Art. 28 GDPR | Accordo contrattuale

Data Processing Agreement (DPA)

Accordo sul trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (UE) 2016/679

Versione: 2.0.3 | Data di efficacia: 30 Ottobre 2026 | Ultimo aggiornamento: 30 ottobre 2026

Natura del documento. Il presente Accordo disciplina il trattamento dei dati personali che Giorgio Arghittu (Refertius) effettua *per conto* del medico, del professionista sanitario o della struttura che utilizza la piattaforma. È un documento contrattuale distinto dall'Informativa sulla Privacy, dall'informativa ai pazienti, dalla pagina Sicurezza e Conformità e dalla valutazione d'impatto (DPIA).

La sottoscrizione del presente Accordo non costituisce, da sola, attestazione di conformità del trattamento svolto dal Titolare, né certificazione di conformità di Refertius.

La versione 2.0 sostituisce integralmente la versione 2.1 del 7 settembre 2026, conservata come versione storica ai fini di audit e versioning documentale.

PARTE I — LE PARTI

Titolare del trattamento (Cliente)

• Ragione sociale / nome: _____
• Sede: _____
• P.IVA / Codice fiscale: _____
• Email: _____
• Referente privacy: _____

Responsabile del trattamento (Refertius)

• Soggetto: ARGHITTU GIORGIO
• Forma: persona fisica titolare di partita IVA
• Sede: Via Giacomo Griziotti 4 — 20145 Milano, Italia
• P.IVA: 14678340960
• PEC: giorgio@pec.refertius.com
• Contatto privacy: privacy@refertius.com
• Referente privacy: Giorgio Arghittu — privacy@refertius.com
• Responsabile della protezione dei dati (DPO): in fase di formalizzazione. Le comunicazioni in materia di protezione dei dati vanno indirizzate al contatto privacy sopra indicato.
• Rappresentante ex art. 27 GDPR: non applicabile (soggetto stabilito nell'Unione).

ARTICOLO 1 — DEFINIZIONI

"Accordo" o "DPA": il presente Data Processing Agreement;

"Titolare": il medico, il professionista sanitario o la struttura che utilizza la Piattaforma per trattare i dati dei propri pazienti;

"Responsabile": Giorgio Arghittu (Refertius);

"Sub-responsabile": il terzo incaricato dal Responsabile di specifiche attività di trattamento per conto del Titolare;

"Dati Personali": le informazioni di cui all'art. 4.1 GDPR;

"Dati relativi alla salute": i dati di cui all'art. 4.15 GDPR, rientranti nelle categorie particolari dell'art. 9 GDPR;

"Violazione dei Dati": la violazione di cui all'art. 4.12 GDPR;

"Piattaforma": il servizio Refertius come descritto nei Termini di Servizio;

"EXTERNAL_AI_PROCESSING": il flusso di elaborazione automatica che comporta la trasmissione di contenuto a fornitori esterni di trascrizione o di elaborazione linguistica;

"CLINICAL_DOCUMENT_DELIVERY": il flusso di consegna del referto al destinatario indicato e confermato dal medico.

ARTICOLO 2 — OGGETTO, RUOLI E LIMITI

2.1 Il Titolare determina finalità e mezzi del trattamento dei dati dei propri pazienti. Il Responsabile tratta tali dati esclusivamente per conto del Titolare, nei limiti descritti nell'Allegato A.

2.2 Il Responsabile agisce invece come **titolare autonomo** per i trattamenti relativi ad account, autenticazione, fatturazione, sicurezza, log tecnici e comunicazioni di servizio: tali trattamenti sono disciplinati dall'Informativa sulla Privacy e non dal presente Accordo.

2.3 **Refertius non sostituisce il medico.** La Piattaforma è uno strumento di supporto documentale: non emette diagnosi e non decide la firma né la trasmissione del referto. Il controllo professionale sul contenuto del documento, la decisione di firmarlo e la decisione di trasmetterlo restano del Titolare.

2.4 Il presente Accordo non attribuisce al Responsabile alcuna facoltà di determinare finalità proprie sui dati clinici del Titolare.

ARTICOLO 3 — DURATA

3.1 L'Accordo ha efficacia dalla data di efficacia indicata in epigrafe e resta valido per tutta la durata del trattamento dei Dati Personali effettuato per conto del Titolare.

3.2 La cessazione del servizio determina la cessazione del trattamento, salvi gli obblighi di conservazione previsti dalla legge e quanto indicato all'Articolo 13 e nell'Allegato E.

ARTICOLO 4 — ISTRUZIONI DEL TITOLARE (ARTT. 28.3, 29 GDPR)

4.1 Il Responsabile tratta i Dati Personali esclusivamente sulla base delle istruzioni documentate del Titolare. Costituiscono istruzioni documentate: il presente Accordo, la configurazione del servizio scelta dal Titolare e l'utilizzo delle funzionalità della Piattaforma.

4.2 Istruzioni ulteriori sono trasmesse per iscritto a privacy@refertius.com. Se comportano modifiche tecniche o attività straordinarie, la loro esecuzione è subordinata alla fattibilità tecnica e, ove necessario, a un accordo economico separato.

4.3 Se un'istruzione appare al Responsabile in contrasto con la normativa applicabile in materia di protezione dei dati, il Responsabile ne informa il Titolare e può sospenderne l'esecuzione fino a chiarimento.

4.4 Il Responsabile **non utilizza i dati clinici del Titolare per finalità proprie**, incluso l'addestramento di modelli di intelligenza artificiale, in assenza di una base giuridica e di una documentazione specifica e separata concordata con il Titolare.

ARTICOLO 5 — RISERVATEZZA (ART. 28.3.b GDPR)

5.1 L'accesso ai Dati Personali è limitato alle persone autorizzate e nei limiti necessari alle rispettive funzioni, secondo le misure e le procedure applicabili.

5.2 Le persone autorizzate sono vincolate a un obbligo di riservatezza di natura contrattuale o legale, che permane oltre la cessazione del rapporto.

ARTICOLO 6 — SICUREZZA DEL TRATTAMENTO (ART. 32 GDPR)

6.1 Il Responsabile adotta le misure tecniche e organizzative descritte nell'**Allegato C**, adeguate al rischio e soggette a riesame periodico.

6.2 Le Parti riconoscono che nessuna misura di sicurezza può garantire una protezione assoluta. Il Responsabile non dichiara certificazioni di terzi che non possiede.

ARTICOLO 7 — ELABORAZIONI AUTOMATICHE E CONSEGNA DEL REFERTO: DUE FLUSSI DISTINTI

7.1 EXTERNAL_AI_PROCESSING

Per la trascrizione, la strutturazione, la generazione e la verifica automatica del testo del referto il Responsabile può ricorrere a fornitori esterni di elaborazione (Allegato D). In tale flusso:

• sono trasmessi solo i dati necessari alla funzione richiesta (minimizzazione);

• l'identità diretta del paziente è schermata prima della trasmissione e ripristinata solo all'interno dell'ambiente Refertius (identity shielding);

• il controllo è **fail-closed**: se la schermatura non risulta verificata, la richiesta al fornitore esterno non viene effettuata e l'operazione termina con errore tecnico;

• non è previsto alcun percorso alternativo che aggiri il controllo, incluso il ricorso a fornitori alternativi.

7.2 CLINICAL_DOCUMENT_DELIVERY

Il medico può disporre esplicitamente l'invio del referto al destinatario da lui indicato e confermato, tipicamente il paziente. In tale flusso:

• il **PDF completo del referto** è il contenuto oggetto della consegna e viene trasmesso al fornitore di consegna email indicato nell'Allegato D;

• il PDF contiene dati identificativi e dati relativi alla salute del paziente: la schermatura dell'identità di cui al 7.1 **non** si applica a questo flusso;

• l'invio richiede un medico autenticato, la verifica lato server della titolarità del referto e un'azione esplicita del medico; in mancanza di tali condizioni l'invio non viene effettuato;

• oggetto della email e nome del file allegato sono imposti dal sistema in forma neutra e il corpo del messaggio non contiene contenuto clinico.

Le Parti riconoscono espressamente che il contenuto clinico del referto è trasmesso a un fornitore terzo di consegna email quando il medico dispone l'invio: non è dichiarato che il contenuto del referto non sia mai trasmesso a terzi.

7.3 **Fonti esterne e codifiche.** Il Responsabile può consultare fonti istituzionali e cataloghi di terzi (banche dati sui farmaci e relativi codici, nomenclatori regionali e nazionali delle prestazioni, classificazioni diagnostiche) al solo fine di supportare la redazione del documento. Tali soggetti non ricevono dati personali dei pazienti e non agiscono come sub-responsabili. L'impiego di tali fonti non costituisce garanzia di correttezza, completezza o aggiornamento del dato: la verifica del contenuto resta in capo al Titolare.

ARTICOLO 8 — SUB-RESPONSABILI (ARTT. 28.2, 28.4 GDPR)

8.1 Il Titolare autorizza in via generale il ricorso ai soggetti elencati nell'**Allegato D**, secondo la classificazione e lo stato di due diligence ivi indicati.

8.2 Il Responsabile impone contrattualmente a ciascun sub-responsabile obblighi di protezione dei dati adeguati, nella misura consentita dai termini del fornitore, e resta responsabile verso il Titolare dell'adempimento degli obblighi del sub-responsabile.

8.3 Le modifiche all'elenco sono notificate al Titolare con almeno 30 giorni di preavviso. Il Titolare può opporsi entro tale termine per motivi ragionevoli e documentati relativi alla protezione dei dati; l'obiezione è gestita in forma documentata e le Parti ricercano una soluzione alternativa. Se una soluzione non è praticabile, il Titolare può recedere dalla parte di servizio interessata.

8.4 L'Allegato D costituisce l'elenco ufficiale dei sub-responsabili. In caso di divergenza tra le pagine informative del sito e il presente elenco, **prevale il presente Accordo**.

ARTICOLO 9 — VIOLAZIONI DEI DATI (ARTT. 33-34 GDPR)

⚠ Notifica senza ingiustificato ritardo

Il Responsabile notifica al Titolare ogni violazione dei Dati Personali trattati per conto del Titolare **senza ingiustificato ritardo** dopo esserne venuto a conoscenza, in tempo utile perché il Titolare possa adempiere ai propri obblighi ai sensi degli artt. 33 e 34 GDPR.

9.1 La notifica contiene le informazioni disponibili al momento, tra cui:

• descrizione della natura della violazione;
• categorie e numero approssimativo di interessati coinvolti;
• categorie e numero approssimativo di registrazioni coinvolte;

• punto di contatto per ulteriori informazioni;
• probabili conseguenze della violazione;
• misure adottate o proposte per porvi rimedio.

9.2 Quando non è possibile fornire tutte le informazioni contestualmente, esse sono fornite in fasi successive senza ulteriore ingiustificato ritardo.

9.3 Il Responsabile collabora con il Titolare nella valutazione del rischio e negli adempimenti verso l'Autorità di controllo e gli interessati. Le Parti riconoscono che i tempi di notifica possono dipendere anche dalle informazioni ricevute dai sub-responsabili: il Responsabile non assume termini inferiori a quelli che è in grado di rispettare.

ARTICOLO 10 — DIRITTI DEGLI INTERESSATI (ART. 28.3.e GDPR)

10.1 Il Responsabile assiste il Titolare, nella misura ragionevolmente possibile e tenuto conto delle funzionalità disponibili, nelle richieste relative a accesso, rettifica, cancellazione, limitazione, portabilità, opposizione e agli altri diritti applicabili.

10.2 La valutazione e la risposta alle richieste degli interessati restano in capo al Titolare, salvo diverso accordo scritto. Le richieste ricevute direttamente dal Responsabile sono inoltrate al Titolare senza risposta nel merito.

ARTICOLO 11 — ASSISTENZA, DPIA E COOPERAZIONE (ARTT. 28.3.f, 32-36 GDPR)

11.1 Su richiesta scritta, il Responsabile fornisce le informazioni e la documentazione disponibili utili al Titolare per la valutazione d'impatto sulla protezione dei dati (DPIA), per le valutazioni di sicurezza, per le richieste dell'Autorità di controllo e per gli obblighi di accountability.

11.2 L'assistenza è prestata in misura proporzionata al ruolo del Responsabile e alle informazioni effettivamente disponibili. Attività straordinarie, ripetute o particolarmente onerose possono essere subordinate a costi preventivamente concordati.

ARTICOLO 12 — CONSERVAZIONE DEI DATI

12.1 Le durate di conservazione, differenziate per categoria di dato, sono indicate nell'**Allegato E**. Non è prevista una durata unica per tutte le categorie.

12.2 Le durate applicate dai sub-responsabili sono quelle previste dai rispettivi accordi sul trattamento dei dati indicati nell'Allegato D.

ARTICOLO 13 — CANCELLAZIONE E RESTITUZIONE

13.1 Alla cessazione del servizio, o su istruzione del Titolare, il Responsabile restituisce e/o cancella i Dati Personali trattati per conto del Titolare, secondo le istruzioni del Titolare, la normativa applicabile e la politica di conservazione, salvo obblighi di conservazione. La restituzione avviene tramite le funzionalità di esportazione disponibili; l'esportazione dei referti è utilizzabile anche durante il rapporto ed è distinta dalla chiusura dell'account.

13.1-bis L'Archivio del servizio è uno spazio operativo di consultazione e gestione durante il rapporto; non costituisce l'archivio sanitario istituzionale del Titolare e non trasferisce al Responsabile gli obblighi di conservazione della documentazione sanitaria del Titolare. L'eventuale conferma di ricezione dell'esportazione documenta la restituzione e non modifica la ripartizione dei ruoli prevista dal presente Accordo.

13.2 La chiusura dell'account segue la sequenza: richiesta → esportazione (pacchetto con manifest SHA-256) → download verificato → conferma di ricezione → controllo di conservazione → cancellazione. La cancellazione rimuove, in un'unica transazione del database, i dati applicativi associati all'account e, successivamente, i file collegati negli storage gestiti dal Responsabile, con verifica dell'avvenuta rimozione; l'accesso all'account è eliminato per ultimo. Nessuna cancellazione avviene se l'esportazione, il download o la conferma di ricezione non sono completati.

13.3 Restano conservati i dati la cui conservazione è richiesta dalla legge e le copie presenti nei backup dell'infrastruttura fino alla loro scadenza secondo la relativa configurazione. Il Responsabile **non dichiara** una cancellazione istantanea e integrale da ogni backup o da ogni sistema di terzi.

13.4 In presenza di un obbligo giuridico, di un contenzioso o di una richiesta dell'autorità che richieda la conservazione, la cancellazione può essere sospesa limitatamente alle categorie di dati interessate; gli altri dati seguono la disciplina ordinaria.

ARTICOLO 14 — AUDIT (ART. 28.3.h GDPR)

14.1 Il Titolare ha diritto di ottenere, con richiesta scritta e preavviso ragionevole, le informazioni e la documentazione necessarie a dimostrare il rispetto degli obblighi del presente Accordo, anche mediante questionari, evidenze documentali e descrizione delle misure adottate.

14.2 Ispezioni presso il Responsabile o audit condotti da un revisore indipendente sono ammessi quando giustificati, secondo modalità concordate e proporzionate, di norma non più di una volta per anno civile, salvo violazioni accertate o richiesta dell'Autorità di controllo.

14.3 Le attività di audit si svolgono nel rispetto della riservatezza, della sicurezza dei sistemi e dei diritti di terzi, senza pregiudizio per la continuità del servizio.

ARTICOLO 15 — TRASFERIMENTI VERSO PAESI TERZI (ARTT. 44 SS. GDPR)

15.1 Le Parti riconoscono che alcuni trattamenti necessari all'erogazione del servizio possono comportare trasferimenti di Dati Personali verso paesi terzi: il presente Accordo non dichiara che tutti i trattamenti avvengano esclusivamente all'interno dell'Unione europea.

15.2 I trasferimenti, i fornitori coinvolti, i meccanismi applicabili e le eventuali misure supplementari sono indicati nell'**Allegato F**.

15.3 Il Responsabile riesamina periodicamente le garanzie applicabili, incluse le Clausole Contrattuali Standard (SCC) adottate con Decisione di esecuzione (UE) 2021/914, e informa il Titolare delle variazioni rilevanti.

ARTICOLO 16 — OBBLIGHI DEL TITOLARE

Il Titolare:

• determina finalità e mezzi del trattamento dei dati dei propri pazienti;

• dispone di una base giuridica idonea, incluse le condizioni dell'art. 9 GDPR per i dati relativi alla salute;

• fornisce agli interessati l'informativa prevista dagli artt. 13-14 GDPR;

• utilizza la Piattaforma nel rispetto della normativa applicabile e delle regole deontologiche;

• fornisce istruzioni lecite e verifica le configurazioni rilevanti del servizio;
• decide se firmare il referto e a quale destinatario trasmetterlo;
• risponde delle proprie decisioni cliniche e del contenuto del documento che sottoscrive.

Quanto sopra non esonera il Responsabile dagli obblighi che il GDPR pone direttamente in capo al responsabile del trattamento.

ARTICOLO 17 — RESPONSABILITÀ

17.1 Ciascuna Parte risponde secondo l'art. 82 GDPR e la disciplina applicabile. Il Responsabile risponde dei danni causati dal trattamento se non ha adempiuto agli obblighi del GDPR specificamente diretti ai responsabili o se ha agito in modo difforme rispetto alle istruzioni legittime del Titolare.

17.2 Le limitazioni di responsabilità previste dai Termini di Servizio si applicano nei limiti massimi consentiti dalla legge e non limitano gli obblighi inderogabili del GDPR.

ARTICOLO 18 — DISPOSIZIONI FINALI

18.1 Le modifiche al presente Accordo sono concordate per iscritto; gli aggiornamenti dell'Allegato D seguono la procedura dell'Articolo 8.3.

18.2 In caso di contrasto, il presente Accordo prevale sui Termini di Servizio limitatamente al trattamento dei Dati Personali effettuato per conto del Titolare.

18.3 **Legge applicabile:** legge italiana. Foro esclusivo di Milano.

18.4 La presente versione sostituisce le precedenti versioni del DPA a decorrere dalla data di efficacia. Le versioni precedenti sono conservate come versioni storiche ai fini di audit.

18.5 **Contatti:** Giorgio Arghittu (Refertius) — privacy@refertius.com — PEC giorgio@pec.refertius.com.

ALLEGATO A — DESCRIZIONE DEL TRATTAMENTO

A.1 Natura e operazioni di trattamento

• registrazione della visita, quando la funzione è utilizzata dal medico;
• trascrizione dell'audio;
• strutturazione delle informazioni cliniche;
• generazione del referto;
• controlli automatici sul contenuto del documento;
• revisione e modifica da parte del medico;
• firma del documento;
• conservazione del documento secondo le funzionalità del servizio;
• esportazione del documento;
• invio del referto al destinatario indicato dal medico, su iniziativa del medico;
• cancellazione dei dati;
• teleconsulto e televisita: raccolta da remoto delle risposte del paziente tramite QR personale, trascrizione e sintesi per il medico, videochiamata in tempo reale senza registrazione.

A.2 Finalità

• erogazione del servizio;
• trascrizione;
• elaborazione e strutturazione della documentazione clinica;
• generazione del referto;
• verifica e controllo del documento;
• archiviazione secondo le funzionalità del servizio;
• sicurezza e prevenzione degli abusi;
• supporto tecnico;
• invio del referto al destinatario su istruzione del medico;
• adempimento di obblighi di legge, quando applicabile.

ALLEGATO B — CATEGORIE DI INTERESSATI E DI DATI

B.1 Categorie di interessati

- pazienti del Titolare;
- medico/professionista utente della Piattaforma;
- personale autorizzato della struttura cliente;
- destinatari del referto indicati dal medico;
- soggetti eventualmente menzionati nella documentazione clinica.

B.2 Categorie di dati

- **Dati identificativi:** nome, cognome, identificativi del paziente, codice fiscale quando trattato, dati di contatto, email, telefono quando previsto;
- **Categorie particolari — dati relativi alla salute (art. 9 GDPR):**anamnesi, sintomi, segni e reperti, diagnosi, esami e risultati, terapie e farmaci, referti, altre informazioni cliniche, trascrizioni della visita, registrazioni audio della visita quando utilizzate;
- **Dati tecnici:** account, autenticazione, log tecnici minimizzati, identificativi tecnici, dati necessari al funzionamento e alla sicurezza;
- **Dati di audit:** eventi di sicurezza, eventi relativi a operazioni rilevanti sul documento, timestamp, identificativi tecnici.
- **Teleconsulto e televisita:** data di nascita, email e cellulare del paziente; risposte vocali e scritte con trascrizione e sintesi; dati tecnici di connessione alla videochiamata. Interessati: i pazienti che rispondono al teleconsulto o partecipano alla televisita.

Precisazione. Il Responsabile non dichiara di trattare esclusivamente dati pseudonimizzati. La schermatura dell'identità riguarda i soli flussi EXTERNAL_AI_PROCESSING; all'interno dell'ambiente Refertius e nel flusso di consegna del referto al destinatario i dati identificativi sono trattati direttamente.

ALLEGATO C — MISURE TECNICHE E ORGANIZZATIVE

C.1 Misure implementate

• autenticazione degli utenti e controllo degli accessi;
• isolamento dei dati tra utenti mediante Row Level Security a livello di database;
• verifica lato server della titolarità delle risorse prima delle operazioni sensibili, incluso l'invio del referto, con esito fail-closed;
• cifratura in transito (TLS) verso l'applicazione e verso i fornitori;
• cifratura a riposo di database e storage secondo la configurazione del provider di infrastruttura;
• storage dei file non pubblico, con accesso mediato dall'autorizzazione applicativa;
• minimizzazione dei dati trasmessi ai fornitori esterni;
• schermatura dell'identità del paziente nei flussi EXTERNAL_AI_PROCESSING;
• comportamento fail-closed dei controlli di protezione dei dati: se il controllo non è superato, l'operazione non prosegue;
• logging tecnico minimizzato secondo allow-list: nessun contenuto clinico, nome, codice fiscale o email del paziente nei log tecnici;
• registro di audit degli eventi rilevanti, inclusi gli invii di referto, con soli dati tecnici;
• procedure di cancellazione dei dati, comprese le rimozioni dei file collegati;
• cancellazione automatica delle registrazioni audio secondo l'Allegato E;
• gestione degli incidenti di sicurezza e notifica al Titolare;
• backup dell'infrastruttura gestiti dal provider secondo la configurazione documentata;
• verifiche automatiche periodiche delle invarianti di sicurezza e privacy nel processo di sviluppo.

C.2 Misure e qualifiche non dichiarate

Il Responsabile non dichiara: certificazioni ISO 27001, SOC 2 o HDS; cifratura end-to-end; qualifiche di tipo "zero trust" o "sicurezza assoluta"; assenza totale di retention; impossibilità assoluta di accesso umano. Le certificazioni eventualmente possedute dai fornitori restano attribuite ai fornitori stessi e non costituiscono certificazioni di Refertius.

ALLEGATO D — ELENCO DEI SUB-RESPONSABILI E DEI FORNITORI

Per ciascun sub-responsabile è indicato l'accordo sul trattamento dei dati (art. 28 GDPR) in vigore. I fornitori che non ricevono dati dei pazienti sono elencati per trasparenza.

Soggetto	Funzione	Categorie di dati	Localizzazione	Base / garanzie	Classificazione	Due diligence
Supabase, Inc.	Hosting applicativo, database, storage, autenticazione	Identificativi, dati relativi alla salute, tecnici, audit	Progetto in UE (AWS eu-west-3, Parigi); società con sede USA	DPA firmato il 30/03/2026; SCC	Sub-responsabile	**DPA firmato** — backup gestiti da Supabase nel progetto Refertius; PITR non attivo
Deepgram, Inc.	Trascrizione dell'audio delle visite e delle risposte del teleconsulto	Audio della visita e testo trascritto	USA	DPA firmato (Deepgram 31/07/2026, Refertius 04/08/2026); SCC. Con il parametro mip_opt_out=true audio e trascrizioni non sono scritti su storage persistente né usati per il miglioramento dei modelli	Sub-responsabile	**DPA firmato**
Anthropic, PBC	Elaborazione del testo del referto	Testo clinico	USA	DPA incorporato nei Commercial Terms, versione 24/02/2025; SCC	Sub-responsabile	**DPA in vigore**
OpenAI Ireland Ltd	Trascrizione di riserva, elaborazione del testo e sintesi del teleconsulto	Testo clinico; audio nella trascrizione di riserva	UE / USA	DPA firmato il 29/08/2026; SCC	Sub-responsabile	**DPA firmato**
Resend, Inc.	Email al paziente con link sicuro valido 45 giorni e verifica data di nascita, senza PDF allegato; copia al medico con allegato	Indirizzo del destinatario e link neutro; PDF clinico completo solo nella copia al medico	USA	DPA incorporato nei termini, versione 31/12/2025; SCC ed EU-US Data Privacy Framework	Sub-responsabile	**DPA in vigore**
Google (Gemini)	Lettura di carta intestata, logo e firma caricati dal medico; non riceve dati dei pazienti	Immagini caricate dal medico (carta intestata, logo, firma)	USA	Termini del fornitore	Fornitore tecnico — nessun dato dei pazienti	Non riceve dati dei pazienti
Sentry	Monitoraggio degli errori tecnici del browser, configurato per non ricevere contenuti clinici	Dati tecnici e diagnostici	USA	Termini del fornitore	Fornitore tecnico — nessun dato dei pazienti	Non riceve contenuti clinici
Stripe	Pagamenti del medico; non riceve dati dei pazienti	Dati di account e di pagamento del medico	UE / USA	Termini e garanzie del fornitore	Titolare autonomo per i propri trattamenti di pagamento — non sub-responsabile del trattamento clinico	Non riceve dati dei pazienti
Google (Analytics / Ads)	Misurazione e marketing del solo sito pubblico	Dati di navigazione del sito; nessun dato clinico e nessun dato del paziente	UE / USA	Termini del fornitore	Non rientra nel presente Accordo: trattamento del sito pubblico svolto da Refertius come titolare autonomo	Non riceve dati dei pazienti
Lovable (piattaforma di hosting) su infrastruttura Cloudflare	Rete, CDN e hosting del sito e delle funzioni server; inclusi dati in transito	Dati tecnici di navigazione e dati in transito	Rete edge globale	Termini del fornitore	Fornitore tecnico (hosting)	Catena contrattuale tramite Lovable e garanzie sui trasferimenti da verificare

Soggetto	Funzione	Categorie di dati	Localizzazione	Base / garanzie	Classificazione	Due diligence
Daily (Daily.co, Inc.)	Videochiamata della televisita	Audio e video in tempo reale, non registrati; dati tecnici di connessione (identificativi non nominativi di stanza e partecipante, indirizzo IP, orari, statistiche di rete)	Audio/video: Francoforte, riserva Londra (Regno Unito); dati tecnici: USA	DPA art. 28 con SCC Modulo 3 firmato il 30/10/2026; EU-US Data Privacy Framework	Sub-responsabile	Nessuna registrazione né trascrizione salvata; dati tecnici conservati 3 giorni

Televisita con Daily: media cifrati DTLS-SRTP, segnalazione e API protette da TLS; il link di accesso alla videochiamata vale 60 minuti. Il presente allegato è aggiornato secondo la procedura dell’Articolo 8.3.

ALLEGATO E — CONSERVAZIONE E CANCELLAZIONE

Categoria	Conservazione
Registrazioni audio della visita	Audio visite: Eliminazione entro 24 ore dalla creazione. Audio risposte teleconsulto: entro 7 giorni dalla firma del referto e, in ogni caso, entro 30 giorni dalla chiusura del teleconsulto; coda e cancellazione Storage periodica.
Trascrizioni e testi intermedi di elaborazione	Trascrizione e sintesi del teleconsulto restano nell’archivio del medico secondo le sue istruzioni; nessun TTL autonomo qui configurato. Copie consegna: link 45 giorni, revoca o scadenza avvia la rimozione periodica dei file.
Referti e documentazione clinica	Per la durata dell'account, salvo cancellazione richiesta dal Titolare; la conservazione a fini clinico-legali è determinata dal Titolare
Pacchetti di esportazione	Pacchetto pronto: 7 giorni (poi cancellato); codici di download: 10 minuti; in chiusura account il pacchetto è cancellato dopo la conferma di ricezione. Eventi e ricevute di esportazione: 5 anni (solo metadati)
Dati di account e fatturazione	Per la durata del rapporto e secondo gli obblighi fiscali applicabili
Log tecnici	Log di sicurezza: 12 mesi, poi cancellati dal job giornaliero di retention (policy interna Refertius); minimizzati, senza contenuto clinico né identificativi del paziente
Registro di audit	5 anni, poi cancellati dal job giornaliero di retention (policy interna Refertius), salvo legal hold attivo sull'utente
Backup dell'infrastruttura	Backup fisici giornalieri gestiti da Supabase (retention del provider secondo il piano del progetto); PITR non attivo; file Storage esclusi dai backup del database
Dati conservati dai sub-responsabili	Secondo i rispettivi accordi sul trattamento dei dati (Allegato D); Deepgram non conserva audio né trascrizioni

La cancellazione avviene su istruzione del Titolare tramite le funzionalità del servizio, inclusa la procedura di cancellazione dell'account, nei limiti indicati all'Articolo 13.

ALLEGATO F — TRASFERIMENTI VERSO PAESI TERZI

Trattamento	Fornitore	Paese	Meccanismo	Misure supplementari
Hosting, database, storage	Supabase	Progetto in UE (Parigi); società USA	SCC (DPA 30/03/2026)	Cifratura in transito e a riposo, controllo degli accessi
Trascrizione	Deepgram	USA	SCC (DPA 04/08/2026)	Nessuna conservazione persistente (mip_opt_out=true)

Trattamento	Fornitore	Paese	Meccanismo	Misure supplementari
Generazione e verifica del referto	Anthropic	USA	SCC (DPA 24/02/2025)	Minimizzazione del contenuto
Trascrizione di riserva, elaborazione del testo e sintesi del teleconsulto	OpenAI Ireland Ltd	UE / USA	SCC (DPA 29/08/2026)	Minimizzazione del contenuto
Consegna email del referto	Resend	USA	SCC ed EU-US Data Privacy Framework (DPA 31/12/2025)	Metadati neutri e link al paziente senza PDF; allegato solo nella copia al medico
Monitoraggio errori	Sentry	USA	Termini del fornitore	Configurato per non ricevere contenuti clinici
Televisita	Daily	Dati tecnici di connessione: USA. Audio/video: UE (Francoforte), riserva Regno Unito (Londra)	Dati tecnici: EU-US Data Privacy Framework e SCC Modulo 3 (DPA 30/10/2026). Audio/video nel Regno Unito: decisione di adeguatezza UE	Nessuna registrazione né trascrizione salvata; media cifrati DTLS-SRTP; dati tecnici conservati 3 giorni
Pagamenti	Stripe	UE / USA	Garanzie del fornitore	Nessun dato clinico trasmesso

Valutazione d'impatto sui trasferimenti: in fase di formalizzazione.

SOTTOSCRIZIONE

REFERTIUS (Responsabile)

Nome: _____

Qualifica: _____

Firma: _____

Data: _____

CLIENTE / TITOLARE

Ragione sociale: _____

Nome: _____

Qualifica: _____

Firma: _____

Data: _____

Il presente Accordo può essere accettato anche in forma elettronica in fase di sottoscrizione del servizio, quando tale modalità è resa disponibile dalla Piattaforma; l'accettazione è registrata con identificativo dell'utente, data e ora e versione del documento.

© 2026 Giorgio Arghittu (Refertius) - P.IVA 14678340960