ACCORDO SUL TRATTAMENTO DEI DATI (DPA)

AI SENSI DELL'ART. 28 DEL REGOLAMENTO (UE) 2016/679 (GDPR)

TRA

L'Azienda Sanitaria Locale N.7 DEL Sulcis Iglesiente con sede legale in Carbonia (CI) via Dalmazia 83 C.F./P.IVA 03990310926 d'ora in avanti denominata **"Titolare del trattamento"** o **"ASL"**, rappresentata dal dott. Paolo Cannas Legale Rappresentante pro-tempore

E

PUBLIPEAS srl, con sede legale in via S. Pellico 10 Casoria (NA) CAP 80026 C.F./P.IVA 05452191215, d'ora in avanti denominato **"Responsabile del trattamento"** o **"Fornitore"**, rappresentato dal Legale Rappresentante pro-tempore Dott.ssa Assunta Telese.

PREMESSO CHE:

- Con Contratto/Convenzione stipulato in data [Data] (di seguito **"Contratto Principale"**), la ASL ha affidato al Fornitore l'esecuzione del servizio di: **attività di screening mammella, cervice uterina, colon retto con l'ausilio di un poliambulatorio mobile attrezzato da impiegare nel territorio della ASL Sulcis Iglesiente e servizi connessi di call center per prenotazioni e inviti per lo screening oncologico istituzionale.**
- L'esecuzione delle attività sopra citate comporta necessariamente il trattamento di dati personali, anche appartenenti a **categorie particolari (dati relativi alla salute)**, dei cittadini residenti nel territorio di competenza della ASL.
- Con il presente Data Processing Agreement, le Parti intendono disciplinare tale trattamento in conformità all'art. 28 del Regolamento (UE) 2016/679 ("GDPR") e alla normativa applicabile in materia di protezione dei dati personali.

SI CONVIENE E SI STIPULA QUANTO SEGUE:

Art. 1 - Oggetto e Nomina

Le premesse costituiscono parte integrante e sostanziale del presente accordo.

La ASL nomina il Fornitore, che accetta, Responsabile del Trattamento dei dati personali ex art. 28 GDPR relativamente alle sole attività descritte nel Contratto Principale e secondo le specifiche tecniche contenute nel presente Atto.

Il Responsabile si impegna a trattare i dati personali esclusivamente nei limiti necessari all'esecuzione dei servizi affidati e nel rispetto delle istruzioni documentate impartite dal Titolare.

Art. 2 - Natura, Finalità e Dettagli del Trattamento

Il trattamento è svolto a bordo dell'unità mobile nel territorio della ASL, presso la sede del Responsabile per le attività di call center e, per la refertazione a distanza, mediante accesso ai sistemi informativi del Titolare (RIS/PACS, piattaforma screening) attraverso canali cifrati messi a disposizione o autorizzati dal Titolare. La durata del trattamento coincide con quella del Contratto Principale (art. 7).

Il trattamento ha per oggetto le operazioni strettamente necessarie alla gestione del programma di screening oncologico quali: raccolta, registrazione, organizzazione, conservazione, consultazione, estrazione, comunicazione, cancellazione o altre operazioni effettivamente pertinenti.

- **Categorie di interessati:** Cittadini/pazienti inclusi nelle coorti di screening della ASL nelle fasce di età previste, per ciascuna linea di screening - mammella, cervice uterina, colon-retto -, dai programmi regionali di screening oncologico
- **Tipologia di dati personali:** Dati anagrafici, codice fiscale, dati di contatto, tessere sanitarie, dati sulla salute (esiti esami, anamnesi, appuntamenti diagnostici, familiarità oncologica, immagini diagnostiche, campioni biologici etichettati e relativa documentazione di tracciabilità, questionari di rischio).

Art. 3 - Obblighi del Responsabile del Trattamento

Il Responsabile si impegna a:

1. **Istruzioni Documentate:** Trattare i dati esclusivamente sulla base delle istruzioni documentate fornite dalla ASL. Non utilizzare i dati per finalità proprie;

2. **Dovere di informazione** Informare immediatamente il Titolare qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, in materia di protezione dei dati (art. 28, par. 3, ultimo capoverso, GDPR);

3. **Informativa all'utenza** Utilizzare, nei rapporti con gli utenti, esclusivamente l'informativa e la modulistica predisposte dal Titolare, astenendosi dal raccogliere consensi o dal rendere informative in nome proprio.

4. **Riservatezza:** Garantire che le persone autorizzate al trattamento (es. medici, infermieri, tecnici, amministrativi) designate per iscritto quali persone autorizzate ai sensi dell'art. 2-quaterdecies del d.lgs. 196/2003, si siano impegnate alla massima riservatezza o abbiano un adeguato obbligo legale di riservatezza. Il Responsabile assicura inoltre che l'accesso ai dati sia consentito esclusivamente ai soggetti che ne abbiano effettiva necessità in relazione alle mansioni svolte e che tali soggetti ricevano adeguate istruzioni in materia di trattamento e protezione dei dati personali.
5. **Misure di Sicurezza (Art. 32 GDPR):** Adottare tutte le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio elevato del trattamento (dati sanitari). In particolare:

    a. Sistemi di **cifratura e pseudonimizzazione** dei dati sensibili;

    b. Controllo degli accessi rigoroso basato su profili autorizzativi (Principio del *least privilege*);

    c. **Tracciamento degli accessi (Log di audit)** con conservazione non inferiore a 24 mesi, in conformità alle Linee guida del Garante in materia di dossier sanitario (provv. 4 giugno 2015);
    d. Sistemi di disaster recovery e backup periodici per garantire la resilienza;

    e. Accesso ai sistemi informativi del Titolare (RIS/PACS, piattaforma screening, applicativi) esclusivamente mediante i canali cifrati (VPN) e le credenziali personali, nominative e non cedibili, rilasciate o autorizzate dal Titolare, nel rispetto delle politiche di sicurezza aziendali; cifratura dei dati memorizzati sui dispositivi e sui supporti informatici mobili impiegati a bordo dell'unità mobile.

Il Titolare potrà, in qualsiasi momento, richiedere al Responsabile il riscontro e la verifica delle misure adottate ed in uso nonché chiederne l'implementazione ovvero la modifica, tenendo conto dello stato dell'arte e dei costi di attuazione.

6. **Sub-responsabili:** Non affidare a terzi (sub-responsabili) alcuna operazione di trattamento senza la **previa autorizzazione scritta**, specifica o generale, della ASL. Il Responsabile assicura che ogni sub-responsabile sia vincolato, mediante contratto o altro atto giuridico, a obblighi in materia di protezione dei dati personali sostanzialmente equivalenti a quelli previsti dal presente Data Processing Agreement.

   In caso di autorizzazione generale, il Responsabile comunica per iscritto al Titolare, con congruo anticipo, ogni prevista aggiunta o sostituzione di sub-responsabili, consentendo al Titolare di opporsi a tali modifiche (art. 28, par. 2, GDPR). L'elenco dei sub-responsabili di cui il Responsabile intende avvalersi (ivi compresi eventuali fornitori di servizi informatici, di connettività e di call center, nonché i professionisti refertatori non dipendenti) è comunicato per iscritto al Titolare prima dell'avvio del servizio.
   Resta inteso che l'incarico dei Sub-Responsabili potrà avvenire solo prima dell'inizio di qualsivoglia operazione di trattamento da parte di questi ultimi.

   Il Responsabile del trattamento resta comunque unico responsabile di tutti gli obblighi assunti con il presente accordo. Il Responsabile risponderà, dunque, del corretto svolgimento delle attività devolute al Sub-Responsabile da lui nominato e degli eventuali inadempimenti o violazioni da quest'ultimo commessi.

7. **Diritti degli Interessati:** Assistere la ASL con misure tecniche e organizzative adeguate a dare seguito alle richieste di esercizio dei diritti dei pazienti (accesso, cancellazione, rettifica), trasmettendo alla ASL ogni richiesta entro **3 giorni** dalla ricezione. Qualora una richiesta proveniente da un interessato sia ricevuta direttamente dal Responsabile e riguardi dati trattati per conto del Titolare, il Responsabile la trasmette tempestivamente al Titolare e non vi dà autonomamente seguito, salvo diversa istruzione o obbligo derivante dalla normativa applicabile.

Art. 4 - Gestione delle Violazioni di Dati (Data Breach)

Il Responsabile si impegna a notificare alla ASL qualsiasi violazione dei dati personali (**Data Breach**) senza ingiustificato ritardo e, in ogni caso, **entro e non oltre 24 ore** dal momento in cui ne viene a conoscenza.

La notifica dovrà avvenire tramite PEC all'indirizzo del Titolare protocollo@pec.aslsulcis.it e tramite PEO al DPO (dpo@aslsulcis.it) e all'Ufficio Privacy aziendale (ufficio.privacy@aslsulcis.it) fornendo tutte le informazioni disponibili ai sensi dell'art. 33, par. 3, GDPR.

Il Responsabile collabora con il Titolare nell'attività di analisi, contenimento, mitigazione e gestione dell'incidente, adottando senza ritardo le misure ragionevolmente necessarie per limitarne le conseguenze.

Art. 5 - Audit e Ispezioni

Il Responsabile mette a disposizione della ASL tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al articolo di cui all'art. 28 GDPR e al presente Accordo e consente e contribuisce alle attività di **audit, comprese le ispezioni**, eseguiti dalla ASL e/o dal DPO aziendale.

Art. 6 – Assistenza al Titolare e valutazione d'impatto

Tenuto conto della natura del trattamento e delle informazioni a propria disposizione, il Responsabile presta al Titolare l'assistenza necessaria per garantire il rispetto degli obblighi previsti dagli artt. 32-36 GDPR.

In particolare, ove necessario, il Responsabile fornisce le informazioni ragionevolmente richieste dal Titolare ai fini della predisposizione o dell'aggiornamento di una valutazione d'impatto sulla protezione dei dati e collabora nell'eventuale procedura di consultazione preventiva dell'Autorità di controllo.

Art. 7 - Durata e Destinazione dei Dati alla Cessazione

Il presente Atto ha la medesima durata del Contratto Principale e pertanto, cesserà al momento del completo adempimento o dello scioglimento del vincolo contrattuale.

Alla cessazione del rapporto, il Responsabile dovrà **restituire integralmente** i dati alla ASL in un formato strutturato e interoperabile, distruggendo le copie residue e attestandone per iscritto l'avvenuta distruzione salvo che la legge ne imponga la conservazione.

In difetto di indicazioni da parte del Titolare, il Responsabile provvederà alla trasmissione di apposita comunicazione finalizzata a disciplinare la gestione dei dati nei termini su indicati.

Nell'ipotesi di mancato riscontro da parte del Titolare, nel termine di 20 (venti) giorni dal ricevimento della suddetta comunicazione, il Responsabile procederà comunque, con la restituzione dei dati e delle copie dei backup, con conseguente cancellazione e distruzione di ogni eventuale copia.

Art. 8 – Responsabilità e conformità normativa

Ciascuna Parte è tenuta al rispetto degli obblighi direttamente posti a proprio carico dal GDPR e dalla normativa applicabile in materia di protezione dei dati personali.

Il Responsabile informa tempestivamente il Titolare di qualsiasi circostanza che possa incidere in maniera significativa sulla propria capacità di adempiere agli obblighi derivanti dal presente Data Processing Agreement.

Resta ferma l'applicazione delle disposizioni del GDPR in materia di responsabilità e diritto al risarcimento, nonché delle eventuali ulteriori previsioni sulla responsabilità contenute nel contratto principale, purché compatibili con la normativa inderogabile applicabile.

Art. 9 – Rapporti con il contratto principale e disposizioni finali

Il presente Data Processing Agreement costituisce parte integrante del contratto intercorrente tra le Parti avente ad oggetto il servizio di screening indicato in premessa (Contratto Principale).

In caso di contrasto tra le disposizioni del presente Accordo relative alla protezione dei dati personali e quelle contenute nel contratto principale, prevalgono le disposizioni del presente Accordo per quanto concerne gli aspetti specificamente relativi al trattamento dei dati personali, salvo che sia espressamente previsto diversamente e purché la diversa disciplina sia compatibile con il GDPR.

Qualsiasi modifica del presente Data Processing Agreement dovrà risultare da atto scritto, anche in formato elettronico.

Per quanto non espressamente previsto trovano applicazione il Regolamento (UE) 2016/679, la normativa nazionale applicabile e gli altri atti normativi pertinenti in materia di protezione dei dati personali.

Luogo, Data Carbonia, lì

Per l'Azienda Sanitaria Locale (Titolare) IL Direttore Generale Asl Sulcis Iglesiente Dott. Paolo Cannas

CANNAS PAOLO
Firmato digitalmente da CANNAS PAOLO
Data: 2026.11.02 16:22:00 +01'00'

Per l'Operatore Economico (Responsabile)

ASSUNTA TELESE
02.11.2026 12:59:52 GMT+01:00