INNOVAMED — DOCUMENTO LEGALE

GLDA — GESTIONI LAVORI DATI APPALTI S.R.L. · C.F./P.IVA 14385190963

Data Processing Agreement (Master) — InnovaMed

Versione 1.0 · 10 aprile 2026

Soggetto giuridico	GLDA — GESTIONI LAVORI DATI APPALTI S.R.L.
Sede legale	Via della Resistenza 56, 20090 Buccinasco (MI), Italia
C.F. / P.IVA	14385190963
REA	MI - 2779148
PEC	glda@legalmail.it
Contatto privacy	privacy@innovaflow.it
Legale rappresentante	D'ALESSANDRO Giuseppe, Amministratore Unico
Versione documento	1.0
Data di emissione	10 aprile 2026
Hash SHA-256 sorgente	1884aaecb131857b48aa732511b59069c4962cb678d26dfa11de70a0720e5984

Documento da firmare digitalmente da Giuseppe D'Alessandro

Il presente PDF e auto-generato dal sorgente markdown e rappresenta la versione definitiva pronta per firma digitale CAdES o PAdES qualificata. La riga hash SHA-256 soprastante identifica univocamente il testo sorgente a fini di audit GDPR e rende verificabile l'integrita del documento stampato. Eventuali modifiche al sorgente dopo la firma richiedono una nuova versione (es. v1.1) con nuovo hash e nuova firma.

Accordo sul Trattamento dei Dati Personali (DPA) — Master

ai sensi dell'art. 28 del Regolamento (UE) 2016/679 (GDPR)

Servizio: InnovaMed (`https://med.innovaflow.it`) **Versione del modello:** 1.0 **Data di emissione:** 10 aprile 2026 **Base di riferimento:** Allegato C del Codice di Condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale, approvato dal Garante per la protezione dei dati personali con Provvedimento n. 498/2024 del 17 ottobre 2024.

> ***Modalita di sottoscrizione.*** *Il presente DPA e un* ***modello pre-firmato*** *dal legale rappresentante di GLDA SRL una sola volta, in data 10 aprile 2026. Ciascun Titolare cliente lo accetta integralmente al momento dell'attivazione del proprio studio sulla piattaforma InnovaMed mediante meccanismo di* ***accettazione elettronica click-wrap****, le cui evidenze (versione del documento, data, hash SHA-256 del testo accettato, indirizzo IP di origine, user agent) sono conservate da GLDA SRL ai sensi del successivo art. 17 e costituiscono prova legale dell'accordo ex artt. 20-22 del Reg. (UE) 910/2014 (eIDAS) e art. 2702 c.c. La firma autografa rimane disponibile, su richiesta del Titolare, in modalita off-line in copia controfirmata.*

TRA

GLDA - GESTIONI LAVORI DATI APPALTI S.R.L. (in forma abbreviata "GLDA S.r.l.") Sede legale: Via della Resistenza 56, 20090 Buccinasco (MI), Italia Codice Fiscale e Partita IVA: 14385190963 Numero REA: MI - 2779148 (Camera di Commercio Milano Monza Brianza Lodi) Capitale sociale: € 1.000,00 i.v. PEC: glda@legalmail.it Email punto di contatto privacy: privacy@innovaflow.it In persona del legale rappresentante pro tempore **D'ALESSANDRO Giuseppe**, Amministratore Unico, nato a Napoli il 3 dicembre 1969, codice fiscale DLSGPP69T03F839R

di seguito denominata **"GLDA"** o **"Responsabile del trattamento"**

E

[RAGIONE SOCIALE DELLO STUDIO MEDICO / NOME E COGNOME DEL PROFESSIONISTA SANITARIO] Sede / Studio: [VIA, CAP, CITTA], Italia C.F. / P.IVA: [CODICE FISCALE / PARTITA IVA] Iscrizione all'Ordine dei Medici Chirurghi e degli Odontoiatri (o altro Ordine professionale competente) di [PROVINCIA], n. [NUMERO ISCRIZIONE] PEC: [INDIRIZZO PEC] Email: [INDIRIZZO EMAIL] In persona del legale rappresentante / titolare pro tempore [NOME COGNOME]

di seguito denominato **"il Titolare"** o **"Titolare del trattamento"**

(GLDA e il Titolare sono congiuntamente denominate le **"Parti"** e singolarmente la **"Parte"**)

PREMESSO CHE

(A) Il Titolare esercita l'attivita di professionista sanitario in regime privato libero-professionale e, ai sensi dell'art. 9, par. 2, lett. h) del Regolamento (UE) 2016/679 (di seguito, "**GDPR**"), tratta dati personali comuni e dati relativi alla salute dei propri pazienti per finalita di prevenzione, diagnosi, cura e assistenza sanitaria, in qualita di Titolare del trattamento;

(B) GLDA e una societa che ha sviluppato e commercializza il servizio **InnovaMed**, una piattaforma software-as-a-service (SaaS) destinata agli studi medici privati libero-professionali italiani, che fornisce funzionalita di gestione dell'agenda degli appuntamenti, anagrafica pazienti, archiviazione di documentazione sanitaria operativa, generazione di bozze di refertazione, comunicazione organizzativa verso i pazienti tramite WhatsApp Business Cloud API ed email, nonche un chatbot conversazionale basato su modelli di intelligenza artificiale per la gestione automatizzata delle richieste di prenotazione, modifica e cancellazione degli appuntamenti;

(C) Le Parti hanno sottoscritto, o sono in procinto di sottoscrivere, un contratto di fornitura del servizio InnovaMed (di seguito, il "**Contratto Principale**"), avente ad oggetto l'erogazione del Servizio come descritto al punto (B) che precede;

(D) L'erogazione del Servizio comporta il trattamento, da parte di GLDA per conto del Titolare, di dati personali comuni e di categorie particolari di dati ai sensi dell'art. 9 GDPR, con particolare riferimento a dati relativi alla salute dei pazienti del Titolare;

(E) Il Garante per la protezione dei dati personali, con il "Compendio sul trattamento dei dati personali attraverso piattaforme volte a mettere in contatto i pazienti con i professionisti sanitari accessibili via web e app" pubblicato in data 28 marzo 2024 (di seguito, il "**Compendio Garante 28/03/2024**"), ha espressamente stabilito che, per i trattamenti di tipo tecnico-amministrativo quali la gestione dell'agenda degli appuntamenti e l'archiviazione della documentazione medica, il gestore della piattaforma debba essere designato Responsabile del trattamento dal professionista sanitario operante in qualita di Titolare;

(F) Il medesimo Compendio Garante 28/03/2024 ha inoltre stabilito che i proprietari e i gestori delle piattaforme **non sono abilitati a trattare dati sanitari per finalita di diagnosi, assistenza e terapia**, riservate esclusivamente ai professionisti sanitari abilitati;

(G) Il Garante per la protezione dei dati personali, con Provvedimento n. 498/2024 del 17 ottobre 2024, ha approvato il **Codice di Condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale**, il cui Allegato C contiene uno schema di accordo ex art. 28 GDPR avente natura di modello esemplificativo approvato dall'Autorita di controllo;

(H) Il presente DPA e redatto in conformita all'art. 28 GDPR, al Codice in materia di protezione dei dati personali (D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018), al Compendio Garante 28/03/2024 e allo schema di cui all'Allegato C del Codice di Condotta sopra citato;

(I) Le Parti intendono pertanto disciplinare con il presente DPA i termini e le condizioni del trattamento dei dati personali eseguito da GLDA per conto del Titolare, in conformita alla normativa applicabile in materia di protezione dei dati personali.

Tutto cio premesso, le Parti convengono e stipulano quanto segue.

ART. 1 — QUALIFICAZIONE DEI RUOLI

1.1 Le Parti riconoscono espressamente che **GLDA SRL opera, rispetto ai trattamenti di dati personali dei pazienti del Titolare, in qualita esclusiva di Responsabile del trattamento ex art. 28 GDPR**, conformemente al Compendio Garante 28/03/2024, che testualmente stabilisce, per i trattamenti di tipo tecnico-amministrativo (gestione dell'agenda degli appuntamenti e archiviazione della documentazione medica), la designazione del gestore della piattaforma quale Responsabile del trattamento da parte del professionista sanitario (Titolare).

1.2 **Divieto assoluto di trattamento clinico.** GLDA non effettua alcun trattamento di dati sanitari dei pazienti per finalita di diagnosi, assistenza o terapia, che restano riservate esclusivamente al professionista sanitario Titolare.

1.3 **Doppia veste di GLDA.** Le Parti riconoscono che GLDA opera simultaneamente in due distinte qualita, tra loro nettamente separate:

(a) **Responsabile del trattamento ex art. 28 GDPR** — per tutti i dati personali dei pazienti del Titolare trattati nell'ambito del Servizio InnovaMed, ivi inclusi dati anagrafici, dati di contatto, dati relativi alla salute, bozze di referto, note operative, conversazioni con il chatbot, parametri vitali, allergie, farmaci, anamnesi ed ogni altro dato inserito dal Titolare o dal suo staff nella piattaforma. Il presente DPA disciplina integralmente tali trattamenti;

(b) **Titolare autonomo del trattamento** — per i dati del rapporto contrattuale B2B con il Titolare, ivi inclusi dati anagrafici del Titolare persona fisica e dei suoi collaboratori con account (utenti dello studio), dati di autenticazione, dati di fatturazione, log tecnici applicativi (privi di contenuti clinici dei pazienti), metadati di sistema, preferenze di configurazione della piattaforma. Tali trattamenti sono retti da un'autonoma Informativa privacy ex art. 13 GDPR resa da GLDA al Titolare e non formano oggetto del presente DPA.

1.4 Il Titolare mantiene la piena responsabilita delle finalita e dei mezzi essenziali del trattamento dei dati dei propri pazienti, quali determinati dalla legge e dal rapporto professionale con il paziente. GLDA si limita a fornire i mezzi tecnici non essenziali (piattaforma software, infrastruttura cloud, modelli di intelligenza artificiale, canali di comunicazione) ai sensi delle Linee Guida EDPB 07/2020 sui concetti di Titolare e Responsabile del trattamento.

ART. 2 — DEFINIZIONI

2.1 **"GDPR"**: il Regolamento (UE) 2016/679 del 27 aprile 2016.

2.2 **"Codice Privacy"**: il D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018.

2.3 **"Titolare del trattamento"**: il Titolare come identificato in epigrafe, ai sensi dell'art. 4, n. 7, GDPR.

2.4 **"Responsabile del trattamento"**: GLDA SRL, ai sensi dell'art. 4, n. 8, GDPR.

2.5 **"Interessato"**: la persona fisica cui si riferiscono i dati personali oggetto di trattamento, ai sensi dell'art. 4, n. 1, GDPR. Ai fini del presente DPA, gli Interessati sono principalmente i pazienti del Titolare, eventuali familiari/conviventi delegati alla prenotazione e gli utenti dello studio limitatamente ai dati operativi.

2.6 **"Dato personale"**: qualsiasi informazione riguardante una persona fisica identificata o identificabile.

2.7 **"Categorie particolari di dati"**: i dati di cui all'art. 9, par. 1, GDPR, con particolare riferimento ai dati relativi alla salute (art. 4, n. 15, GDPR).

2.8 **"Trattamento"**: qualsiasi operazione applicata a dati personali ai sensi dell'art. 4, n. 2, GDPR.

2.9 **"Violazione dei dati personali"** o **"Data Breach"**: l'evento ai sensi dell'art. 4, n. 12, GDPR.

2.10 **"Sub-responsabile"**: il soggetto terzo nominato da GLDA ai sensi dell'art. 28, par. 2 e 4, GDPR, il cui elenco aggiornato e riportato nell'**Allegato I**.

2.11 **"Istruzioni documentate"**: le istruzioni del Titolare a GLDA ai sensi dell'art. 28, par. 3, lett. a), GDPR, costituite dal presente DPA, dal Contratto Principale e dall'Allegato III.

2.12 **"Servizio"** o **"InnovaMed"**: la piattaforma SaaS fornita da GLDA al Titolare in forza del Contratto Principale.

2.13 **"DPF"**: il Data Privacy Framework UE-USA, adottato con Decisione di esecuzione (UE) 2023/1795 del 10 luglio 2023.

2.14 **"SCC"**: le Clausole Contrattuali Tipo adottate con Decisione di esecuzione (UE) 2021/914 del 4 giugno 2021.

2.15 **"TIA"**: Transfer Impact Assessment ai sensi della sentenza CGUE C-311/18 (Schrems II) e delle Raccomandazioni EDPB 01/2020.

ART. 3 — OGGETTO, DURATA, NATURA E FINALITA DEL TRATTAMENTO

3.1 **Oggetto.** Oggetto del presente DPA e il trattamento dei dati personali che GLDA eseguira, in qualita di Responsabile del trattamento, per conto del Titolare nell'ambito dell'erogazione del Servizio InnovaMed.

3.2 **Durata.** Il presente DPA entra in vigore alla data di accettazione click-wrap da parte del Titolare e rimane efficace per tutta la durata del Contratto Principale, fatti salvi gli obblighi che, per loro natura, sopravvivono alla cessazione del medesimo.

3.3 **Natura del trattamento.** Il trattamento eseguito da GLDA ha natura automatizzata, mediante strumenti elettronici, e consiste in operazioni di raccolta, registrazione, strutturazione, conservazione, estrazione, consultazione, uso, comunicazione mediante trasmissione, interconnessione limitata alla perimetrazione di studio, cancellazione e distruzione dei dati personali. Le operazioni sono eseguite esclusivamente su istruzione documentata del Titolare.

3.4 **Finalita del trattamento.** Il trattamento e finalizzato esclusivamente a fornire al Titolare il Servizio InnovaMed, con riferimento a:

(a) **Gestione dell'agenda degli appuntamenti**: creazione, modifica, conferma, cancellazione e visualizzazione degli appuntamenti, con invio automatizzato di reminder organizzativi;

(b) **Anagrafica pazienti**: archiviazione e gestione dei dati anagrafici, di contatto, dei consensi informati e delle preferenze di comunicazione;

(c) **Archiviazione della documentazione sanitaria operativa**: storage di bozze di referti, note operative, parametri vitali, allergie, farmaci, anamnesi, documenti caricati dal Titolare o dal suo staff, **senza alcuna elaborazione clinica automatizzata** ne supporto decisionale diagnostico-terapeutico;

(d) **Generazione di bozze di refertazione**: produzione di bozze di documenti clinici su template personalizzabili, prive di valore legale probatorio autonomo e destinate ad essere firmate digitalmente e conservate a norma dal Titolare con strumenti esterni di sua scelta;

(e) **Chatbot conversazionale WhatsApp**: risposta automatizzata alle richieste organizzative dei pazienti del Titolare in materia di prenotazione, modifica, cancellazione e informazioni sugli appuntamenti, mediante elaborazione in tempo reale dei messaggi con modelli di intelligenza artificiale generativa (Google Gemini via Vertex AI), con output puramente organizzativo e mai clinico;

(f) **Comunicazioni organizzative verso i pazienti**: invio di reminder, conferme, inviti alla registrazione e messaggi di servizio via WhatsApp Business Cloud API ed email, limitatamente a dati anagrafici neutri e metadati di appuntamento;

(g) **Inbox conversazioni**: visualizzazione cronologica delle conversazioni con possibilita di takeover manuale da parte del Titolare;

(h) **Gestione utenti dello studio**: amministrazione degli account del personale del Titolare con sistema di permessi granulare;

(i) **Audit logging e tracciabilita**: registrazione degli accessi e delle operazioni eseguite nella piattaforma ai fini della sicurezza, conformemente ai provvedimenti del Garante in materia di amministratori di sistema e di dossier sanitario.

3.5 Le finalita sopra elencate sono **tassative ed esaustive**. Qualsiasi trattamento ulteriore o diverso richiederebbe un'istruzione documentata specifica del Titolare e, ove non supportato da una base giuridica autonoma riconducibile al Titolare medesimo, sarebbe illecito e risolverebbe immediatamente il presente DPA ai sensi dell'art. 28, par. 10, GDPR.

ART. 4 — TIPI DI DATI PERSONALI E CATEGORIE DI INTERESSATI

4.1 **Categorie di interessati.**

(a) Pazienti del Titolare;

(b) Familiari, conviventi o altri soggetti delegati dai pazienti alla prenotazione;

(c) Utenti dello studio (staff, dottori associati al Titolare) limitatamente ai dati di profilo e di utilizzo della piattaforma;

(d) Terzi menzionati nei dati clinici (ad esempio familiari nell'anamnesi), trattati come testo libero inserito dal Titolare sotto la sua esclusiva responsabilita.

4.2 **Categorie di dati personali comuni:**

(a) dati anagrafici (nome, cognome, data di nascita, luogo di nascita, codice fiscale, sesso);

(b) dati di contatto (numero di telefono WhatsApp, indirizzo email, indirizzo fisico);

(c) dati relativi all'appuntamento (data, ora, tipo visita, dottore, durata, stato);

(d) dati di autenticazione e di sessione (solo per utenti dello studio);

(e) metadati di comunicazione WhatsApp (ID messaggio, timestamp, stato consegna);

(f) contenuto delle conversazioni WhatsApp tra paziente e chatbot/operatore;

(g) log di accesso e di utilizzo della piattaforma.

4.3 **Categorie particolari di dati ex art. 9 GDPR.** Per i pazienti e per i soggetti menzionati nell'anamnesi, sono trattati dati relativi alla salute inseriti manualmente dal Titolare o dal suo staff: allergie e intolleranze; farmaci in uso; anamnesi personale e familiare (testo libero); parametri vitali; note cliniche operative; bozze di referti; tipo di visita e specializzazione medica.

4.4 **Dati non trattati.** GLDA non tratta, per conto del Titolare, dati giudiziari, dati biometrici identificativi, dati genetici, dati relativi a vita sessuale o orientamento sessuale, salvo il caso in cui tali informazioni siano inserite liberamente dal Titolare nei campi di testo libero della piattaforma sotto la propria esclusiva responsabilita.

4.5 **Minimizzazione.** GLDA si impegna a trattare esclusivamente i dati strettamente necessari all'erogazione del Servizio. I messaggi WhatsApp verso i pazienti contengono solo dati anagrafici neutri e metadati di appuntamento, mentre i dettagli sanitari sensibili sono accessibili esclusivamente tramite link protetti al portale web dello studio.

ART. 5 — OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO (ART. 28, PAR. 3, GDPR)

5.1 Istruzioni documentate e divieto di finalita proprie (art. 28, par. 3, lett. a)

5.1.1 GLDA trattera i dati personali del Titolare esclusivamente sulla base di istruzioni documentate del Titolare medesimo, comprese quelle relative al trasferimento di dati personali verso un Paese terzo, salvo che lo richieda il diritto dell'Unione o degli Stati membri cui GLDA e soggetta; in tal caso, GLDA informera il Titolare prima del trattamento, salvo divieto di legge per rilevanti motivi di interesse pubblico.

5.1.2 Le istruzioni documentate iniziali sono costituite dal presente DPA, dal Contratto Principale, dall'Allegato III e da ogni successiva istruzione scritta del Titolare impartita a mezzo email a `privacy@innovaflow.it`, PEC `glda@legalmail.it` o strumenti equivalenti che ne garantiscano la tracciabilita.

5.1.3 **Clausola "no finalita proprie".** Il Titolare da istruzione a GLDA di trattare i dati personali dei pazienti **esclusivamente** per le finalita strettamente necessarie a fornire il Servizio descritto nell'art. 3 del presente DPA. **GLDA SI IMPEGNA ESPRESSAMENTE a NON utilizzare i dati per finalita proprie**, ivi inclusi a titolo esemplificativo e non esaustivo:

(a) addestramento, fine-tuning, adattamento, valutazione o miglioramento di modelli di intelligenza artificiale, propri o di terzi;

(b) analisi statistica o benchmarking tra studi clienti (cross-tenant);

(c) costruzione di dataset di ricerca, epidemiologici, scientifici o commerciali;

(d) cessione, licenza, vendita o condivisione con terzi a qualsiasi titolo;

(e) profilazione, targeting o marketing verso il paziente o verso il medico;

(f) miglioramento del prodotto su dati reali di produzione contenenti dati personali;

(g) partecipazione a progetti di ricerca di qualsiasi natura che comportino il trattamento dei dati del Titolare;

(h) creazione di "base di conoscenza" o indici derivati a partire dai dati del Titolare.

5.1.4 Qualsiasi uso ulteriore richiederebbe autorizzazione scritta del Titolare e base giuridica autonoma. In sua assenza, tale trattamento costituirebbe violazione dell'art. 28 GDPR, riqualificherebbe GLDA come Titolare autonomo ai sensi dell'art. 28, par. 10, GDPR, risolverebbe immediatamente il presente DPA e il

Contratto Principale con applicazione delle penali ivi previste.

5.1.5 GLDA informera immediatamente il Titolare qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni applicabili.

5.2 Riservatezza del personale (art. 28, par. 3, lett. b)

5.2.1 GLDA garantisce che le persone autorizzate al trattamento dei dati personali per suo conto si siano impegnate alla riservatezza mediante sottoscrizione di specifici accordi di confidenzialita o siano soggette a un adeguato obbligo legale di segretezza.

5.2.2 L'accesso ai dati personali e limitato al personale di GLDA che ne abbia effettiva necessita per lo svolgimento delle proprie mansioni (need-to-know), previa nomina formale a "soggetto autorizzato al trattamento" ex art. 29 GDPR e art. 2-quaterdecies del Codice Privacy.

5.2.3 Il personale autorizzato riceve istruzioni operative in materia di protezione dei dati personali, sicurezza informatica, riconoscimento di tentativi di phishing e procedure di gestione dei data breach.

5.3 Misure di sicurezza (art. 28, par. 3, lett. c) e art. 32 GDPR)

5.3.1 GLDA adotta tutte le misure richieste dall'art. 32 GDPR, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalita del trattamento, nonche del rischio per i diritti e le liberta delle persone fisiche.

5.3.2 L'elenco sintetico delle misure tecniche e organizzative adottate e riportato nell'**Allegato II** al presente DPA. Il dettaglio operativo e contenuto nel **Security Datasheet** di InnovaMed, disponibile su richiesta scritta del Titolare.

5.3.3 GLDA si impegna a mantenere aggiornate le misure di sicurezza nel tempo, ad applicare i principi di "privacy by design" e "privacy by default" ex art. 25 GDPR, e a comunicare tempestivamente al Titolare ogni modifica sostanziale delle medesime.

5.4 Ricorso a Sub-responsabili (art. 28, par. 3, lett. d, e par. 2 e 4)

5.4.1 Il Titolare autorizza, con autorizzazione generale ai sensi dell'art. 28, par. 2, GDPR, GLDA a ricorrere ai sub-responsabili del trattamento elencati nell'**Allegato I** al presente DPA.

5.4.2 GLDA si impegna a informare preventivamente il Titolare di eventuali modifiche alla lista dei sub-responsabili (aggiunta o sostituzione), con un **preavviso minimo di 30 (trenta) giorni** rispetto all'efficacia della modifica, mediante pubblicazione della versione aggiornata dell'elenco all'indirizzo `https://med.innovaflow.it/trust/sub-processors` e/o comunicazione via email all'indirizzo di contatto indicato in epigrafe.

5.4.3 Entro il medesimo termine di 30 giorni dalla notifica, il Titolare puo opporsi per iscritto alle modifiche, fornendo motivazioni ragionevoli basate su profili di protezione dei dati. In caso di opposizione motivata, le Parti si impegnano a ricercare in buona fede una soluzione alternativa; ove entro

30 giorni ulteriori non sia possibile raggiungere un accordo, il Titolare avra diritto a risolvere il Contratto Principale senza penali, con preavviso di 30 giorni. Il mancato esercizio del diritto di opposizione entro il termine equivale ad approvazione tacita.

5.4.4 GLDA si impegna a vincolare ciascun sub-responsabile, mediante contratto scritto, ai medesimi obblighi di protezione dei dati stabiliti nel presente DPA, e in particolare a fornire garanzie sufficienti di adozione di misure tecniche e organizzative adeguate ai sensi dell'art. 28 GDPR.

5.4.5 GLDA mantiene piena responsabilita nei confronti del Titolare per l'adempimento degli obblighi dei propri sub-responsabili, conformemente all'art. 28, par. 4, GDPR.

5.5 Assistenza per l'esercizio dei diritti degli interessati (art. 28, par. 3, lett. e)

5.5.1 GLDA assiste il Titolare con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti degli interessati di cui agli artt. 15-22 GDPR.

5.5.2 GLDA mette a disposizione del Titolare, attraverso la piattaforma InnovaMed, funzionalita per:

(a) estrarre in formato strutturato (JSON/CSV) i dati personali di un determinato interessato (artt. 15 e 20 GDPR);

(b) rettificare o integrare i dati anagrafici e clinici di un interessato (art. 16 GDPR);

(c) cancellare i dati di un interessato nel rispetto degli obblighi di conservazione (art. 17 GDPR);

(d) limitare il trattamento mediante disattivazione dell'account paziente (art. 18 GDPR);

(e) opporsi al trattamento rispetto a specifiche finalita (art. 21 GDPR).

5.5.3 Qualora GLDA riceva direttamente una richiesta di esercizio dei diritti da parte di un interessato, la inoltrera senza indebito ritardo al Titolare, astenendosi dal rispondere direttamente all'interessato, salvo diversa istruzione del Titolare.

5.6 Assistenza per obblighi ex artt. 32-36 GDPR (art. 28, par. 3, lett. f)

5.6.1 GLDA assiste il Titolare nel garantire il rispetto degli obblighi di cui agli articoli 32-36 GDPR, in particolare:

(a) **Sicurezza del trattamento (art. 32)**: mediante le misure dell'Allegato II e la documentazione tecnica disponibile su richiesta;

(b) **Notifica di violazioni dei dati (art. 33)**: secondo le modalita e i tempi di cui all'art. 6 del presente DPA;

(c) **Comunicazione di violazioni agli interessati (art. 34)**: fornendo al Titolare tutte le informazioni necessarie per valutare il rischio e predisporre la comunicazione;

(d) **Valutazione d'impatto sulla protezione dei dati — DPIA (art. 35)**: mettendo a disposizione del Titolare gli elementi tecnici di prodotto utili alla redazione di una DPIA quando sia richiesta in ragione delle caratteristiche specifiche del Titolare. GLDA ricorda che, per il singolo studio medico libero professionale tipico, il Compendio Garante 28/03/2024 non impone in via generale la DPIA per il solo uso di una piattaforma SaaS gestionale;

(e) **Consultazione preventiva del Garante (art. 36)**: fornendo le informazioni tecniche necessarie qualora il Titolare debba consultare l'Autorita.

5.7 Cancellazione o restituzione dei dati a fine contratto (art. 28, par. 3, lett. g)

5.7.1 Si rinvia integralmente all'art. 7 del presente DPA.

5.8 Audit right del Titolare (art. 28, par. 3, lett. h)

5.8.1 Si rinvia integralmente all'art. 8 del presente DPA.

5.9 Registro delle attivita di trattamento (art. 30, par. 2, GDPR)

5.9.1 GLDA mantiene un Registro delle attivita di trattamento svolte per conto del Titolare conforme all'art. 30, par. 2, GDPR, che sara messo a disposizione del Titolare e/o dell'Autorita di controllo su richiesta.

5.10 Punto di contatto privacy

5.10.1 GLDA dichiara di **non avere designato un Responsabile della Protezione dei Dati (DPO)** ai sensi dell'art. 37 GDPR, in esito a valutazione scritta motivata redatta ai sensi del principio di accountability ex art. 5.2 GDPR e in conformita alle Linee Guida WP243 rev.01 dell'EDPB e alle FAQ Garante in materia. Tale valutazione (documento "Valutazione DPO scritta") e disponibile al Titolare su richiesta.

5.10.2 Il punto di contatto per le questioni privacy e l'indirizzo `privacy@innovaflow.it`, presidiato internamente dal Privacy Lead di GLDA (figura interna nominata ex art. 29 GDPR, non DPO).

ART. 6 — VIOLAZIONI DEI DATI PERSONALI (DATA BREACH)

6.1 **SLA di notifica.** GLDA, una volta venuta a conoscenza di una violazione dei dati personali relativa ai dati trattati per conto del Titolare, la notifichera al Titolare **senza ingiustificato ritardo e comunque entro 24 (ventiquattro) ore** dalla conferma del breach. Tale termine e volto a garantire al Titolare il tempo sufficiente per adempiere al proprio obbligo di notifica al Garante entro 72 ore ex art. 33 GDPR e alle finestre piu stringenti riconosciute dal Garante per il dossier sanitario (orientativamente 48 ore, cfr. Provv. Garante 331/2015).

6.2 **Contenuto della notifica.** La notifica di GLDA al Titolare conterra almeno le informazioni di cui all'art. 33, par. 3, GDPR, in particolare:

(a) la descrizione della natura della violazione, incluse le categorie e il numero approssimativo di interessati e di record interessati;

(b) il nome e i dati di contatto del punto di contatto privacy (`privacy@innovaflow.it`) presso cui ottenere ulteriori informazioni;

(c) la descrizione delle probabili conseguenze della violazione;

(d) la descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e attenuarne gli effetti negativi;

(e) la cronologia degli eventi (detection, triage, containment, mitigation);

(f) ogni ulteriore informazione utile al Titolare per la valutazione del rischio.

6.3 **Canale di notifica.** La notifica sara trasmessa via email all'indirizzo di contatto del Titolare indicato in epigrafe, con conferma di ricezione richiesta entro 4 ore dall'invio. In caso di indisponibilita del canale email, la notifica sara trasmessa via PEC.

6.4 **Collaborazione nella notifica al Garante e agli interessati.** GLDA fornira al Titolare, senza ulteriori costi, ogni ragionevole assistenza per la predisposizione della notifica al Garante ex art. 33 GDPR e dell'eventuale comunicazione agli interessati ex art. 34 GDPR, incluso un template pre-compilato al 90% delle informazioni tecniche gia in possesso di GLDA.

6.5 **Registro interno delle violazioni.** GLDA mantiene un registro interno delle violazioni conforme all'art. 33, par. 5, GDPR, accessibile al Titolare su richiesta motivata e al Garante su ordine.

6.6 **Procedura post-mortem.** Entro 7 (sette) giorni dalla notifica, GLDA trasmettera al Titolare un post-mortem contenente analisi delle cause, impatto effettivo, misure correttive adottate e piano di remediation.

6.7 **Procedura interna.** Le modalita operative di gestione data breach sono disciplinate dalla "Procedura interna data breach v1.0" di GLDA, disponibile al Titolare su richiesta.

ART. 7 — CANCELLAZIONE O RESTITUZIONE DEI DATI ALLA CESSAZIONE

7.1 Alla cessazione del Contratto Principale, qualunque ne sia la causa, GLDA, a scelta del Titolare da esercitarsi per iscritto entro 15 (quindici) giorni dalla cessazione:

(a) **restituisce** al Titolare tutti i dati personali trattati per suo conto in formato elettronico strutturato (JSON e/o CSV, con export dei documenti binari in formato nativo), messo a disposizione tramite download sicuro da area riservata;

(b) ovvero **cancella** tutti i dati personali trattati per conto del Titolare dai propri sistemi, ivi compresi i sistemi dei sub-responsabili.

7.2 **Silenzio del Titolare.** In caso di mancata indicazione della scelta entro il termine di cui al punto 7.1, GLDA procedera, trascorsi ulteriori 30 (trenta) giorni, alla cancellazione automatica di tutti i dati, previa ulteriore comunicazione di avviso al Titolare.

7.3 **Termine di cancellazione.** La cancellazione dei dati dai sistemi di produzione avverra **entro 30 giorni** dalla richiesta o dallo scadere del termine di cui al punto 7.2, e dai sistemi di backup **entro 90 giorni** in ragione dei cicli di rotazione dei backup cifrati.

7.4 **Obblighi di legge derogatori.** GLDA potra conservare i dati personali del Titolare oltre i termini sopra indicati esclusivamente ove cio sia imposto da obblighi di legge dell'Unione o di uno Stato membro, dandone tempestiva comunicazione scritta al Titolare con indicazione della norma di riferimento, della durata della conservazione e delle misure di limitazione adottate.

7.5 **Certificazione di cancellazione.** A completamento delle operazioni, GLDA rilascera al Titolare una **certificazione scritta di avvenuta cancellazione**, indicante data, ambito (sistemi di produzione, backup, log, cache), sub-responsabili coinvolti e firma del legale rappresentante.

ART. 8 — DIRITTO DI AUDIT DEL TITOLARE

8.1 GLDA mette a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR, e consente e contribuisce alle attivita di revisione, ivi comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato.

8.2 **Frequenza.** Il diritto di audit puo essere esercitato dal Titolare **una volta all'anno** in via ordinaria, salvi i casi di data breach, di richiesta documentata del Garante, di sostanziale modifica della lista sub-responsabili o di reclamo circostanziato di un interessato.

8.3 **Preavviso.** L'audit deve essere preannunciato con preavviso minimo di **30 giorni**, salvo casi di urgenza motivata.

8.4 **Modalita.** L'audit puo essere condotto:

(a) mediante questionario di autovalutazione compilato da GLDA;

(b) mediante verifica documentale (certificazioni, politiche, registri, log);

(c) mediante ispezione on-site presso la sede di GLDA;

(d) mediante audit di un terzo incaricato dal Titolare, vincolato a obblighi di riservatezza equivalenti.

8.5 **Costi.** I costi dell'audit sono a carico della Parte richiedente, salvo nel caso in cui l'audit evidenzi violazioni sostanziali del presente DPA da parte di GLDA, nel qual caso i costi sono a carico di GLDA.

8.6 **Documentazione alternativa.** A parziale assolvimento dell'obbligo di audit, GLDA puo mettere a disposizione del Titolare il proprio Security Datasheet, eventuali certificazioni di terza parte, rapporti di penetration test e altra documentazione equivalente.

ART. 9 — RISERVATEZZA

9.1 Ciascuna Parte si impegna a mantenere riservate tutte le informazioni di cui venga a conoscenza in ragione del presente DPA, ivi incluse le informazioni tecniche sulle misure di sicurezza, i dati personali trattati e i contenuti degli audit.

9.2 L'obbligo di riservatezza sopravvive alla cessazione del presente DPA per un periodo di 5 (cinque) anni, salvi gli obblighi di segretezza permanenti per legge.

9.3 Ciascuna Parte garantisce che i propri dipendenti, collaboratori e sub-fornitori siano vincolati da analoghi obblighi di riservatezza.

ART. 10 — TRASFERIMENTI DI DATI VERSO PAESI TERZI

10.1 **Principio di residenza EU.** GLDA si impegna a trattare i dati personali del Titolare prevalentemente in server ubicati nel territorio dell'Unione Europea o dello Spazio Economico Europeo, salve le eccezioni strutturali indicate al punto 10.2.

10.2 **Trasferimenti residui verso Paesi terzi.** In ragione dell'architettura tecnica del Servizio si verificano i seguenti trasferimenti residui:

(a) **Stati Uniti d'America** — sede legale di alcuni sub-responsabili (Vercel Inc., Resend Inc., Functional Software Inc. / Sentry, Google LLC, Meta Platforms Inc.) ai quali puo occorrere accesso remoto di supporto ai dati ospitati in data center europei. **Garanzie adottate**:

- adesione dei sub-responsabili al **Data Privacy Framework UE-USA** (DPF) ex Decisione (UE) 2023/1795, verificabile pubblicamente sul registro `https://www.dataprivacyframework.gov/list`;
- sottoscrizione delle **Clausole Contrattuali Tipo (SCC)** ex Decisione (UE) 2021/914 Modulo 2 o Modulo 3 con ciascun sub-responsabile;
- esecuzione di una **Transfer Impact Assessment (TIA)** documentata, ai sensi della sentenza CGUE C-311/18 (Schrems II) e delle Raccomandazioni EDPB 01/2020.

(b) **Emirati Arabi Uniti** — limitatamente al servizio di alert tecnici via Telegram Bot API (Telegram FZ-LLC, sede a Dubai), utilizzato esclusivamente per inviare al Privacy Lead di GLDA alert operativi contenenti **solo metadati tecnici** (ID esecuzione, ID studio pseudonimizzato, tipologia di errore) e **mai contenuti di pazienti, dati sanitari o dati identificativi degli interessati**. La TIA conclude che il trasferimento e a rischio residuo trascurabile in ragione dell'assenza strutturale di dati personali sostanziali.

10.3 **Vertex AI — region europea.** Per l'elaborazione dei messaggi conversazionali del chatbot, GLDA utilizza esclusivamente l'endpoint **Vertex AI region `europe-west4` (Eemshaven, Paesi Bassi)**, con Cloud Data Processing Addendum (CDPA) di Google Cloud accettato, data residency EU applicata, **Training Restriction attiva** ai sensi dell'art. 17 CDPA e configurazione tendente alla **minimizzazione della retention** lato modello.

10.4 **Meta / WhatsApp.** Le comunicazioni con i pazienti via WhatsApp Business Cloud API sono gestite da Meta Platforms Ireland Limited (Dublino, Irlanda), titolare autonomo per alcuni trattamenti connessi al funzionamento del canale. I dati eventualmente trasferiti da Meta Ireland verso Meta Platforms Inc. negli Stati Uniti sono coperti dall'adesione di Meta al Data Privacy Framework UE-USA.

10.5 GLDA si impegna a trasmettere al Titolare, su richiesta scritta, copia delle SCC sottoscritte con i sub-responsabili e della documentazione TIA, nei limiti degli obblighi di riservatezza verso i sub-responsabili stessi.

10.6 L'elenco aggiornato dei sub-responsabili, con indicazione per ciascuno del Paese di trattamento e delle garanzie applicate, e riportato nell'**Allegato I**.

ART. 11 — MISURE DI SICUREZZA (ART. 32 GDPR)

11.1 Le misure tecniche e organizzative adottate da GLDA per garantire la sicurezza del trattamento ai sensi dell'art. 32 GDPR sono sintetizzate nell'**Allegato II** al presente DPA. Il dettaglio operativo e contenuto nel **Security Datasheet** di InnovaMed, documento tecnico autonomo manutenuto da GLDA, disponibile al Titolare su richiesta.

11.2 In sintesi, tali misure comprendono: cifratura dei dati in transito (TLS 1.3) e a riposo (AES-256), Row Level Security nativa Postgres, autenticazione a due fattori obbligatoria sui ruoli con accesso a dati sanitari, audit log con retention 24 mesi, backup giornalieri cifrati con test di restore periodico, vulnerability management continuo, procedure di data breach 24 ore, controllo accessi role-based, pseudonimizzazione dei log applicativi e Zero Data Retention sulla pipeline AI.

ART. 12 — OUT-OF-SCOPE E DELIMITAZIONI DEL SERVIZIO

12.1 **Fascicolo Sanitario Elettronico 2.0 (FSE 2.0).** InnovaMed **non e un sistema di alimentazione del Fascicolo Sanitario Elettronico 2.0** ai sensi del DM 7 settembre 2023 e successive modifiche. Il Titolare dichiara di essere informato che:

(a) l'obbligo di alimentazione del FSE 2.0 riguarda strutture sanitarie pubbliche, strutture private accreditate, MMG, PLS e strutture convenzionate con il SSN;

(b) secondo la posizione FNOMCeO, il medico libero professionista in regime privatistico puro non e destinatario diretto dell'obbligo FSE 2.0;

(c) qualora il Titolare operi in regime convenzionato o accreditato, e responsabilita esclusiva dello stesso dotarsi di un gestionale clinico certificato FSE-ready distinto da InnovaMed;

(d) InnovaMed fornisce export dati in formato JSON/CSV per facilitare migrazioni verso gestionali certificati.

Il Titolare manleva GLDA, nei limiti consentiti dall'art. 1229 c.c., da qualsiasi pretesa derivante da una mancata alimentazione del FSE 2.0.

12.2 **Sistema Tessera Sanitaria (STS).** InnovaMed **non trasmette dati al Sistema Tessera Sanitaria** di cui al DM 31 luglio 2015. Il Titolare mantiene l'obbligo esclusivo di trasmissione dei dati delle spese sanitarie al Sistema TS, con qualsiasi strumento a sua scelta. GLDA declina ogni responsabilita per omesse, tardive o errate trasmissioni al Sistema TS. InnovaMed gestisce esclusivamente il flag "opposizione_sts" per ogni paziente.

12.3 **Firma digitale qualificata e conservazione sostitutiva AgID.** InnovaMed **non integra firma digitale qualificata** ai sensi del Reg. (UE) 910/2014 (eIDAS) e del D.Lgs. 82/2005 (CAD), ne opera quale **sistema di conservazione a norma accreditato presso l'Agenzia per l'Italia Digitale (AgID)**. Le bozze di referto generate da InnovaMed costituiscono documenti di lavoro privi di valore legale probatorio autonomo. Il Titolare e l'unico responsabile di:

(a) verificare l'accuratezza clinica del contenuto;

(b) apporre firma digitale qualificata con strumenti di propria scelta;

(c) conservare il documento firmato presso sistemi a norma di propria scelta.

12.4 **Dispositivo medico.** InnovaMed **non e un dispositivo medico** ai sensi del Reg. (UE) 2017/745 (MDR) e non richiede marcatura CE come dispositivo medico. La sua finalita d'uso (intended purpose) e limitata alle operazioni di **storage, archival, communication and simple search** consentite dalla **MDCG 2019-11 rev.1** (giugno 2025). InnovaMed non fornisce supporto decisionale clinico, non elabora alert clinici automatici, non calcola scoring di rischio, non interpreta esami, non suggerisce diagnosi, non calcola interazioni farmacologiche, non propone dosaggi. Il Titolare e l'unico responsabile della validita clinica dei dati inseriti e delle decisioni cliniche prese sulla base degli stessi.

ART. 13 — RESPONSABILITA E LIMITAZIONI

13.1 Ciascuna Parte risponde dei danni cagionati all'altra Parte in conseguenza dell'inadempimento degli obblighi assunti con il presente DPA, nei limiti di quanto previsto dagli articoli 82 GDPR e 1229 c.c.

13.2 **Limitazione di responsabilita.** Fermo restando quanto previsto dall'art. 1229 c.c., la responsabilita complessiva di GLDA verso il Titolare per qualsiasi pretesa derivante dal o connessa al presente DPA e limitata, in aggregato, all'importo corrispondente al **corrispettivo complessivamente pagato dal Titolare a GLDA nei 12 mesi precedenti** l'evento generatore della pretesa, ovvero, in caso di mancato raggiungimento di tale periodo, al corrispettivo complessivamente pagato fino alla data della pretesa. Tale limitazione **non si applica in caso di dolo, colpa grave** o violazione di obblighi inderogabili di legge.

13.3 **Manleva del Titolare.** Il Titolare manleva GLDA da ogni pretesa di terzi che derivi da:

(a) uso improprio o illecito della piattaforma da parte del Titolare o dei suoi utenti autorizzati;

(b) inesattezza, incompletezza o illiceita dei dati inseriti dal Titolare nella piattaforma;

(c) omessa raccolta dei consensi degli interessati o mancata consegna dell'informativa privacy ex art. 13 GDPR da parte del Titolare;

(d) decisioni cliniche assunte sulla base dei dati trattati con InnovaMed;

(e) omessa alimentazione del FSE 2.0, omessa trasmissione al Sistema TS, omessa firma digitale qualificata, omessa conservazione a norma;

(f) violazioni della normativa fiscale, sanitaria, deontologica e del Codice Privacy di cui sia responsabile il Titolare.

13.4 Ciascuna Parte e responsabile del pagamento di eventuali sanzioni amministrative irrogate dal Garante nei propri confronti in ragione di inadempimenti agli obblighi ad essa riferibili.

ART. 14 — DURATA, CESSAZIONE E MODIFICHE

14.1 Il presente DPA entra in vigore alla data di accettazione click-wrap da parte del Titolare e resta efficace per l'intera durata del Contratto Principale.

14.2 In caso di cessazione del Contratto Principale, le disposizioni del presente DPA destinate per loro natura a sopravvivere continuano ad avere effetto, ivi inclusi gli obblighi di cancellazione o restituzione dei dati (art. 7), riservatezza (art. 9), responsabilita (art. 13), audit (art. 8) per le operazioni svolte prima della cessazione.

14.3 **Modifiche al DPA.** Il presente DPA puo essere modificato solo per iscritto, con accordo di entrambe le Parti, fatte salve:

(a) le modifiche imposte da variazioni della normativa applicabile o da provvedimenti del Garante;

(b) gli aggiornamenti dell'Allegato I (lista sub-responsabili) effettuati da GLDA nel rispetto della procedura di cui all'art. 5.4.

14.4 **Versionamento del modello master.** GLDA mantiene un changelog pubblico delle versioni del DPA master pubblicato su `https://med.innovaflow.it/trust/dpa`. Il Titolare e tenuto a riconfermare l'accettazione del DPA in caso di modifiche sostanziali; in caso di mancata accettazione entro 30 giorni dalla notifica, il Titolare ha diritto di recesso senza penali ai sensi dell'art. 5.4.3.

14.5 **Prevalenza.** In caso di contrasto tra le disposizioni del presente DPA e quelle del Contratto Principale, prevalgono le disposizioni del presente DPA limitatamente alle materie relative alla protezione dei dati personali.

ART. 15 — LEGGE APPLICABILE E FORO COMPETENTE

15.1 Il presente DPA e regolato dalla legge italiana e, per quanto non espressamente previsto, dal GDPR, dal Codice Privacy e dalle norme attuative applicabili.

15.2 Per qualsiasi controversia derivante dall'interpretazione, esecuzione, validita, risoluzione e, in generale, dal presente DPA, le Parti concordano di tentare preliminarmente una composizione amichevole della controversia entro 30 giorni dalla contestazione scritta.

15.3 In mancanza di composizione amichevole, sara esclusivamente competente il **Foro di Milano**, con esclusione di ogni altro foro concorrente o alternativo.

ART. 16 — DISPOSIZIONI FINALI

16.1 **Integrazione.** Il presente DPA, unitamente ai suoi Allegati I, II e III, contiene l'intero accordo tra le Parti in materia di protezione dei dati personali e sostituisce ogni precedente accordo, scritto o verbale, relativo al medesimo oggetto.

16.2 **Invalidita parziale.** L'eventuale invalidita di una clausola non inficera la validita delle restanti disposizioni.

16.3 **Cessione.** Il presente DPA non puo essere ceduto da alcuna delle Parti senza il preventivo consenso scritto dell'altra Parte, fatte salve le operazioni di riorganizzazione aziendale infragruppo e le cessioni d'azienda o di ramo d'azienda, comunicate con un preavviso di almeno 30 giorni.

16.4 **Tolleranza.** L'eventuale tolleranza di una Parte rispetto all'inadempimento dell'altra non costituisce rinuncia a far valere i diritti nascenti dal presente DPA.

16.5 **Comunicazioni.** Tutte le comunicazioni tra le Parti relative al presente DPA saranno effettuate per iscritto, via email ai recapiti indicati in epigrafe o via PEC agli indirizzi ivi riportati.

ART. 17 — DISCIPLINA DELL'ACCETTAZIONE CLICK-WRAP

17.1 **Modalita di accettazione.** Il Titolare accetta integralmente il presente DPA mediante meccanismo elettronico click-wrap presentato durante la procedura di onboarding del proprio studio sulla piattaforma InnovaMed. L'accettazione e perfezionata mediante:

(a) visualizzazione integrale del testo del DPA in versione leggibile;

(b) spunta di **checkbox non pre-spuntata** ("Dichiaro di aver letto e di accettare integralmente il Data Processing Agreement (DPA) v1.0 del 10 aprile 2026");

(c) invio del form da parte del legale rappresentante / titolare dello studio identificato tramite credenziali di accesso univoche.

17.2 **Tracciamento dell'accettazione.** Al momento dell'accettazione, GLDA registra in modo automatico e tamper-evident i seguenti elementi, conservati per tutta la durata del Contratto Principale e per ulteriori 10 anni dalla cessazione:

Campo	Descrizione
`dpa_versione`	"1.0"
`dpa_data_emissione`	"2026-04-10"
`dpa_hash_sha256`	Hash SHA-256 del testo esatto del DPA mostrato al Titolare
`studio_id`	UUID dello studio cliente
`utente_id`	UUID dell'utente che ha eseguito l'accettazione
`nome_legale_rappresentante`	Nome completo dichiarato in onboarding
`timestamp_accettazione`	Data e ora UTC + Europe/Rome
`ip_origine`	Indirizzo IP della richiesta di accettazione
`user_agent`	User agent del browser
`metodo_accettazione`	"click_wrap_onboarding"

17.3 **Valore probatorio.** Il log di accettazione costituisce prova dell'accordo ai sensi degli artt. 20-22 del Reg. (UE) 910/2014 (eIDAS) e dell'art. 2702 c.c., e puo essere esibito in qualsiasi sede giudiziale o stragiudiziale a richiesta del Titolare, del Garante o dell'autorita giudiziaria.

17.4 **Disponibilita di firma autografa.** Il Titolare che desideri sottoscrivere il presente DPA in modalita autografa o con firma elettronica qualificata, in luogo dell'accettazione click-wrap, puo richiederlo via email a `privacy@innovaflow.it`. GLDA fornira copia controfirmata in formato PDF/A entro 5 giorni lavorativi.

17.5 **Conservazione del documento accettato.** Il Titolare puo in qualsiasi momento scaricare dalla propria area riservata copia del DPA accettato, completa di evidenze di accettazione (timestamp, hash, IP).

SOTTOSCRIZIONE MASTER (PRE-FIRMA UNILATERALE GLDA)

Il presente DPA modello viene pre-firmato unilateralmente da GLDA SRL in data 10 aprile 2026, perfezionandosi nei confronti di ciascun Titolare al momento dell'accettazione click-wrap secondo le modalita di cui all'art. 17.

Per GLDA SRL (Responsabile del trattamento)

Luogo e data: **Buccinasco (MI), 10 aprile 2026**

Firma digitale del legale rappresentante:

D'ALESSANDRO Giuseppe Amministratore Unico — GLDA SRL Codice fiscale: DLSGPP69T03F839R PEC: dalessandro.g@legalmail.it

---

Per il Titolare — accettazione perfezionata via click-wrap come da art. 17 al momento dell'attivazione dello studio sulla piattaforma InnovaMed.

Ai sensi e per gli effetti degli articoli 1341 e 1342 c.c., il Titolare, mediante l'accettazione click-wrap, dichiara di aver esaminato e di accettare specificamente le seguenti clausole: art. 1 (Qualificazione dei ruoli); art. 5.1 (Istruzioni documentate e divieto di finalita proprie); art. 5.4 (Sub-responsabili e autorizzazione generale); art. 6 (Violazioni dei dati personali — SLA 24 ore); art. 7 (Cancellazione o restituzione dei dati); art. 8 (Diritto di audit); art. 10 (Trasferimenti extra-UE); art. 12 (Out-of-scope e delimitazioni del servizio); art. 13 (Responsabilita e limitazioni); art. 14 (Modifiche e versionamento); art. 15 (Foro competente — Milano); art. 17 (Disciplina dell'accettazione click-wrap).

ALLEGATO I — LISTA SUB-RESPONSABILI DEL TRATTAMENTO

L'elenco aggiornato dei sub-responsabili autorizzati da GLDA per l'erogazione del Servizio InnovaMed e pubblicato all'indirizzo:

`https://med.innovaflow.it/trust/sub-processors`

Alla data del presente DPA (10 aprile 2026) i sub-responsabili attivi sono:

#	Sub-responsabile	Finalita	Region primaria	Garanzie
1	**Supabase Inc. / Supabase Pte. Ltd.**	Database PostgreSQL gestito, Storage, Auth	UE — `eu-central-1` Francoforte	DPA Supabase + SCC 2021/914 + RLS + cifratura at-rest AES-256
2	**Google Cloud EMEA Limited / Google LLC** — Vertex AI	Modello AI Gemini per chatbot conversazionale	UE — `europe-west4` Eemshaven (Paesi Bassi)	CDPA Google + SCC Modulo 2 + DPF + Training Restriction art. 17 + minimizzazione retention

#	Sub-responsabile	Finalita	Region primaria	Garanzie
3	**Meta Platforms Ireland Limited** — WhatsApp Business Cloud API	Canale di messaggistica con i pazienti	UE (Irlanda) + USA infragruppo	DPF + SCC 2021/914 + WhatsApp Business Terms + verifica X-Hub-Signature-256
4	**Vercel Inc.**	Hosting Next.js, Edge Functions, CDN, cron jobs	UE — `fra1` Francoforte	DPA Vercel + DPF + SCC Modulo 3 + TIA
5	**Resend, Inc.**	Email transazionali (welcome, reminder, conferme)	USA + backhaul EU	DPA Resend + DPF + SCC Modulo 3 + TIA + TLS SMTP imposto
6	**Functional Software, Inc. (Sentry)**	Error tracking e APM	UE — `eu.sentry.io` Francoforte	DPA Sentry + region EU + DPF + SCC + PII scrubbing lato SDK
7	**Telegram FZ-LLC**	Alert tecnici al solo Privacy Lead di GLDA — solo metadati pseudonimizzati, nessun dato di interessati	EAU (Dubai)	TIA con rischio residuo trascurabile per assenza strutturale di dati personali sostanziali
8	**Cloudflare, Inc.**	DNS, email routing per `privacy@innovaflow.it`, eventuale CDN/WAF	USA con region EU per DNS resolver	DPA Cloudflare + DPF + SCC Modulo 3

Le certificazioni DPF dei soggetti USA sono verificabili sul registro pubblico `https://www.dataprivacyframework.gov/list`.

Eventuali modifiche all'elenco sub-responsabili seguono la procedura di cui all'art. 5.4 del presente DPA.

ALLEGATO II — MISURE TECNICHE E ORGANIZZATIVE DI SICUREZZA (ART. 32 GDPR) — SINTESI

> *Il dettaglio operativo delle seguenti misure è contenuto nel* ***Security Datasheet di InnovaMed*** *(documento autonomo), disponibile al Titolare su richiesta a* `privacy@innovaflow.it`.

Cifratura

- Cifratura in transito TLS 1.3 con cifrari AEAD e forward secrecy; HSTS preload su tutti i domini pubblici.
- Cifratura a riposo AES-256 sul database PostgreSQL gestito da Supabase e su Storage.

Controllo accessi

- Autenticazione tramite Better Auth con **2FA TOTP obbligatoria** sui ruoli con accesso a dati sanitari (admin, proprietario, dottore), in linea con l'orientamento del Garante (Provv. Garante 474/2025 caso Careggi e Linee guida dossier sanitario 4/6/2015).
- Autorizzazione granulare role-based con catalog di permessi configurabile per studio (helper `withSession` + `requirePermission`).
- **Row Level Security (RLS)** nativa Postgres con isolamento per `studio_id`; zero query cross-studio da codice applicativo.
- Device fingerprinting con cookie HttpOnly Secure SameSite per rilevazione sessioni anomale.
- Principio need-to-know per il personale GLDA, con nomine ex art. 29 GDPR e rotazione credenziali.

Audit logging tamper-evident

- Registro audit append-only via trigger Postgres su tutte le tabelle sensibili (`note_cliniche`, `parametri_vitali`, `allergie_paziente`, `farmaci_paziente`, `referti`, `appuntamenti`, `pazienti`).
- Policy RLS che impediscono UPDATE e DELETE sulla tabella `audit_log` anche al `service_role`.
- **Retention 24 mesi** in linea con il Provv. Garante 474/2025.
- Tracciamento di: tabella, record_id, azione, utente_id, studio_id, IP, user agent, diff JSON, motivazione, timestamp.

Backup

- Backup giornalieri automatici cifrati (Supabase PITR + snapshot).
- Retention: 30 giorni giornalieri + opzionali backup off-site cifrati su storage S3-compatible europeo.

- Test di restore periodici documentati.
- **Disaster Recovery Plan** scritto con RPO/RTO compatibili con il livello di servizio del pilota.

Vulnerability management

- Dependabot per CVE su dipendenze pnpm; npm audit in CI pipeline; patch security applicate entro 7 giorni dal rilascio.
- Security Headers strict (HSTS, X-Content-Type-Options, X-Frame-Options, Referrer-Policy, Permissions-Policy, Content-Security-Policy).

Rate limiting

- Soglie differenziate per endpoint (admin, pazienti, conversazioni, webhook WhatsApp).
- Verifica obbligatoria di `X-Hub-Signature-256` su tutti i webhook Meta in entrata.
- Verifica `Bearer CRON_SECRET` su tutti gli endpoint cron.

Error tracking

- Sentry EU region (`eu.sentry.io` Francoforte) con **PII scrubbing lato SDK** (hook `beforeSend`).
- Breadcrumbs tecnici con `execution_id` e senza contenuti paziente.
- Alert Telegram al solo Privacy Lead con esclusivamente metadati tecnici (no dati personali).

Pipeline AI

- Modello Google Gemini invocato tramite **Vertex AI region** `europe-west4`.
- CDPA Google con SCC Modulo 2 incorporate.
- **Training Restriction art. 17 CDPA attiva**: Google non utilizza i dati del Titolare per addestrare modelli.
- **Hallucination guard** sugli output AI; **circuit breaker** per modello con apertura automatica e fallback message generico.

Misure organizzative

- Nomine ex art. 29 GDPR sottoscritte per ogni soggetto autorizzato al trattamento.
- Contratti con sub-responsabili con clausole art. 28 GDPR + SCC ove necessarie.
- Procedura interna data breach con SLA 24h verso il Titolare.
- Procedura interna gestione richieste di esercizio dei diritti.

ALLEGATO III — ISTRUZIONI DOCUMENTATE DEL TITOLARE

Il Titolare, mediante l'accettazione del presente DPA, da espressamente le seguenti istruzioni documentate a GLDA ai sensi dell'art. 28, par. 3, lett. a, GDPR:

III.1 — Istruzioni di trattamento

(a) Trattare i dati personali dei propri pazienti **esclusivamente per le finalita** elencate all'art. 3 del presente DPA, senza alcuna finalita propria di GLDA.

(b) Trattare i dati personali in **modalita multi-tenant con isolamento per studio**, senza alcuna interconnessione cross-studio se non quelle tecniche strettamente necessarie alla fornitura del Servizio.

(c) **Pseudonimizzare** i dati nei log applicativi e nei sistemi di error tracking secondo le policy descritte nell'Allegato II.

(d) **Inviare via WhatsApp solo dati anagrafici neutri e metadati di appuntamento**; veicolare ogni contenuto sanitario sensibile esclusivamente tramite link protetti al portale web (deep-link policy).

(e) Conservare i dati per la durata del Contratto Principale e cancellarli o restituirli alla cessazione secondo l'art. 7.

III.2 — Istruzioni in materia di sicurezza

(a) Adottare e mantenere le misure tecniche e organizzative dell'Allegato II.

(b) Mantenere attiva la Training Restriction su Vertex AI per impedire l'uso dei dati del Titolare per addestramento di modelli AI di Google.

(c) Mantenere attiva la cifratura at-rest, la 2FA sui ruoli con accesso a dati sanitari e l'audit log con retention 24 mesi.

III.3 — Istruzioni in materia di sub-responsabili

(a) Avvalersi dei sub-responsabili elencati nell'Allegato I, con autorizzazione generale ex art. 28, par. 2, GDPR.

(b) Notificare al Titolare ogni modifica con preavviso minimo di 30 giorni secondo la procedura di cui all'art. 5.4.

III.4 — Istruzioni in materia di trasferimenti extra-UE

(a) Limitare i trasferimenti extra-UE alle sole esigenze strutturali del Servizio descritte all'art. 10.

(b) Mantenere SCC e DPF coverage per ciascun sub-responsabile USA.

(c) Limitare il trasferimento via Telegram a soli metadati tecnici pseudonimizzati, senza dati di interessati.

III.5 — Istruzioni in materia di esercizio dei diritti degli interessati

(a) Inoltrare al Titolare ogni richiesta di esercizio dei diritti (artt. 15-22 GDPR) ricevuta direttamente da un interessato, senza rispondere direttamente, salvo diversa istruzione del Titolare.

(b) Mettere a disposizione del Titolare le funzionalita di accesso, rettifica, cancellazione, portabilita e limitazione descritte all'art. 5.5.

III.6 — Istruzioni in materia di data breach

(a) Notificare al Titolare ogni violazione confermata entro 24 ore dalla conferma, secondo le modalita di cui all'art. 6.

(b) Fornire al Titolare un template di notifica al Garante pre-compilato al 90%.

(c) Mantenere il registro interno delle violazioni accessibile al Titolare su richiesta.

GLDA SRL — InnovaMed — DPA Master v1.0 — 10 aprile 2026 Sede legale: Via della Resistenza 56, 20090 Buccinasco (MI) — C.F./P.IVA 14385190963 — REA MI-2779148 PEC: glda@legalmail.it — Punto di contatto privacy: privacy@innovaflow.it Conforme al Compendio Garante 28/03/2024 e al Codice di Condotta Software Gestionali (Provv. Garante 498/2024 del 17/10/2024).