

Clinovus AI

Accordo sul trattamento dei dati personali

Data Processing Agreement — Art. 28 GDPR

Riferimento / Reference	CLINOVUS-DPA-MED-2026
Versione / Version	1.1 (sostituisce la 1.0 del 15.05.2026 / supersedes 1.0 of 15.05.2026)
Data emissione / Issue date	5 ottobre 2026 / 5 October 2026
Entrata in vigore / Effective	Nuovi account: alla data di emissione. Account esistenti: 4 novembre 2026, dopo il preavviso di 30 giorni (art. 15.2). / New accounts: on the issue date. Existing accounts: 4 November 2026, after 30 days' notice (Art. 15.2).
Lingue / Languages	Italiano e Inglese (IT prevale in caso di conflitto)
Titolare / Controller	Medico utilizzatore della piattaforma
Responsabile / Processor	Plancherel Solutions
Foro / Jurisdiction	Italia / Italy
Legge applicabile / Governing law	Italiana / Italian
Contatto protezione dati / Data protection contact	dpo@clinovusai.com

Il presente Accordo è concluso in occasione della creazione dell'account Clinovus AI da parte del medico, in qualità di Titolare del trattamento dei dati dei propri pazienti. È redatto in italiano e in inglese; in caso di conflitto interpretativo, prevale la versione italiana.

This Agreement is concluded upon creation of the Clinovus AI account by the physician, acting as Data Controller of the personal data of their patients. It is drafted in Italian and English; in case of conflict, the Italian version prevails.

Indice / Table of contents

	Preambolo / Preamble
Art. 1	Definizioni / Definitions
Art. 2	Oggetto, durata, natura e finalità / Object, duration, nature and purpose
Art. 3	Categorie di dati e interessati / Categories of data and data subjects
Art. 4	Obblighi del Responsabile / Obligations of the Processor
Art. 5	Sub-responsabili / Sub-processors
Art. 6	Trasferimenti / Transfers
Art. 7	Diritti degli interessati / Rights of data subjects
Art. 8	Violazioni dei dati / Data breaches
Art. 9	Audit e ispezioni / Audit and inspections
Art. 10	Cancellazione e restituzione / Deletion and return
Art. 11	Durata e termine / Term and termination
Art. 12	Responsabilità / Liability
Art. 13	Cessione del contratto / Assignment
Art. 14	Foro e legge / Jurisdiction and law
Art. 15	Disposizioni finali / Final provisions
	Accettazione / Acceptance (click-wrap)
	Allegato A — Descrizione del trattamento / Annex A — Description of processing
	Allegato B — Lista sub-responsabili / Annex B — List of sub-processors
	Allegato C — Misure di sicurezza / Annex C — Security measures
	Allegato D — Modifiche rispetto alla versione 1.0 / Annex D — Changes from version 1.0

Preambolo / Preamble

Il presente Accordo è stipulato tra:

This Agreement is entered into between:

IL TITOLARE / THE CONTROLLER	IL RESPONSABILE / THE PROCESSOR
Il medico utilizzatore della piattaforma Clinovus AI, identificato dai dati dell'account creato sul sito clinovusai.com. / The physician using the Clinovus AI platform, identified by the account data created on clinovusai.com.	Plancherel Solutions (ditta individuale di diritto svizzero), titolare: Jean-Paul Plancherel, sede: Canton Vaud, Svizzera, IDI CHE-379.895.072. / Plancherel Solutions (Swiss sole proprietorship), owner: Jean-Paul Plancherel, registered in the Canton of Vaud, Switzerland, UID CHE-379.895.072.

PREMESSO CHE (A) il Titolare offre servizi sanitari ai propri pazienti, in qualità di professionista sanitario tenuto al segreto professionale, ed effettua trattamenti di dati personali, ivi compresi dati relativi alla salute (categorie particolari ex art. 9 GDPR); (B) il Responsabile fornisce, tramite la piattaforma SaaS Clinovus AI, servizi tecnologici di supporto al medico per la trascrizione, la strutturazione a partire dalla dettatura o dal materiale fornito dal medico, l'organizzazione e la consultazione di documentazione clinica; (C) le parti intendono regolare il trattamento dei dati personali effettuato dal Responsabile per conto del Titolare, ai sensi dell'art. 28 GDPR.

WHEREAS (A) the Controller provides healthcare services to their patients, as a healthcare professional subject to professional secrecy, and processes personal data including health data (special categories under Art. 9 GDPR); (B) the Processor provides, through the Clinovus AI SaaS platform, technological services supporting the physician in transcribing, structuring from the physician's dictation or material, organising and consulting clinical documentation; (C) the parties intend to govern the processing of personal data carried out by the Processor on behalf of the Controller, pursuant to Art. 28 GDPR.

TUTTO CIÒ PREMESSO, LE PARTI CONVENGONO QUANTO SEGUE:

NOW, THEREFORE, THE PARTIES AGREE AS FOLLOWS:

Art. 1 — Definizioni / Definitions

GDPR	Regolamento (UE) 2016/679 sul trattamento dei dati personali. / Regulation (EU) 2016/679 on the processing of personal data.
Codice Privacy / Italian Privacy Code	D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018. / Legislative Decree 196/2003 as amended by Legislative Decree 101/2018.
Dati personali / Personal data	Qualsiasi informazione riguardante una persona fisica identificata o identificabile (art. 4(1) GDPR). / Any information relating to an identified or identifiable natural person (Art. 4(1) GDPR).
Categorie particolari / Special categories	Dati di cui all'art. 9(1) GDPR, in particolare dati relativi alla salute. / Data referred to in Art. 9(1) GDPR, in particular health data.
Trattamento / Processing	Qualsiasi operazione applicata a dati personali (art. 4(2) GDPR). / Any operation performed on personal data (Art. 4(2) GDPR).
Titolare / Controller	Il medico utilizzatore della piattaforma, ai sensi dell'art. 4(7) GDPR. / The physician using the platform, within the meaning of Art. 4(7) GDPR.
Responsabile / Processor	Plancherel Solutions, ai sensi dell'art. 4(8) GDPR. / Plancherel Solutions, within the meaning of Art. 4(8) GDPR.
Sub-responsabile / Sub-processor	Soggetto terzo cui il Responsabile affida operazioni di trattamento, ai sensi dell'art. 28(2) e (4) GDPR. / Third party to whom the Processor entrusts processing operations, pursuant to Art. 28(2) and (4) GDPR.
Interessati / Data subjects	Pazienti del Titolare i cui dati sono trattati attraverso la piattaforma. / Patients of the Controller whose data are processed through the platform.
Violazione / Personal data breach	Definita dall'art. 4(12) GDPR. / As defined in Art. 4(12) GDPR.
Piattaforma / Platform	Servizio Clinovus AI accessibile su clinovusai.com e domini correlati. / Clinovus AI service accessible at clinovusai.com and related domains.

**Istruzioni documentate /
Documented instructions**

Le istruzioni del Titolare risultanti dal presente DPA, dalle Condizioni generali e dalle configurazioni della Piattaforma. / Instructions resulting from this DPA, the Terms of Service and the Platform configurations.

Art. 2 — Oggetto, durata, natura e finalità / Object, duration, nature and purpose

2.1 Il Titolare nomina il Responsabile per il trattamento dei dati personali dei propri pazienti, effettuato attraverso la Piattaforma per le finalità descritte nell'Allegato A.

2.1 The Controller appoints the Processor to process the personal data of their patients, carried out through the Platform for the purposes described in Annex A.

2.2 Durata. Il presente Accordo decorre dall'accettazione (accettazione elettronica alla creazione dell'account) e ha durata pari alla durata dell'utilizzo della Piattaforma; resta in vigore fino all'estinzione di tutti gli obblighi residui in materia di sicurezza, cancellazione, restituzione e cooperazione.

2.2 Duration. This Agreement starts upon acceptance (electronic acceptance at account creation) and lasts for the duration of the use of the Platform; it remains in force until all residual obligations regarding security, deletion, return and cooperation are extinguished.

2.3 Natura del trattamento. Trattamento prevalentemente automatizzato di documentazione clinica, trascrizione audio, consultazione di una base di conoscenze mediche e di registri ufficiali e supporto conversazionale, mediante tecnologie di intelligenza artificiale (LLM, ASR, RAG).

2.3 Nature of processing. Predominantly automated processing of clinical documentation, audio transcription, consultation of a medical knowledge base and official registers, and conversational support, by means of artificial intelligence technologies (LLM, ASR, RAG).

2.4 Finalità. Supportare il Titolare nella redazione della documentazione clinica a partire dalla sua dettatura o dal materiale da lui fornito e nella consultazione di informazioni mediche con fonti. La Piattaforma non è un dispositivo medico, non è destinata a supportare decisioni diagnostiche o terapeutiche e non sostituisce il giudizio professionale del medico, che valida ogni contenuto.

2.4 Purpose. To support the Controller in drafting clinical documentation from their dictation or the material they provide, and in consulting sourced medical information. The Platform is not a medical device, is not intended to support diagnostic or therapeutic decisions and does not replace the physician's professional judgement; the physician validates all content.

Art. 3 — Categorie di dati e interessati / Categories of data and data subjects

3.1 Categorie di interessati. Pazienti del Titolare i cui dati sono trattati attraverso la Piattaforma. Eventualmente: terzi menzionati nella documentazione clinica (familiari, altri professionisti).

3.1 Categories of data subjects. Patients of the Controller whose data are processed through the Platform. Where applicable: third parties mentioned in clinical documentation (family members, other professionals).

3.2 Categorie di dati. (i) Dati identificativi del paziente: iniziali, età, sesso (anonimizzazione raccomandata); (ii) dati sanitari ai sensi dell'art. 9 GDPR: sintomi, anamnesi, diagnosi, esami, terapie, allergie; (iii) dati derivati dalla consultazione: registrazioni audio, trascrizioni, richieste e risposte dell'IA, documenti caricati.

3.2 Categories of data. (i) Patient identification data: initials, age, sex (anonymisation recommended); (ii) health data under Art. 9 GDPR: symptoms, history, diagnoses, tests, therapies, allergies; (iii) consultation-derived data: audio recordings, transcripts, AI prompts and outputs, uploaded documents.

3.3 Minimizzazione. Il Titolare si impegna a non inserire nella Piattaforma dati personali eccedenti rispetto alle finalità, e in particolare a usare iniziali o codici identificativi al posto del nome completo del paziente, ove possibile.

3.3 Minimisation. The Controller undertakes not to enter into the Platform personal data exceeding the purposes, and in particular to use initials or identification codes instead of the patient's full name, where possible.

Art. 4 — Obblighi del Responsabile / Obligations of the Processor

Il Responsabile si impegna a:

The Processor undertakes to:

**(a) Istruzioni documentate /
Documented instructions**

Trattare i dati personali solo su istruzione documentata del Titolare, salvo obbligo di legge. / Process personal data only on documented instructions from the Controller, unless required by law.

(b) Riservatezza / Confidentiality	Garantire che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza. / Ensure that persons authorised to process the data are committed to confidentiality or are under a statutory obligation of confidentiality.
(c) Sicurezza / Security	Adottare le misure tecniche e organizzative adeguate ai sensi dell'art. 32 GDPR, descritte nell'Allegato C. / Adopt appropriate technical and organisational measures pursuant to Art. 32 GDPR, as described in Annex C.
(d) Sub-responsabili / Sub-processors	Rispettare l'art. 5 del presente DPA per il ricorso a sub-responsabili. / Comply with Art. 5 of this DPA for engaging sub-processors.
(e) Diritti degli interessati / Data subject rights	Assistere il Titolare con misure tecniche e organizzative adeguate per soddisfare gli obblighi di risposta alle richieste degli interessati. / Assist the Controller with appropriate technical and organisational measures to fulfil obligations to respond to data subject requests.
(f) Sicurezza, violazioni, DPIA / Security, breaches, DPIA	Assistere il Titolare nel garantire il rispetto degli obblighi di cui agli artt. 32-36 GDPR, tenuto conto della natura del trattamento e delle informazioni a disposizione. / Assist the Controller in ensuring compliance with Arts. 32-36 GDPR, taking into account the nature of processing and the information available.
(g) Cancellazione / Deletion	Su scelta del Titolare, cancellare o restituire tutti i dati personali al termine della prestazione (cfr. art. 10). / At the Controller's choice, delete or return all personal data after the end of the provision of services (cf. Art. 10).
(h) Conformità verificabile / Demonstrable compliance	Mettere a disposizione del Titolare le informazioni necessarie per dimostrare il rispetto degli obblighi del presente DPA e consentire audit (cfr. art. 9). / Make available to the Controller the information necessary to demonstrate compliance with this DPA and allow audits (cf. Art. 9).
(i) Notifica violazioni / Breach notification	Notificare al Titolare ogni violazione dei dati personali senza ingiustificato ritardo, e comunque entro 24 ore dalla conoscenza, fornendo le informazioni di cui all'art. 33(3) GDPR. / Notify the Controller of any personal data breach without undue delay, and in any case within 24 hours of becoming aware, providing the information referred to in Art. 33(3) GDPR.
(j) Punto di contatto / Point of contact	Fornire un punto di contatto unico per ogni questione relativa al trattamento: dpo@clinovusai.com. / Provide a single point of contact for any matter relating to the processing: dpo@clinovusai.com.

Art. 5 — Sub-responsabili / Sub-processors

5.1 Autorizzazione generale. Il Titolare concede al Responsabile autorizzazione generale a ricorrere ai sub-responsabili elencati nell'**Allegato B**.

5.1 General authorisation. The Controller grants the Processor general authorisation to engage the sub-processors listed in Annex B.

5.2 Modifiche. Il Responsabile informa il Titolare di ogni modifica prevista riguardante l'aggiunta o la sostituzione di sub-responsabili con preavviso di **30 giorni**, dando al Titolare l'opportunità di opporsi.

5.2 Changes. The Processor informs the Controller of any intended change concerning the addition or replacement of sub-processors with **30 days'** notice, giving the Controller the opportunity to object.

5.3 Diritto di opposizione. Il Titolare può opporsi a un nuovo sub-responsabile per motivi ragionevoli legati alla protezione dei dati. In tal caso, il Responsabile può: (a) astenersi dall'introdurre il nuovo sub-responsabile; (b) proporre una soluzione alternativa; (c) consentire al Titolare di recedere dal contratto senza penali, con rimborso pro-rata della porzione di abbonamento non goduta.

5.3 Right to object. The Controller may object to a new sub-processor on reasonable data-protection grounds. In such case, the Processor may: (a) refrain from introducing the new sub-processor; (b) propose an alternative solution; (c) allow the Controller to terminate the contract without penalty, with pro-rata refund of the unused subscription portion.

5.4 Catena contrattuale. Il Responsabile impone ai sub-responsabili obblighi in materia di protezione dei dati equivalenti a quelli del presente DPA, in particolare sulla sicurezza (art. 32 GDPR).

5.4 Contractual chain. The Processor imposes on sub-processors data-protection obligations equivalent to those set out in this DPA, in particular regarding security (Art. 32 GDPR).

5.5 Responsabilità. Il Responsabile risponde nei confronti del Titolare per l'adempimento degli obblighi del sub-responsabile, ai sensi dell'art. 28(4) GDPR.

5.5 Liability. *The Processor is liable to the Controller for the sub-processor's fulfilment of its obligations, pursuant to Art. 28(4) GDPR.*

Art. 6 — Trasferimenti / Transfers

6.1 Localizzazione. Il trattamento dei dati dei pazienti avviene in **Svizzera** (datacenter di Infomaniak Network SA), paese coperto dalla decisione di adeguatezza UE del 26.07.2000. Nessun dato dei pazienti è trasferito al di fuori della Svizzera.

6.1 Location. *Patient data is processed in **Switzerland** (Infomaniak Network SA datacentres), a country covered by the EU adequacy decision of 26.07.2000. No patient data is transferred outside Switzerland.*

6.2 Trasferimenti accessori. I soli dati che possono lasciare la Svizzera sono i dati di fatturazione del medico trattati da Stripe (Allegato B), che possono essere trasferiti verso gli Stati Uniti sulla base del **Data Privacy Framework UE-USA** (decisione di adeguatezza del 10.07.2023) e delle clausole contrattuali tipo. Il Responsabile monitora la validità di tali garanzie.

6.2 Accessory transfers. *The only data that may leave Switzerland is the physician's billing data processed by Stripe (Annex B), which may be transferred to the United States on the basis of the **EU-US Data Privacy Framework** (adequacy decision of 10.07.2023) and standard contractual clauses. The Processor monitors the validity of these safeguards.*

6.3 Modifiche del quadro normativo. In caso di invalidazione di una decisione di adeguatezza, il Responsabile adotta tempestivamente garanzie appropriate (art. 46 GDPR) o sospende il trasferimento.

6.3 Regulatory changes. *In case of invalidation of an adequacy decision, the Processor promptly adopts appropriate safeguards (Art. 46 GDPR) or suspends the transfer.*

Art. 7 — Diritti degli interessati / Rights of data subjects

7.1 Il Responsabile mette a disposizione del Titolare strumenti tecnici (pagina /account: export dei dati, cancellazione) per soddisfare le richieste degli interessati ai sensi degli artt. 15-22 GDPR.

7.1 *The Processor makes available to the Controller technical tools (/account page: data export, deletion) to handle data subject requests under Arts. 15-22 GDPR.*

7.2 Se l'interessato si rivolge direttamente al Responsabile, il Responsabile inoltra la richiesta al Titolare senza ingiustificato ritardo, fornendo le informazioni utili.

7.2 *If the data subject contacts the Processor directly, the Processor forwards the request to the Controller without undue delay, providing the relevant information.*

7.3 Il Responsabile non risponde direttamente all'interessato salvo istruzioni del Titolare o obbligo di legge.

7.3 *The Processor does not respond directly to the data subject unless instructed by the Controller or required by law.*

Art. 8 — Violazioni dei dati / Data breaches

8.1 Notifica al Titolare. Il Responsabile notifica al Titolare ogni violazione dei dati personali senza ingiustificato ritardo e comunque entro 24 ore dalla presa di conoscenza, fornendo: (a) descrizione della violazione; (b) categorie e numero approssimativo di interessati e di registrazioni coinvolte; (c) probabili conseguenze; (d) misure adottate o proposte; (e) recapiti del punto di contatto.

8.1 Notification to Controller. *The Processor notifies the Controller of any personal data breach without undue delay and in any case within 24 hours of becoming aware, providing: (a) description of the breach; (b) categories and approximate number of data subjects and records concerned; (c) likely consequences; (d) measures taken or proposed; (e) contact details of the point of contact.*

8.2 Notifica al Garante. La notifica al Garante ai sensi dell'art. 33 GDPR rimane responsabilità del Titolare, supportato dal Responsabile.

8.2 Notification to the Supervisory Authority. *Notification to the Italian Supervisory Authority pursuant to Art. 33 GDPR remains the Controller's responsibility, with the Processor's support.*

8.3 Documentazione. Le parti documentano la violazione, le sue conseguenze e le misure adottate, conformemente all'art. 33(5) GDPR.

8.3 Documentation. *The parties document the breach, its consequences and the measures taken, in accordance with Art. 33(5) GDPR.*

Art. 9 — Audit e ispezioni / Audit and inspections

9.1 Il Responsabile mette a disposizione del Titolare le informazioni necessarie per dimostrare il rispetto degli obblighi del presente DPA.

9.1 The Processor makes available to the Controller the information necessary to demonstrate compliance with this DPA.

9.2 Modalità di audit. Considerata la natura del servizio SaaS multi-tenant, il Responsabile soddisfa l'obbligo di audit fornendo: (a) la documentazione tecnica del trattamento (DPIA, registro, misure di sicurezza); (b) le certificazioni del fornitore di hosting (Infomaniak, ISO 27001); (c) report di penetration test annuale (a partire dal 2027). Su richiesta motivata, il Titolare può chiedere chiarimenti specifici tramite il punto di contatto.

9.2 Audit modalities. Given the multi-tenant SaaS nature of the service, the Processor satisfies the audit obligation by providing: (a) technical documentation of the processing (DPIA, record of processing, security measures); (b) the hosting provider's certifications (Infomaniak, ISO 27001); (c) annual penetration test reports (starting 2027). On reasoned request, the Controller may seek specific clarifications via the point of contact.

9.3 Ispezioni fisiche. Ispezioni fisiche dirette nei datacenter non sono consentite per ragioni di sicurezza multi-tenant; il Responsabile collabora ad audit di terze parti certificate qualora il Titolare lo richieda, a spese del Titolare.

9.3 Physical inspections. Direct physical inspections of datacentres are not permitted for multi-tenant security reasons; the Processor cooperates with certified third-party audits if requested by the Controller, at the Controller's expense.

Art. 10 — Cancellazione e restituzione / Deletion and return

10.1 Al termine del contratto, il Titolare sceglie tra: (a) esportazione dei dati tramite le funzionalità della Piattaforma (pagina /account); (b) cancellazione integrale, effettuata automaticamente al termine di un periodo di grazia di 30 giorni dalla richiesta.

10.1 At contract termination, the Controller chooses between: (a) export of data via the Platform's features (/account page); (b) full deletion, carried out automatically at the end of a 30-day grace period from the request.

10.2 Backup. Le copie residue nei backup cifrati scompaiono secondo il normale ciclo di rotazione (massimo 30 giorni).

10.2 Backups. Residual copies in the encrypted backups disappear under the standard rotation cycle (maximum 30 days).

10.3 Resta salvo l'obbligo di conservazione dei log di cancellazione (account_deletion_log) per 5 anni, ai fini di accountability, in forma anonimizzata.

10.3 The obligation to retain deletion logs (account_deletion_log) for 5 years, for accountability purposes, in anonymised form, remains in force.

Art. 11 — Durata e termine / Term and termination

11.1 Il presente DPA cessa al termine dell'utilizzo della Piattaforma, fatti salvi gli obblighi che sopravvivono per loro natura (sicurezza, cancellazione, riservatezza).

11.1 This DPA ends upon termination of the use of the Platform, without prejudice to obligations surviving by their nature (security, deletion, confidentiality).

11.2 Recesso per causa. Ciascuna parte può recedere per inadempimento grave dell'altra parte agli obblighi del presente DPA, con preavviso scritto di 30 giorni non sanato.

11.2 Termination for cause. Either party may terminate for the other party's material breach of this DPA, with 30 days' written notice not cured.

Art. 12 — Responsabilità / Liability

12.1 Ciascuna parte è responsabile del danno cagionato da un trattamento non conforme al GDPR, ai sensi dell'art. 82 GDPR.

12.1 Each party is liable for damage caused by processing that does not comply with the GDPR, pursuant to Art. 82 GDPR.

12.2 Il Responsabile risponde per i danni causati dal trattamento solo se non ha adempiuto agli obblighi del GDPR specificamente diretti ai responsabili o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare.

12.2 The Processor is liable for damage caused by processing only if it has not complied with GDPR obligations specifically directed at processors or has acted outside or contrary to the Controller's lawful instructions.

12.3 Salva la responsabilità per dolo e colpa grave, la responsabilità complessiva del Responsabile per ogni anno contrattuale è limitata al doppio dei corrispettivi pagati dal Titolare nei 12 mesi precedenti l'evento.

12.3 Save for wilful misconduct and gross negligence, the Processor's aggregate liability for each contract year is limited to twice the fees paid by the Controller in the 12 months preceding the event.

Art. 13 — Cessione del contratto / Assignment

Il Titolare consente, ai sensi degli artt. 1406 ss. del Codice civile italiano, alla cessione del presente DPA da parte del Responsabile a un'entità che subentri nella fornitura della Piattaforma alle stesse condizioni e con continuità di tutte le obbligazioni in materia di protezione dei dati. La cessione è notificata al Titolare con preavviso di 30 giorni e gli dà diritto di recedere senza penali entro 60 giorni dalla notifica.

The Controller consents, pursuant to Arts. 1406 ff. of the Italian Civil Code, to the assignment of this DPA by the Processor to an entity taking over the provision of the Platform under the same conditions and with continuity of all data-protection obligations. The assignment is notified to the Controller with 30 days' notice and entitles the Controller to terminate without penalty within 60 days of notification.

Art. 14 — Foro competente e legge applicabile / Jurisdiction and governing law

14.1 Il presente DPA è regolato dalla legge italiana.

14.1 This DPA is governed by Italian law.

14.2 Per ogni controversia è competente in via esclusiva il foro di Roma, Italia, fatto salvo il foro inderogabile del consumatore o del lavoratore ove applicabile.

14.2 Any dispute is subject to the exclusive jurisdiction of Rome, Italy, subject to the non-derogable jurisdiction of consumer or worker forums where applicable.

Art. 15 — Disposizioni finali / Final provisions

15.1 In caso di conflitto tra il presente DPA e le Condizioni generali della Piattaforma, il presente DPA prevale per quanto riguarda gli aspetti di protezione dei dati.

15.1 In case of conflict between this DPA and the Platform's Terms of Service, this DPA prevails for data-protection matters.

15.2 Eventuali modifiche al presente DPA sono comunicate con preavviso di 30 giorni e si considerano accettate in assenza di opposizione scritta.

15.2 Any amendments to this DPA are communicated with 30 days' notice and are deemed accepted in the absence of written objection.

15.3 Il presente DPA è composto da 15 articoli e 4 allegati (A, B, C, D) che ne formano parte integrante.

15.3 This DPA consists of 15 articles and 4 annexes (A, B, C, D) forming an integral part.

Accettazione / Acceptance

Il presente Accordo costituisce la versione di riferimento del Data Processing Agreement pubblicata e mantenuta dal Responsabile all'indirizzo <https://clinovusai.com/legal/dpa-v1.1.pdf>. È concluso tra le parti in forma elettronica, come consentito dall'art. 28(9) GDPR.

This Agreement constitutes the reference version of the Data Processing Agreement published and maintained by the Processor at <https://clinovusai.com/legal/dpa-v1.1.pdf>. It is concluded between the parties in electronic form, as permitted by Art. 28(9) GDPR.

Modalità di conclusione. Il Titolare accetta il presente Accordo alla creazione del proprio account su clinovusai.com, spuntando la casella di accettazione delle Condizioni generali, che rinvia espressamente al presente DPA con link diretto al PDF. L'accettazione è registrata dal Responsabile con: (i) data e ora UTC, (ii) indirizzo IP del Titolare, (iii) versione del DPA accettata e sua impronta SHA-256.

Method of conclusion. The Controller accepts this Agreement upon creating their account on clinovusai.com, by ticking the acceptance box of the Terms of Service, which expressly refers to this DPA with a direct link to the PDF. The acceptance is recorded by the Processor with: (i) UTC date and time, (ii) the Controller's IP address, (iii) the accepted DPA version and its SHA-256 fingerprint.

Versionamento e modifiche. Il Responsabile può aggiornare il presente DPA pubblicando una nuova versione. Le modifiche sono comunicate al Titolare per e-mail con preavviso di 30 giorni, durante i quali il Titolare può esercitare il diritto di recesso. Le versioni precedenti restano pubblicate e disponibili su richiesta a dpo@clinovusai.com.

Versioning and amendments. The Processor may update this DPA by publishing a new version. Amendments are notified to the Controller by email 30 days in advance, during which the Controller may exercise the right to terminate. Previous versions remain published and are available on request at dpo@clinovusai.com.

Integrità del documento. L'impronta SHA-256 della versione di riferimento è pubblicata all'indirizzo <https://clinovusai.com/legal/dpa-v1.1.pdf.sha256>, per consentire al Titolare di verificare l'integrità del documento accettato.

Document integrity. The SHA-256 fingerprint of the reference version is published at <https://clinovusai.com/legal/dpa-v1.1.pdf.sha256> so that the Controller can verify the integrity of the accepted document.

Versione di riferimento / Reference version	v1.1 — 05.10.2026
URL pubblicato / Published URL	https://clinovusai.com/legal/dpa-v1.1.pdf
Titolare / Controller	medico utilizzatore, identificato dai dati dell'account / physician using the service, identified by account data
Responsabile / Processor	Plancherel Solutions — Canton Vaud, Svizzera — Jean-Paul Plancherel
IDI svizzero / Swiss UID	CHE-379.895.072
Contatto protezione dati / Data protection contact	dpo@clinovusai.com
Forma di conclusione / Method	accettazione elettronica (click-wrap), art. 28(9) GDPR / electronic click-wrap acceptance, Art. 28(9) GDPR

Allegato A — Descrizione del trattamento / Annex A — Description of processing

Finalità / Purpose	Supporto al medico nella redazione della documentazione clinica a partire dalla sua dettatura o dal materiale da lui fornito, trascrizione audio, consultazione di fonti e chat IA. / Support for the physician in drafting clinical documentation from their dictation or material, audio transcription, consultation of sources and AI chat.
Natura / Nature	Trattamento automatizzato tramite IA generativa, riconoscimento vocale (ASR) e ricerca documentale (RAG). / Automated processing via generative AI, speech recognition (ASR) and document retrieval (RAG).
Durata / Duration	Durata dell'utilizzo della Piattaforma da parte del Titolare. / Duration of the Controller's use of the Platform.
Tipologie di dati / Data types	Identificativi, dati sanitari, audio, trascrizioni, richieste all'IA, documenti. / Identification data, health data, audio, transcripts, AI prompts, documents.
Categorie particolari / Special categories	Sì — dati relativi alla salute (art. 9 GDPR). / Yes — health data (Art. 9 GDPR).
Interessati / Data subjects	Pazienti del Titolare. / Patients of the Controller.
Conservazione / Retention	Audio delle consultazioni: cancellato automaticamente 30 giorni dopo la registrazione. Documenti esportati e allegati: 90 giorni. Cestino: 30 giorni. Conversazioni, trascrizioni e note: finché l'account è attivo. Backup cifrati: 30 giorni. / Consultation audio: automatically deleted 30 days after recording. Exported documents and attachments: 90 days. Trash: 30 days. Conversations, transcripts and notes: while the account is active. Encrypted backups: 30 days.
Cancellazione / Deletion	Cancellazione integrale automatica al termine di un periodo di grazia di 30 giorni dalla richiesta. / Automatic full deletion at the end of a 30-day grace period from the request.

Allegato B — Lista sub-responsabili / Annex B — List of sub-processors

Sub-responsabile / Sub-processor	Sede / Location	Finalità / Purpose	Base del trasferimento / Transfer basis
Infomaniak Network SA	Ginevra, CH	Hosting dei server, backup cifrati, API del modello IA, invio delle e-mail del servizio / Server hosting, encrypted backups, AI model API, sending of service emails	Adeguatezza CH / CH adequacy
Stripe Payments Europe, Ltd.	Dublino, IE	Pagamenti dell'abbonamento del medico (nessun dato dei pazienti) / Payment of the physician's subscription (no patient data)	UE; verso gli USA: DPF UE-USA e clausole tipo / EU; to the US: EU-US DPF and standard clauses

Ultimo aggiornamento / Last update: 05.10.2026. Modifiche con preavviso di 30 giorni (art. 5.2). Rispetto alla versione 1.0, Google Ireland Ltd. (GA4) e Microsoft Ireland Operations Ltd. (Clarity) sono stati rimossi: nessuno dei due è utilizzato. / Compared to version 1.0, Google Ireland Ltd. (GA4) and Microsoft Ireland Operations Ltd. (Clarity) have been removed: neither is used.

Allegato C — Misure di sicurezza / Annex C — Security measures

Le misure tecniche e organizzative adottate dal Responsabile ai sensi dell'art. 32 GDPR sono descritte qui di seguito; il dettaglio figura nel documento DPIA (CLINOVUS-DPIA-2026-001).

The technical and organisational measures adopted by the Processor under Art. 32 GDPR are described below; details are in the DPIA document (CLINOVUS-DPIA-2026-001).

Cifratura / Encryption	In transito: TLS 1.3 e HSTS. A riposo: volumi dati cifrati LUKS2 (AES-XTS) sui server che ospitano dati dei pazienti, sbloccati automaticamente all'avvio tramite server di chiavi interni; backup cifrati (AES-256). / In transit: TLS 1.3 and HSTS. At rest: LUKS2 (AES-XTS) encrypted data volumes on the servers holding patient data, unlocked at boot through internal key servers; encrypted backups (AES-256).
Autenticazione / Authentication	Password con hash (bcrypt); autenticazione a due fattori (TOTP) disponibile; token di accesso di 12 ore; sessione chiusa dopo 30 giorni di inattività; token verificato a ogni richiesta su due livelli indipendenti. / Hashed passwords (bcrypt); two-factor authentication (TOTP) available; 12-hour access tokens; session closed after 30 days of inactivity; token verified on every request at two independent layers.
Accesso amministrativo / Administrative access	Solo tramite chiavi SSH, da indirizzi autorizzati; firewall con blocco predefinito a livello di rete e di server; servizi eseguiti con account dedicati a privilegi minimi. / SSH keys only, from authorised addresses; default-deny firewall at network and server level; services run under dedicated least-privilege accounts.
Isolamento / Isolation	Isolamento logico per account: ogni accesso a una risorsa verifica che appartenga al medico autenticato; Row Level Security PostgreSQL sulle tabelle esposte. / Logical isolation per account: every access to a resource checks that it belongs to the authenticated physician; PostgreSQL Row Level Security on exposed tables.
Limitazione del traffico / Rate limiting	Limiti per indirizzo su autenticazione, API, caricamenti e trascrizione. / Per-address limits on authentication, API, uploads and transcription.
Registri / Logs	Registri di sistema e di accesso conservati 90 giorni; registro applicativo delle operazioni sensibili (audit_log). / System and access logs kept for 90 days; application log of sensitive operations (audit_log).
Backup	Due volte al giorno, cifrati, conservati 30 giorni; ripristino verificato. / Twice daily, encrypted, kept for 30 days; restoration verified.
Aggiornamenti / Updates	Aggiornamenti di sicurezza del sistema applicati automaticamente, con riavvio programmato. / System security updates applied automatically, with scheduled reboot.
Monitoraggio / Monitoring	Controlli funzionali automatici ogni ora (autenticazione, trascrizione, generazione dei documenti, export e cancellazione) con allerta per e-mail. / Automatic hourly functional checks (authentication, transcription, document generation, export and deletion) with email alerting.
Cancellazione / Deletion	Procedura automatizzata giornaliera: cancellazione degli account a 30 giorni dalla richiesta e purge per età (audio 30 giorni, documenti e allegati 90 giorni, cestino 30 giorni). / Automated daily procedure: account deletion 30 days after the request and age-based purge (audio 30 days, documents and attachments 90 days, trash 30 days).
Uso dei dati / Data use	I dati non sono mai utilizzati per addestrare modelli di intelligenza artificiale. / Data is never used to train artificial intelligence models.
Contatto / Contact	Punto di contatto per la protezione dei dati: dpo@clinovusai.com. / Data protection point of contact: dpo@clinovusai.com.

Allegato D — Modifiche rispetto alla versione 1.0 / Annex D — Changes from version 1.0

- Nome del Responsabile: «Plancherel Solutions» (senza suffisso).
- *Processor's name: "Plancherel Solutions" (no suffix).*
- Finalità: redazione della documentazione a partire dalla dettatura del medico; la Piattaforma non è un dispositivo medico e non supporta decisioni diagnostiche o terapeutiche.

- *Purpose: drafting documentation from the physician's dictation; the Platform is not a medical device and does not support diagnostic or therapeutic decisions.*
- Allegato B: rimossi Google (GA4) e Microsoft (Clarity), non utilizzati; precisato il perimetro di Infomaniak e di Stripe.
- *Annex B: Google (GA4) and Microsoft (Clarity), not used, removed; scope of Infomaniak and Stripe clarified.*
- Art. 6: unico trasferimento possibile, i dati di fatturazione del medico tramite Stripe.
- *Art. 6: the only possible transfer is the physician's billing data via Stripe.*
- Allegato C: misure descritte come effettivamente in funzione; cifratura a riposo tramite volumi LUKS2 (in luogo di «PostgreSQL TDE»); autenticazione a due fattori disponibile (non obbligatoria); rimossi firewall applicativo, antivirus sugli upload, filtri di iniezione e servizio di monitoraggio esterno, non in funzione.
- *Annex C: measures described as actually in place; encryption at rest through LUKS2 volumes (instead of "PostgreSQL TDE"); two-factor authentication available (not mandatory); application firewall, upload antivirus, injection filters and external monitoring service, not in place, removed.*
- Allegato A: aggiunte le durate di conservazione, tra cui l'audio delle consultazioni (30 giorni).
- *Annex A: retention periods added, including consultation audio (30 days).*
- Art. 13: clausola di cessione generica, senza indicazione di una società.
- *Art. 13: generic assignment clause, without naming a company.*
- Contatto: punto di contatto per la protezione dei dati (nessun DPO designato).
- *Contact: data protection point of contact (no DPO designated).*