Allegato 2 — Misure tecniche e organizzative

Allegato all'Accordo per il trattamento dei dati (art. 28 GDPR) versione 2.0 — Allegato versione 2.1, in vigore dall'11 ottobre 2026

1. Premessa

Questo allegato descrive le misure tecniche e organizzative che LIME TIME SOFTWARE S.L. applica, come responsabile del trattamento (art. 28 GDPR), ai dati personali trattati per conto del Titolare tramite Open Kanino.

Voce	Dettaglio
Responsabile del trattamento	LIME TIME SOFTWARE S.L., CIF B76267442, C/ Rambla Pedro Lezcano Montalvo nº 4, Local 4, 35200 Telde (Las Palmas), Spagna
Titolare del trattamento ("Titolare")	Lo studio, il professionista o la società che utilizza Open Kanino
Riferimento normativo	Art. 32 Regolamento (UE) 2016/679 (GDPR); Ley Orgánica 3/2018 (LOPDGDD)
Documento	Allegato 2 all'Accordo per il trattamento dei dati, versione 2.1
Contatto privacy	privacy@openkanino.it
Responsabile della protezione dei dati (DPO)	Isabella Lopes, isabellalopesdpo@gmail.com

Aggiornamento delle misure. Il Responsabile può aggiornare le misure descritte in questo allegato per adeguarle all'evoluzione tecnologica e ai rischi, a condizione che il livello di sicurezza complessivo non venga ridotto. La versione in vigore è pubblicata sul sito ufficiale di Open Kanino, come allegato ai Termini del servizio (https://www.openkanino.it/terms-and-conditions), e ogni modifica rilevante viene comunicata al Titolare.

2. Infrastruttura e localizzazione dei dati

Tutti i dati dei pazienti sono trattati e conservati nell'Unione Europea, nel data center DigitalOcean di Amsterdam (Paesi Bassi, regione AMS3), su server virtuali DigitalOcean (Droplet) utilizzati unicamente per l'erogazione del servizio Open Kanino.

Componente	Contenuto	Dove	Protezione a riposo
Server applicativo	Codice dell'applicazione	DigitalOcean, Amsterdam	Solo dati tecnici temporanei (sessioni, log)
Database	Anagrafiche, agenda, piani di cura, diario clinico, preventivi, fatture, pagamenti	Server del database MySQL, DigitalOcean, Amsterdam, con replica in tempo reale su un secondo server nella stessa rete privata	Cifrato (dati su volumi di archiviazione cifrati)

Componente	Contenuto	Dove	Protezione a riposo
Archivio file	Immagini diagnostiche, documenti, allegati, PDF generati	Volume di archiviazione a blocchi DigitalOcean, Amsterdam	Cifrato
Server messaggistica WhatsApp	Coda dei messaggi in uscita	Server interno, DigitalOcean, Amsterdam	—
Backup	Copie di database e file	DigitalOcean, Amsterdam	Copie del database cifrate; conservazione massima 7 giorni

I server non sono gestiti in locali di Lime Time Software: la sicurezza fisica dei data center è garantita da DigitalOcean.

Certificazioni	Ambito
ISO/IEC 27001, ISO 22301, ISO 9001, SOC 1, SOC 2 e SOC 3 Type II, PCI-DSS	Data center AMS3 di Amsterdam, dove risiedono i dati
SOC 2 Type II, SOC 3 Type II, CSA STAR Level 1	DigitalOcean come fornitore di servizi cloud

Il traffico verso l'applicazione passa attraverso Cloudflare, che filtra gli attacchi informatici prima che raggiungano i server. I dati dei pazienti non vengono conservati su computer o supporti rimovibili del personale.

3. Riservatezza (art. 32, par. 1, lett. b)

L'accesso ai dati è consentito solo agli utenti autenticati e autorizzati del Titolare e, per attività di manutenzione, assistenza tecnica e sicurezza, al personale autorizzato del Responsabile. Le persone autorizzate dal Responsabile al trattamento si sono impegnate alla riservatezza o sono soggette a un adeguato obbligo legale di riservatezza (art. 28, par. 3, lett. b GDPR).

Accesso fisico. I server si trovano nei data center di DigitalOcean, con accesso fisico controllato dal fornitore. Lime Time Software non gestisce sale server proprie.

Accesso all'applicazione

- Accesso con utente e password personali; non sono previste credenziali condivise.
- Password memorizzate solo come hash bcrypt, mai in chiaro né con algoritmi reversibili.
- Regole minime verificate dal server: almeno 9 caratteri, lettere e numeri, divieto di riutilizzare la password attuale o le ultime 5.
- Scadenza della password dopo 90 giorni, con avviso all'utente.
- Autenticazione a due fattori disponibile per tutti gli utenti, tramite app di autenticazione (TOTP, es. Google Authenticator).
- Blocco dello schermo per inattività, con sblocco tramite password.
- Protezione delle sessioni contro richieste da siti esterni (controllo dell'origine delle richieste).

Accesso ai dati

- Ruoli e livelli di accesso per gli operatori del Titolare, impostati dall'account principale.
- Possibilità di limitare pagina per pagina le sezioni visibili a ciascun operatore.
- Nessun accesso diretto al database da parte degli utenti.
- Accesso tecnico ai server solo per il personale autorizzato del Responsabile, tramite connessione cifrata (SSH).

Separazione dei dati tra studi. Il servizio è condiviso tra più studi (multi-tenant): ogni dato è associato al Titolare e l'applicazione verifica questa appartenenza in lettura e scrittura. I file di ciascuno studio sono conservati in cartelle separate. L'ambiente di test usa un database distinto da quello di produzione e contiene solo dati fittizi o anonimizzati.

4. Cifratura e pseudonimizzazione (art. 32, par. 1, lett. a)

I dati sono cifrati sia durante la trasmissione sia a riposo; le password sono protette con hash bcrypt.

Ambito	Misura
Trasmissione browser – server	HTTPS con TLS su tutte le pagine e le chiamate dell'applicazione
Accesso tecnico ai server	SSH
Database, replica e copie del database	Volumi di archiviazione DigitalOcean cifrati a riposo; copie del database cifrate
Immagini, documenti, allegati, PDF	Volume di archiviazione DigitalOcean cifrato a riposo
Password degli utenti	Hash bcrypt con salt casuale
Codici di verifica per la 2FA	Conservati con hash, monouso

Limiti. Le email inviate ai pazienti (es. promemoria) viaggiano cifrate fino al fornitore di posta, ma la loro consegna finale dipende dal server di posta del destinatario. I messaggi WhatsApp sono gestiti dal servizio WhatsApp con la cifratura prevista dal servizio stesso.

Pseudonimizzazione. I dati clinici devono restare riconducibili al paziente per la finalità di cura, quindi non sono pseudonimizzati nell'applicazione. I nomi delle cartelle dei file non contengono dati identificativi del paziente.

5. Integrità (art. 32, par. 1, lett. b)

I dati sono protetti da accessi e modifiche non autorizzati durante la trasmissione, e l'applicazione registra gli accessi, chi crea o modifica i dati principali e chi li cancella.

Trasmissione. Tra il Titolare e Open Kanino i dati viaggiano solo su connessioni cifrate (sezione 4). Non sono previsti scambi di dati tramite supporti fisici o spedizioni. Eventuali migrazioni da precedenti gestionali, su richiesta del Titolare, avvengono con modalità concordate per iscritto che garantiscono un livello di protezione adeguato.

Registrazione delle operazioni

- Indicazione dell'operatore che ha inserito o modificato i dati principali (pazienti, piani di cura, preventivi, fatture).

- Controllo che i dati inviati appartengano al Titolare che li salva (es. il paziente collegato a un appuntamento): i tentativi non validi vengono rifiutati e registrati.

Log di accesso e sicurezza

L'applicazione registra gli accessi e gli eventi di autenticazione e sicurezza, associando, ove disponibili e pertinenti, l'identificativo dell'utente, la data e l'ora dell'evento, l'indirizzo IP, le informazioni relative al dispositivo o alla sessione e l'esito del tentativo di autenticazione.

- I log di accesso e sicurezza sono conservati per un periodo massimo di 12 mesi dalla relativa registrazione, per finalità di sicurezza dei sistemi e dei dati, prevenzione e individuazione di accessi anomali o non autorizzati, analisi e ricostruzione di eventuali incidenti di sicurezza e tutela dei diritti del Titolare e del Responsabile. Decorso tale periodo, i log sono cancellati o resi anonimi, salvo che la loro ulteriore conservazione sia necessaria in relazione a uno specifico incidente di sicurezza, a una richiesta o provvedimento dell'autorità competente, all'adempimento di un obbligo di legge oppure all'accertamento, esercizio o difesa di un diritto. In tali casi, la conservazione ulteriore è limitata ai dati pertinenti e al periodo strettamente necessario alla relativa finalità.
- La cessazione del rapporto contrattuale o la chiusura dell'account non comportano la cancellazione anticipata dei log ancora compresi nel periodo di conservazione sopra indicato, né determinano la decorrenza di un nuovo periodo di conservazione.
- L'accesso ai log è limitato al personale autorizzato secondo le rispettive funzioni e necessità operative. I log sono sottoposti a misure tecniche e organizzative adeguate volte a proteggerli da accessi, alterazioni, divulgazioni o cancellazioni non autorizzati.
- I log di accesso e sicurezza sono mantenuti distinti, per quanto tecnicamente applicabile, dai contenuti clinici trattati attraverso il servizio e sono limitati alle informazioni necessarie al perseguimento delle finalità sopra indicate.

Registro delle eliminazioni

Funzione facoltativa, disattivata per impostazione predefinita. Se il Titolare la attiva, l'applicazione registra automaticamente le cancellazioni dei dati principali eseguite nel suo account (es. pazienti, appuntamenti, piani di cura, diario clinico, anamnesi, preventivi, fatture, pagamenti, documenti e immagini collegati), per consentire al Titolare di sapere chi ha cancellato cosa e di recuperare i dati cancellati per errore.

- La funzione può essere attivata solo dall'account principale del Titolare, previa dichiarazione di aver informato il personale dello studio che le cancellazioni vengono registrate con l'indicazione dell'operatore. La dichiarazione è conservata con data, ora, utente e indirizzo IP. Il Titolare può disattivare la funzione in qualsiasi momento: la registrazione si interrompe e le voci già presenti restano fino alla scadenza del periodo di conservazione.
- Per ogni cancellazione vengono registrati la data e l'ora, l'operatore che l'ha eseguita, la provenienza (applicazione, agenda, interfaccia di programmazione o procedura automatica), il tipo di dato, il paziente collegato e una copia del dato cancellato.
- Il registro è consultabile solo dall'account principale del Titolare e, per attività di assistenza richieste dal Titolare, dal personale autorizzato del Responsabile. Gli altri operatori non possono consultarlo.
- Le voci del registro non possono essere modificate o cancellate dall'applicazione. Il Titolare può oscurare il contenuto di una singola voce o di tutte le voci relative a un paziente, ad esempio per dare seguito a una richiesta di cancellazione dell'interessato (art. 17 GDPR): la copia del dato viene eliminata, resta solo l'indicazione dell'evento (data, operatore, tipo di dato) e l'oscuramento stesso viene registrato. La cancellazione completa di singole voci è eseguita dal Responsabile solo su richiesta scritta del Titolare.
- Le voci sono conservate per 12 mesi dalla registrazione e poi cancellate automaticamente. Alla chiusura dell'account il registro è cancellato insieme agli altri dati del Titolare (sezione 9).

6. Disponibilità e resilienza (art. 32, par. 1, lett. b, c e d)

I dati vengono salvati ogni giorno e possono essere ripristinati in caso di guasto o perdita; i backup restano nel data center di Amsterdam.

Misura	Dettaglio
Backup del server	Giornaliero (servizio di backup DigitalOcean)
Archivio file	Snapshot del volume di archiviazione
Conservazione dei backup	Fino a 7 giorni, poi cancellati automaticamente
Snapshot prima degli aggiornamenti	Copia completa del server prima di ogni intervento rilevante
Infrastruttura	Data center DigitalOcean con alimentazione di continuità e ridondanza dei componenti
Database	Replica in tempo reale su un secondo server nella stessa rete privata di Amsterdam; copia completa del database ogni 6 ore, cifrata e conservata al massimo 7 giorni; ripristino da replica o dall'ultima copia disponibile
Prove di ripristino	Effettuate 3–4 volte l'anno, durante finestre di manutenzione programmate; l'ultima a fine settembre 2026
Protezione della rete	Tre livelli: Cloudflare (filtro degli attacchi e protezione DDoS), firewall di rete DigitalOcean e firewall del server; sono aperti solo l'accesso web e l'accesso tecnico cifrato (SSH)
Aggiornamenti	Aggiornamenti dell'applicazione verificati prima su un ambiente di test
Esportazione da parte del Titolare	Backup completo scaricabile in qualsiasi momento (sezione 9)

7. Gestione degli incidenti e delle violazioni

In caso di violazione dei dati personali, il Responsabile informa il Titolare senza ingiustificato ritardo e comunque entro 24 ore da quando ne viene a conoscenza. Qualora, al momento della prima comunicazione, non siano ancora disponibili tutte le informazioni necessarie, il Responsabile comunica le informazioni ragionevolmente disponibili in quel momento e fornisce quelle ulteriori in fasi successive, senza ulteriore ingiustificato ritardo, non appena disponibili.

1. **Rilevazione e contenimento dell'incidente.** Il Responsabile adotta le misure tecniche e organizzative ragionevolmente necessarie e appropriate alle circostanze per rilevare e contenere l'incidente, limitarne gli effetti e prevenire, per quanto possibile, ulteriori conseguenze.
2. **Analisi dell'incidente.** Il Responsabile svolge le verifiche ragionevolmente necessarie per determinarne, per quanto possibile, la natura e le cause, le categorie di dati personali coinvolti, i Titolari interessati, le categorie e il numero approssimativo degli interessati e delle registrazioni di dati personali coinvolte, nonché le possibili conseguenze della violazione.
3. **Comunicazione ai Titolari interessati.** Il Responsabile comunica la violazione a ciascun Titolare interessato e fornisce, nella misura in cui siano disponibili, le informazioni di cui all'art. 33, paragrafo 3,

GDPR, nonché ogni ulteriore informazione ragionevolmente necessaria per consentire al Titolare di valutare gli adempimenti conseguenti alla violazione.

4. **Assistenza al Titolare.** Il Responsabile, tenendo conto della natura del trattamento e delle informazioni a propria disposizione, assiste il Titolare ai fini dell'adempimento degli obblighi previsti dagli artt. 33 e 34 GDPR. La valutazione circa la necessità di notificare la violazione all'autorità di controllo o di comunicarla agli interessati, nonché i relativi adempimenti, resta di competenza del Titolare.
5. **Misure correttive e documentazione dell'incidente.** Il Responsabile adotta le misure ragionevolmente appropriate per contenere e mitigare gli effetti della violazione e, ove possibile e nell'ambito del proprio ragionevole controllo, individuarne e rimuoverne o correggerne la causa. Il Responsabile conserva adeguata documentazione relativa all'incidente, alle verifiche effettuate e alle misure adottate, nella misura necessaria a documentare la propria gestione dell'incidente e a fornire al Titolare le informazioni necessarie per l'adempimento dei propri obblighi ai sensi della normativa applicabile.

Le segnalazioni vanno inviate a privacy@openkanino.it.

8. Misure organizzative

I dati sono trattati solo su istruzione documentata del Titolare, da personale vincolato alla riservatezza e con sub-responsabili scelti e controllati per iscritto.

- **Istruzioni del Titolare.** Nessun trattamento oltre a quello necessario per erogare il servizio e a quanto previsto dall'Accordo.
- **Personale.** L'accesso tecnico ai dati è riservato a un numero minimo di persone autorizzate, vincolate da un accordo di riservatezza e informate sugli obblighi del GDPR e della LOPDGDD.
- **Lavoro da remoto.** Il personale lavora da remoto con dispositivi protetti da password e disco cifrato; l'accesso ai server avviene solo tramite connessione cifrata.
- **Responsabile della protezione dei dati.** Isabella Lopes, isabellalopesdpo@gmail.com.
- **Sub-responsabili.** Scelti verificando le garanzie offerte, vincolati da un accordo scritto con obblighi equivalenti a quelli di questo Accordo, elencati nell'Allegato 3 con sede, luogo del trattamento e strumento di trasferimento. Ogni modifica è comunicata al Titolare con almeno 30 giorni di preavviso.
- **Assistenza al Titolare.** Supporto per le richieste degli interessati, le valutazioni d'impatto e le verifiche previste dall'Accordo.
- **Certificazioni.** Lime Time Software non possiede attualmente certificazioni ISO/IEC 27001; si avvale di un fornitore di infrastruttura certificato (sezione 2).

9. Esportazione e cancellazione dei dati

Il Titolare può scaricare in ogni momento tutti i propri dati e, alla chiusura dell'account, i dati vengono distrutti entro 7 giorni dalla conferma, backup compresi entro i 7 giorni successivi.

Esportazione. Dall'account principale, in *Impostazioni → Account*, il Titolare scarica un backup completo: pazienti, piani di cura, diario clinico, preventivi, fatture, agenda e le altre tabelle in formato XML; immagini diagnostiche e documenti in un archivio ZIP. L'esportazione è disponibile per tutta la durata del contratto, senza costi aggiuntivi.

Cancellazione a fine rapporto

1. Il Titolare richiede la cancellazione dell'account dall'applicazione.
2. L'account passa in modalità cancellazione: l'accesso resta possibile solo per confermare l'operazione.

3. Il Titolare riceve via email un codice di conferma.
4. Inserito il codice, il personale del Responsabile distrugge l'account e tutti i dati collegati (database e file) entro 7 giorni.
5. Le copie nei backup e negli snapshot vengono cancellate automaticamente entro i successivi 7 giorni.
6. Il Titolare riceve un'email di conferma dell'avvenuta cancellazione.

Sono conservati oltre questi termini solo i log di accesso e sicurezza, per il periodo indicato nella sezione 5, e i dati che il Responsabile deve tenere per obbligo di legge (es. le fatture emesse al Titolare per l'abbonamento), per il tempo previsto dalla legge. Il registro delle eliminazioni (sezione 5) è cancellato insieme agli altri dati dell'account.

10. Protezione fin dalla progettazione e riesame (art. 25 e art. 32, par. 1, lett. d)

Le misure vengono riesaminate almeno una volta l'anno e dopo ogni incidente o cambiamento rilevante dell'infrastruttura.

- **Impostazioni predefinite.** I nuovi operatori ricevono solo l'accesso assegnato dal Titolare; le comunicazioni ai pazienti (email, SMS, WhatsApp) e la sincronizzazione con calendari esterni sono disattivate finché il Titolare non le attiva.
- **Minimizzazione.** Ai fornitori esterni vengono inviati solo i dati necessari al servizio richiesto (es. destinatario e testo del promemoria).
- **Sviluppo.** Le modifiche all'applicazione vengono provate su un ambiente di test prima della pubblicazione, con copia di sicurezza dei file modificati.
- **Riesame.** Verifica annuale di queste misure, dei sub-responsabili e dei loro accordi; aggiornamento di questo allegato quando le misure cambiano.