Durante le riorganizzazioni interne o le cessazioni e il cambio di impiego, devono essere chiaramente definite le modalità di revoca dei diritti e delle responsabilità con le rispettive procedure di passaggio di consegne.
	2.3	Deve essere effettuata una chiara individuazione e designazione delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
Riservatezza del personale	3.1	Il Responsabile deve garantire che tutto il personale comprenda le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità devono essere chiaramente comunicati durante la fase di attivazione del Servizio/Contratto.
	3.2	Prima di assumere i propri compiti, il personale del Responsabile deve essere invitato a riesaminare e concordare la Regolamentazione di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
Formazione	4.1	Il Responsabile deve garantire che tutto il personale sia adeguatamente formato sui controlli di sicurezza previsti per il servizio e per gli eventuali sistemi informatici ad esso correlati. Il personale coinvolto nel trattamento dei dati personali deve inoltre essere adeguatamente informato e periodicamente aggiornato in merito ai requisiti in materia di protezione dei dati e agli obblighi previsti dalla normativa vigente attraverso regolari campagne di sensibilizzazione.
	4.2	Il Responsabile deve disporre programmi di formazione (relativi alla protezione dei dati personali e alla sicurezza delle informazioni) strutturati e regolari per il proprio personale, compresi programmi specifici per l'inserimento di eventuali nuovi arrivati (es.: job rotation, nuove assunzioni, ecc...).
Politica controllo accessi	5.1	Specifici diritti di accesso devono essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza.
	5.2	Deve essere definita una politica di controllo degli accessi. Nel documento l'organizzazione deve determinare le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali.
	5.3	La segregazione dei ruoli per gestire il controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi) dovrebbe essere chiaramente definita e documentata.
Controllo accessi e autenticazione	6.1	Ove fornita dall'Organizzazione, deve essere attuata la politica di controllo accessi applicabile a tutti gli utenti che accedono ai sistemi IT, con particolare riguardo agli aspetti relativi alla creazione, approvazione, riesame ed eliminazione degli account.
	6.2	L'uso di account generici (non personali) deve essere evitato. Nei casi in cui ciò sia necessario, l'utilizzo deve essere autorizzato dal referente dell'Organizzazione. Qualora tale autorizzazione fosse fornita, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità.
	6.3	L'autenticazione deve essere proporzionata al rischio. È obbligatoria l'autenticazione a più fattori per accessi privilegiati, remoti, amministrativi e per gli accessi a sistemi o dati sanitari esposti fuori dal perimetro fidato; eventuali eccezioni devono essere motivate, approvate e protette da misure compensative verificabili.
	6.4	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio, il sistema di controllo degli accessi deve essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano i criteri definiti al punto precedente.
	6.5	Sui sistemi utilizzati (strumentali) per l'erogazione del servizio deve essere possibile configurare i seguenti parametri relativi alle password: complessità, maximum age, password history, lunghezza e il numero di tentativi di accesso non riusciti accettabili. I criteri dovranno essere concordati con il referente dell'Organizzazione (in base alla politica di controllo accessi).
Gestione risorse e degli asset	7.1	Deve essere predisposto un registro delle risorse IT utilizzate per il trattamento dei dati personali (hardware, software e rete), in funzione di quanto applicabile al servizio esternalizzato. Il compito di mantenere e aggiornare il registro deve essere esplicitamente assegnato.
	7.2	Le risorse IT all'interno del registro essere riesaminate e aggiornate regolarmente.
	7.3	I ruoli che hanno accesso alle risorse devono essere definiti e documentati. In particolare devono essere definite le responsabilità in relazione alle risorse.
Sicurezza fisica	8.1	Il perimetro fisico dei locali in cui è ospitata l'infrastruttura IT utilizzata a fini di erogazione del servizio o vengono effettuati trattamenti di dati personali del Titolare deve essere accessibile esclusivamente a personale esplicitamente autorizzato da parte del Responsabile.

CATEGORIA DI CONTROLLO	ID MISURA	DESCRIZIONE DELLA MISURA
	8.2	Il personale autorizzato all'accesso ai locali di trattamento o ai locali in cui è ospitata l'infrastruttura IT per l'erogazione del servizio deve essere dotato di strumenti di identificazione personali (es. badge identificativi, PIN personali).
	8.3	Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Deve essere mantenuto e monitorato in modo sicuro un registro fisico o una traccia elettronica del controllo di tutti gli accessi.
	8.4	I sistemi di rilevamento anti-intrusione dovrebbero essere installati in tutte le zone di sicurezza.
	8.5	Dovrebbero essere predisposte barriere fisiche per impedire l'accesso fisico non autorizzato.
	8.6	Le aree dei locali non usate dovrebbero essere fisicamente bloccate e periodicamente riesaminate.
	8.7	Nella sala server devono essere predisposti opportuni sistemi antincendio automatici, sistemi dedicati di climatizzazione e gruppi di continuità (UPS) che garantiscano l'erogazione sicura del servizio secondo quanto stabilito contrattualmente.
	8.8	Il personale di supporto esterno deve avere accesso limitato alle aree protette.
Change management	9.1	L'organizzazione deve adottare un processo di cambiamento che consenta di assicurarsi che tutte le modifiche al sistema/servizio siano opportunamente registrate (anche con eventuali aggiornamenti dell'inventario delle risorse) e monitorate.
	9.2	Le modifiche materiali che incidono su finalità, categorie di dati, flussi, luoghi, sub-responsabili, livelli di servizio o sicurezza devono essere comunicate preventivamente al Titolare con impatti, tempi e misure; quando modificano le istruzioni o il rischio richiedono autorizzazione documentata. Le modifiche ordinarie restano tracciate nel processo di change management.
	9.3	Lo sviluppo del software deve essere eseguito in un ambiente speciale, non collegato al sistema IT utilizzato per il trattamento dei dati personali in produzione. Quando è necessario eseguire i test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, il fornitore deve predisporre specifiche procedure per la protezione dei dati personali utilizzati nei test.
Logging e monitoraggio	10.1	Devono essere attivati log proporzionati ai rischi e alle finalità di sicurezza, controllo e assistenza, includendo almeno autenticazioni, eventi privilegiati, operazioni rilevanti sui dati e anomalie. Contenuto, accessi, monitoraggio e periodo di conservazione devono essere definiti nell'art. 15, evitando raccolte eccedenti.
	10.2	I log devono essere protetti da alterazioni e accessi non autorizzati, correlabili e sincronizzati con una fonte temporale affidabile. Devono essere previsti monitoraggio, alert, riesame e cancellazione allo scadere del periodo documentato; per i log AdS si applica anche l'art. 12.
	10.3	È necessario registrare le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / eliminazione / modifica dei diritti di accesso degli utenti.
	10.4	Non deve essere possibile la cancellazione o modifica del contenuto dei log. Anche l'accesso ai log deve essere registrato oltre al monitoraggio effettuato per la rilevazione di attività insolite.
	10.5	Deve essere configurato un sistema di monitoraggio per l'elaborazione dei log e la produzione di rapporti sullo stato del sistema e notifica di potenziali allarmi.
Protezione dal malware	12.1	Devono essere attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti
Backup	14.1	Il Responsabile deve definire con il Titolare RTO e RPO per ciascun servizio o dato rilevante, in coerenza con il contratto e con l'analisi di impatto, e dimostrarne il rispetto mediante prove periodiche di continuità e ripristino.
	14.2	Ai backup deve essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.
	14.3	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.
	14.4	Le strategie e procedure di backup, ripristino e disaster recovery devono essere documentate, applicate, monitorate e testate regolarmente; esiti, anomalie e azioni correttive devono essere conservati come evidenze.
	14.5	I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati.
	14.7	Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine.
	14.8	Prima della trasmissione o conservazione presso servizi terzi, i dati di backup devono essere cifrati con algoritmi e parametri adeguati al rischio. Le chiavi sono gestite separatamente, con accessi limitati, rotazione, backup e revoca documentati.
Sicurezza Server e Database	15.1	I database e application server devono essere configurati affinché lavorino con un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.
	15.2	I database e application server devono elaborare solo i dati personali che sono effettivamente necessari per l'elaborazione al fine di raggiungere i propri scopi di elaborazione.

CATEGORIA DI CONTROLLO	ID MISURA	DESCRIZIONE DELLA MISURA
	15.3	La cifratura dei dati a riposo e in transito deve essere adottata quando appropriata al rischio, con gestione documentata delle chiavi. L'eventuale esclusione deve essere motivata e accompagnata da misure compensative approvate e verificabili.
	15.4	Nei sistemi utilizzati per l'erogazione del servizio, ove possibile, devono essere applicate tecniche di pseudonimizzazione attraverso la separazione dei dati dagli identificatori al fine di evitare il collegamento diretto con l'interessato. In caso non fosse possibile, deve essere fornita adeguata (documentata) motivazione e devono essere adottate misure compensative che consentano di proteggere i dati trattati.
Network/Communication security	16.1	Deve essere predisposta e monitorato il rispetto di una policy per la Sicurezza di Rete (Network Security Policy) e per la gestione delle Comunicazioni Sicure (Network Communication Security) che preveda l'adozione di misure di cifratura delle comunicazioni nell'ambito dei processi di trattamento effettuati (TLS/Https, VPN, SSH, ecc...).
Sicurezza desktop/laptop/mobile	17.1	Gli utenti non devono essere in grado di disattivare o aggirare le impostazioni di sicurezza.
	17.2	Le applicazioni anti-virus e le relative signatures devono essere configurate regolarmente in maniera continuativa.
	17.3	Gli utenti non devono avere i privilegi per installare applicazioni software non autorizzate o disattivare applicazioni autorizzate
	17.4	I sistemi utilizzati per l'erogazione del servizio, devono disporre di un timeout di sessione nel caso in cui l'utente non sia stato attivo per un determinato periodo di tempo (max 10 min).
	17.5	Le vulnerabilità e le patch devono essere valutate e trattate secondo criticità, esposizione e SLA contrattuali. Per vulnerabilità critiche o attivamente sfruttate sono richieste mitigazioni tempestive, tracciamento dell'eccezione e comunicazione al Titolare quando il rischio interessa il servizio o i dati ASL.
	17.6	Non è consentito il trasferimento di dati personali dai Database dei sistemi aziendali alle workstation utilizzate a fini di assistenza tecnica, se non previa esplicita autorizzazione del Responsabile dei Sistemi Informativi. I dati temporaneamente memorizzati devono essere cancellati alla fine della sessione di lavoro.
	17.7	Non deve essere consentito il trasferimento di dati personali da workstation a dispositivi di archiviazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
	17.8	Deve essere abilitata la crittografia dei dischi delle postazioni di lavoro/laptop/device mobili utilizzate nell'ambito dell'erogazione del servizio
Dispositivi portatili	18.1	Le procedure di gestione dei dispositivi mobili e portatili devono essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.
	18.2	I dispositivi mobili ai quali è consentito accedere al sistema informativo devono essere pre-registrati e pre-autorizzati: non è consentito l'utilizzo di dispositivi personali, salvo eventuali specifiche autorizzazioni.
	18.3	I dispositivi mobili devono essere soggetti alle stesse procedure di controllo degli accessi (al sistema IT) delle altre apparecchiature terminali (client).
	18.4	Il Responsabile deve individuare e comunicare al Titolare un proprio referente a cui attribuire la responsabilità della gestione dei dispositivi mobili e portatili utilizzati nell'ambito dell'erogazione del servizio.
	18.5	Il Responsabile deve essere in grado di cancellare da remoto i dati personali su un dispositivo mobile compromesso, nel caso in cui questo sia utilizzato nell'ambito dell'erogazione del servizio.
	18.6	In caso di utilizzo promiscuo dei dispositivi mobili (fini di erogazione del servizio al titolare e fini privati) deve essere prevista, mediante opportuni software containers sicuri, la separazione dell'uso privato dall'uso aziendale del dispositivo.
	18.7	I dispositivi mobili devono essere fisicamente protetti contro il furto quando non sono in uso.
Sicurezza del ciclo di vita delle applicazioni	19.1	Lo sviluppo degli applicativi deve essere conforme alle linee guida per lo sviluppo del software sicuro nella pubblica amministrazione pubblicate da AGID.
Sub-responsabile del trattamento	20.1	Il Responsabile deve mettere in atto misure idonee a garantire l'esecuzione esclusiva di istruzioni lecite e documentate contenute nel presente ATD, nei documenti contrattuali e nelle successive comunicazioni tracciate del Titolare.
	20.2	Il Responsabile del Trattamento deve osservare le indicazioni fornite nell'atto di designazione in caso di violazione di dati personali e nelle presenti misure di sicurezza.
	20.3	Il Responsabile deve sottoscrivere l'atto di designazione in cui sono contenuti requisiti formali e obblighi. Il Responsabile del trattamento deve, in risposta, fornire prove documentate sufficienti di conformità (es.: certificazioni di sicurezza, schede tecniche relative alle misure di sicurezza adottate per il servizio/sistema): in caso alternativo, verrà adottata una specifica politica di auditing.
	20.4	Il Responsabile dovrebbe verificare regolarmente la conformità del sub-responsabile al livello concordato di requisiti e obblighi.
	20.5	Il personale del responsabile del trattamento che elabora dati personali deve essere soggetto a specifici accordi documentati di riservatezza / non divulgazione.
Gestione degli incidenti / Violazione dei dati personali	21.1	Il Responsabile deve predisporre un proprio piano di risposta agli incidenti con procedure dettagliate che preveda la comunicazione al titolare (committente), secondo le indicazioni fornite nell'atto di designazione, al fine di garantire una risposta efficace e ordinata agli incidenti e violazioni relativi ai dati personali.

CATEGORIA DI CONTROLLO	ID MISURA	DESCRIZIONE DELLA MISURA
	21.2	Le violazioni dei dati personali, di competenza del Titolare, devono essere segnalate immediatamente alla Direzione. In qualità di Responsabile devono essere adottate specifiche procedure di supporto al Titolare per la notifica e la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR.
	21.3	La procedura di gestione delle violazioni di cui al punto precedente, deve essere documentata: essa deve includere un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.
	21.4	Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione eseguite.
Business Continuity	22.1	Il Responsabile deve predisporre e mantenere un piano di continuità operativa e disaster recovery coerente con RTO/RPO concordati, dipendenze e scenari di indisponibilità. Il piano deve essere testato con periodicità proporzionata al rischio; risultati e azioni correttive sono messi a disposizione del Titolare.
	22.2	Il Piano di Continuità Operativa indicato al punto precedente deve includere azioni chiare e assegnazione di ruoli.
	22.3	Il Piano di Continuità Operativa deve essere in linea con il livello di qualità del servizio da garantire all'Organizzazione (Committente), con particolare riguardo alla sicurezza dei dati personali dei processi fondamentali di erogazione.
Cancellazione/eliminazione dei dati	23.1	I dati e i supporti devono essere cancellati, bonificati o distrutti in modo sicuro e verificabile, secondo tipo di supporto, rischio e stato dell'arte. La distruzione fisica è richiesta quando la cancellazione sicura non è tecnicamente affidabile o quando prevista dalle istruzioni del Titolare.
	23.2	La distruzione di documenti deve avvenire mediante opportuni dispositivi di triturazione.
	23.3	Se sono utilizzati servizi di terzi per eliminare in modo sicuro i supporti di memorizzazione o documenti cartacei, è necessario stipulare uno specifico contratto di servizio e produrre un formale attestato di distruzione.

Articolo 20 – Disposizioni Finali

- 1) La presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Contratto.
- 2) La mancata sottoscrizione del presente Accordo non consente l'avvio dei trattamenti affidati né l'accesso ai dati personali previsti dal Contratto.
- 3) Il Responsabile comunica immediatamente le variazioni soggette a preventiva informazione o autorizzazione ai sensi degli artt. 11, 12 e 17 e, almeno annualmente entro il 31 dicembre, conferma o aggiorna i dati di cui agli artt. 14, 16, 17 e 18.
- 4) Resta inteso che la mancata esecuzione delle istruzioni contenute nel presente ATD, costituisce una violazione del Contratto, di cui il presente ATD è parte integrante, del Regolamento UE 2016/679 e del D.Lgs. 196/2003 (come modificato dal D.Lgs. 101/2018) oltre che di quanto disposto dalla normativa vigente.
- 5) Il presente Accordo è sottoscritto dal Legale Rappresentante del Titolare nell'ambito e nei limiti della delega conferita dal Titolare e dal legale rappresentante del Responsabile o da persona munita di idonei poteri.
Per quanto non espressamente previsto si applicano il GDPR, il Codice e la normativa vigente. In caso di conflitto sulle materie di protezione dei dati, prevale la disposizione più specifica del presente ATD, fatti salvi gli obblighi inderogabili e le successive istruzioni documentate e lecite del Titolare.

Il Legale Rappresentante ASL 03 Pescara

Per ricezione ed integrale accettazione
del Responsabile



Il Dirigente Amministrativo, con la presente sottoscrizione, attesta la regolarità tecnica e amministrativa nonché la legittimità del provvedimento

Il Dirigente Amministrativo

Enrico Croce

firmato digitalmente

Il Direttore dell'UOC Controllo di Gestione attesta che la spesa risulta corrispondente al bilancio di previsione dell'anno corrente.

Il Direttore

firmato digitalmente

Il Direttore dell'UOC Bilancio e Gestione Economica Finanziaria attesta che la spesa risulta imputata sulla voce di conto del Bilancio n.

Anno

Il Direttore

firmato digitalmente

Ai sensi del D. Lgs. 502/92 e successive modificazioni ed integrazioni, i sottoscritti esprimono il seguente parere sul presente provvedimento:

Parere favorevole

IL DIRETTORE AMMINISTRATIVO

Dott. Francesca Rancitelli

firmato digitalmente

Parere favorevole

IL DIRETTORE SANITARIO

Dott. Rossano Di Luzio

firmato digitalmente

IL DIRETTORE GENERALE

Dott. Vero Michitelli

firmato digitalmente

Deliberazione n. 1555 del 05/10/2026 ad oggetto:

APPROVAZIONE SCHEMA DI ACCORDO DI COLLABORAZIONE PER LO SVILUPPO DEL PROGETTO "CAROVANA DELLA PREVENZIONE" E DETERMINAZIONI CONSEGUENTI.

CERTIFICATO DI PUBBLICAZIONE

- Si attesta che il presente atto viene pubblicato, in forma integrale, all'ALBO ON LINE dell'ASL di Pescara (art. 32 L. 69/09 e s.m.i.), in data 6/10/2026 per un periodo non inferiore a 15 giorni consecutivi.

Atto soggetto al controllo della Regione (art. 4, co. 8 L. 412/91): NO

Il Funzionario Incaricato