

# Nomina a responsabile del trattamento ex art. 28 GDPR

- Versione: 1.4
- Ultimo aggiornamento: 2026-06-10

## Parti

Titolare del trattamento

Il professionista, studio o organizzazione che accetta i documenti ClinLoom e usa il servizio con il proprio

account su invito, identificato dai dati forniti in fase di invito, registrazione o accettazione.

Responsabile del trattamento

Michele Gaeta, operante il servizio ClinLoom come persona fisica

Via Val d'Ala 20, 00141 Roma, Italia

Email: michele.gaeta.90@gmail.com

## 1. Oggetto

Il Titolare nomina Michele Gaeta, operante il servizio ClinLoom, quale responsabile del trattamento ai sensi

dell'art. 28 GDPR per i trattamenti necessari all'erogazione di ClinLoom.

ClinLoom e' un servizio di documentazione clinica per psicologi e psicoterapeuti. Il servizio aiuta a

trascrivere, organizzare e preparare bozze di note cliniche da revisionare e approvare dal professionista.

Il Responsabile tratta dati personali esclusivamente su istruzioni documentate del Titolare e nei limiti

necessari a fornire, mantenere e proteggere il servizio.

ClinLoom non e' destinato a essere l'unico archivio della documentazione clinica. Il Titolare resta responsabile

della conservazione della cartella clinica o documentazione professionale secondo i propri obblighi.

## 2. Durata

La nomina resta efficace per la durata dell'accesso del Titolare a ClinLoom e fino alla cancellazione o

restituzione dei dati trattati per conto del Titolare, salvo obblighi di legge.

## 3. Natura e finalita' del trattamento

#### **Elemento | Descrizione**

Natura | raccolta, registrazione, conservazione, cifratura, trascrizione, pseudonimizzazione, organizzazione, generazione di bozze documentali, visualizzazione, modifica, esportazione/cancellazione su istruzione

Finalita' | supporto organizzativo alla documentazione clinica del Titolare; preparazione di bozze di note cliniche da revisionare e approvare

Mezzi principali | applicazione web, database cifrato, storage cifrato, worker asincrono, fornitori AI/STT autorizzati

Localizzazione | dati clinici e inferenza AI in UE/SEE per i provider attivi indicati nella Lista subprocessori ClinLoom

Il servizio non deve essere usato per decisioni cliniche automatizzate, diagnosi automatica, emergenze, triage o raccomandazioni terapeutiche individualizzate.

## **4. Categorie di dati personali**

Il trattamento puo' riguardare:

- categorie particolari di dati ai sensi dell'art. 9 GDPR, inclusi dati relativi alla salute, dati psicologici

e psicoterapeutici, note cliniche, trascrizioni, sintesi, allegati e registrazioni audio;

- dati identificativi minimizzati del paziente, normalmente nome o pseudonimo interno;
- dati di terzi eventualmente menzionati nella documentazione clinica;
- dati del terapeuta/utente, inclusi account, accessi e metadati operativi;
- metadati tecnici necessari a sicurezza, audit e funzionamento, senza contenuti clinici in chiaro ove

ragionevolmente evitabile.

## **5. Categorie di interessati**

- pazienti/clienti del Titolare;
- terapeuti, collaboratori o utenti autorizzati dal Titolare;
- familiari, partner, medici, datori di lavoro o altri terzi eventualmente menzionati dal Titolare nei contenuti.

## **6. Istruzioni e dichiarazioni del Titolare**

Le istruzioni documentate del Titolare derivano da:

- presenti termini e documenti accettati;
- impostazioni dell'account;
- azioni effettuate nell'applicazione;
- richieste documentate inviate via email;
- eventuali istruzioni aggiuntive scritte accettate dal Responsabile.

Il Responsabile informa il Titolare se ritiene che un'istruzione violi il GDPR o altra normativa applicabile.

Accettando la presente nomina, il Titolare dichiara e si impegna a:

- agire come titolare del trattamento per i dati dei propri pazienti, fornendo loro l'informativa e

individuando la base giuridica, incluso il consenso esplicito per l'elaborazione tramite IA esterna

(modulo di supporto: MODULO\_PAZIENTE\_CONSENSO\_IA.md);

- registrare nell'applicazione lo stato del consenso IA di ciascun paziente prima di caricare

materiale da elaborare;

- minimizzare i dettagli identificativi non necessari nei resoconti vocali e nei materiali importati.

Il Titolare prende atto che i resoconti audio e i documenti importati raggiungono i fornitori AI/STT

autorizzati nella loro forma integrale: la pseudonimizzazione opera sul testo trascritto, prima della

sintesi, non sull'audio o sui file originali.

## **7. Obblighi del Responsabile**

Il Responsabile si impegna a:

- trattare i dati solo su istruzioni documentate del Titolare;
- garantire che le persone autorizzate al trattamento siano vincolate alla riservatezza;
- adottare misure tecniche e organizzative adeguate ai sensi dell'art. 32 GDPR;
- non usare dati clinici per training, miglioramento prodotto, analytics, benchmarking o finalità proprie;
- assistere il Titolare, nei limiti ragionevoli, con richieste degli interessati, sicurezza, DPIA e consultazione preventiva;
- notificare al Titolare violazioni di dati personali senza ingiustificato ritardo e comunque entro 72 ore dalla conoscenza;
- mettere a disposizione informazioni ragionevoli per dimostrare la conformità della presente nomina;
- cancellare o restituire i dati alla cessazione o su istruzione del Titolare, salvo obblighi di legge.

## **8. Riservatezza e segreto professionale**

Il Responsabile riconosce che i dati trattati possono essere soggetti a segreto professionale del terapeuta.

Il Responsabile tratta tali informazioni come confidenziali, limita l'accesso al necessario e impone obblighi

equivalenti ai subprocessori che possano accedere ai dati.

## **9. Subprocessori**

Il Titolare autorizza il Responsabile a ricorrere ai subprocessori elencati nella Lista subprocessori ClinLoom.

Il Responsabile impone ai subprocessori obblighi sostanzialmente equivalenti a quelli

della presente nomina,

includere riservatezza, sicurezza, no-training per dati clinici e assistenza al Responsabile.

Stato corrente:

- Google Cloud Vertex AI e' subprocessore attivo per AI/STT/OCR in configurazione UE.

Il Responsabile comunica modifiche sostanziali alla lista dei subprocessori con almeno 14 giorni di preavviso,

salvo urgenze di sicurezza o continuita' operativa. Qualora un subprocessore a monte notifichi al Responsabile

una modifica che incide sui dati del Titolare con un preavviso inferiore a 14 giorni, il Responsabile fornisce

al Titolare il maggior preavviso ragionevolmente possibile nelle circostanze. Il Titolare puo' opporsi per

fondati motivi di protezione dati. In caso di opposizione non risolta, il Titolare puo' cessare l'uso del servizio.

## **10. Trasferimenti**

Il Responsabile configura il servizio affinche' i dati clinici siano trattati in UE/SEE per i provider attivi

indicati come tali nella lista subprocessori.

Trasferimenti verso paesi terzi sono ammessi solo se:

- necessari al servizio autorizzato;
- indicati nella lista subprocessori o in una comunicazione specifica;
- assistiti da garanzie adeguate ai sensi del Capo V GDPR, ove richiesto.

## **11. Misure tecniche e organizzative**

Misure minime:

- TLS per dati in transito;
- cifratura a riposo per identita' paziente, audio, trascrizioni, note, allegati e segreti;
- isolamento logico per account/terapeuta;
- controlli di accesso e principio del privilegio minimo;
- password con hashing robusto e 2FA dove disponibile;
- audit log senza contenuti clinici in chiaro nei metadati;
- pseudonimizzazione prima dell'invio all'AI quando tecnicamente disponibile;
- backup cifrati dove configurati;
- logging tecnico minimizzato;
- gestione patch e vulnerabilita'.

## **12. Richieste degli interessati**

Il Titolare e' responsabile di rispondere ai pazienti. Il Responsabile assiste il Titolare con gli strumenti disponibili o, nella fase attuale, con procedure manuali ragionevoli.

Se il Responsabile riceve direttamente una richiesta relativa a dati clinici, informa il Titolare senza ingiustificato ritardo, salvo divieti di legge.

### **13. Cancellazione e restituzione**

Su istruzione del Titolare o alla cessazione del rapporto, il Responsabile cancella o restituisce i dati clinici secondo istruzioni documentate del Titolare e secondo le regole di conservazione applicabili, salvo obblighi di legge o backup tecnici destinati a cancellazione automatica nel ciclo di rotazione.

### **14. Audit e documentazione**

Il Responsabile mette a disposizione informazioni ragionevoli per dimostrare la conformita'. Audit o ispezioni devono essere concordati con preavviso ragionevole, non compromettere sicurezza o segreti commerciali e possono essere soddisfatti tramite documentazione, report, certificazioni o risposte scritte, salvo necessita' specifiche.

### **15. Responsabilita'**

La responsabilita' delle parti e' disciplinata dal GDPR, dai Termini di servizio e dalle norme inderogabili applicabili.

### **16. Accettazione elettronica**

La presente nomina puo' essere accettata elettronicamente. ClinLoom conserva prova dell'accettazione, inclusi utente, email, timestamp, IP, versione dei documenti e l'hash SHA-256 della versione accettata (colonna legal\_acceptances.documents\_hash).