Accordo per il trattamento dei dati personali

Art. 28 del Regolamento (UE) 2016/679 (GDPR) — Open Kanino — versione 2.0, in vigore dal 9 ottobre 2026. Sostituisce la versione 1.0 del 22 maggio 2018.

Parti

Ruolo	Soggetto
Titolare del trattamento ("Titolare")	Lo studio, il professionista o la società che si registra a Open Kanino e accetta i Termini del servizio
Responsabile del trattamento ("Responsabile")	LIME TIME SOFTWARE S.L., CIF B76267442, C/ Rambla Pedro Lezcano Montalvo nº 4, Local 4, 35200 Telde, Las Palmas (Spagna)
Responsabile della protezione dei dati del Responsabile (DPO)	Isabella Lopes, isabellalopesdpo@gmail.com
Contatto per la protezione dei dati	privacy@openkanino.it

1. Oggetto e ambito

1. Questo Accordo disciplina il trattamento dei dati personali che il Responsabile effettua per conto del Titolare nell'erogazione del servizio Open Kanino.
2. L'Accordo fa parte integrante dei Termini del servizio ed è accettato insieme a essi. In caso di contrasto tra i Termini del servizio e questo Accordo, per la protezione dei dati prevale questo Accordo.
3. Fanno parte dell'Accordo: l'Allegato 1 (Descrizione del trattamento, in fondo a questo documento), l'Allegato 2 (Misure tecniche e organizzative) e l'Allegato 3 (Sub-responsabili del trattamento).

2. Definizioni

I termini usati in questo Accordo hanno il significato previsto dall'art. 4 del GDPR. Inoltre:

- **Normativa sulla protezione dei dati**: il GDPR, la Ley Orgánica 3/2018 (LOPDGDD) e le norme nazionali applicabili al Titolare, compreso il D.Lgs. 196/2003 e successive modifiche per i Titolari con sede in Italia.
- **Sub-responsabile**: un altro responsabile del trattamento di cui il Responsabile si avvale per svolgere attività di trattamento per conto del Titolare.
- **Violazione dei dati personali**: la violazione di sicurezza descritta dall'art. 4, n. 12 del GDPR.
- **Clausole contrattuali tipo**: le clausole adottate con la decisione di esecuzione (UE) 2021/914 della Commissione europea.
- **Paese terzo**: un Paese esterno allo Spazio Economico Europeo (SEE).

3. Istruzioni del Titolare

1. Il Responsabile tratta i dati personali soltanto su istruzione documentata del Titolare, anche in caso di trasferimento verso Paesi terzi, salvo che lo richieda il diritto dell'Unione o dello Stato membro a cui il Responsabile è soggetto; in tal caso ne informa il Titolare prima del trattamento, se la legge lo consente.
2. Costituiscono istruzioni documentate: questo Accordo, i Termini del servizio e le impostazioni che il Titolare sceglie nell'applicazione (per esempio l'attivazione di promemoria, invii al Sistema Tessera Sanitaria o sincronizzazioni con calendari esterni).
3. Il Responsabile informa immediatamente il Titolare se ritiene che un'istruzione violi la Normativa sulla protezione dei dati.
4. Il Responsabile non usa i dati del Titolare per finalità proprie.

4. Obblighi del Responsabile

Il Responsabile:

1. garantisce che le persone autorizzate a trattare i dati siano vincolate alla riservatezza e ricevano istruzioni adeguate;
2. adotta le misure tecniche e organizzative descritte nell'Allegato 2, adeguate al rischio ai sensi dell'art. 32 del GDPR;
3. assiste il Titolare, con misure adeguate, nel dare seguito alle richieste degli interessati (artt. 15–22 del GDPR);
4. assiste il Titolare nel rispetto degli obblighi degli artt. 32–36 del GDPR (sicurezza, notifica delle violazioni, valutazione d'impatto, consultazione preventiva), tenendo conto della natura del trattamento e delle informazioni disponibili;
5. tiene il registro delle attività di trattamento svolte per conto del Titolare (art. 30, par. 2 del GDPR);
6. mette a disposizione del Titolare le informazioni necessarie a dimostrare il rispetto di questo Accordo e consente le verifiche previste dalla sezione 10.

5. Misure di sicurezza

1. Le misure tecniche e organizzative applicate sono descritte nell'Allegato 2.
2. Il Responsabile può aggiornarle 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, e le modifiche rilevanti sono comunicate al Titolare. Gli aggiornamenti che non riducono il livello di sicurezza non richiedono una nuova accettazione dell'Accordo.

6. Sub-responsabili

1. Il Titolare concede al Responsabile un'autorizzazione scritta generale ad avvalersi di sub-responsabili (art. 28, par. 2 del GDPR). I sub-responsabili autorizzati alla data di questo Accordo sono elencati nell'Allegato 3.
2. Il Responsabile comunica al Titolare, con almeno 30 giorni di preavviso, l'aggiunta o la sostituzione di un sub-responsabile, tramite email o avviso nell'applicazione, e aggiorna l'elenco pubblicato.
3. Entro questo termine il Titolare può opporsi per iscritto, per motivi ragionevoli legati alla protezione dei dati. Le parti cercano in buona fede una soluzione; se non la trovano, il Titolare può recedere dal servizio senza penali prima che la modifica abbia effetto.

4. Il Responsabile impone a ciascun sub-responsabile, con un contratto scritto, obblighi di protezione dei dati sostanzialmente equivalenti a quelli di questo Accordo, e resta pienamente responsabile verso il Titolare del loro adempimento.

7. Localizzazione dei dati e trasferimenti verso Paesi terzi

1. I dati dell'applicazione (database, immagini, documenti, backup) sono conservati nell'Unione Europea, nel data center DigitalOcean di Amsterdam (Paesi Bassi).
2. I trasferimenti verso Paesi terzi avvengono solo verso i sub-responsabili indicati nell'Allegato 3 e solo in presenza delle garanzie previste dal capo V del GDPR: una decisione di adeguatezza della Commissione europea (per gli Stati Uniti, l'EU-U.S. Data Privacy Framework per i fornitori certificati) oppure le Clausole contrattuali tipo, con le eventuali misure supplementari necessarie.
3. Se la garanzia usata per un trasferimento perde validità, il Responsabile adotta senza ritardo una garanzia alternativa conforme o sospende il trasferimento, informandone il Titolare.

8. Violazioni dei dati personali

1. Il Responsabile informa il Titolare senza ingiustificato ritardo, e comunque entro 24 ore da quando ne viene a conoscenza, di ogni violazione dei dati personali che riguardi i dati del Titolare.
2. La comunicazione contiene, per quanto disponibili, le informazioni dell'art. 33, par. 3 del GDPR: natura della violazione, categorie e numero approssimativo di interessati e di registrazioni coinvolti, contatto del DPO, probabili conseguenze, misure adottate o proposte. 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.
3. Il Responsabile collabora con il Titolare e adotta le misure necessarie a contenere la violazione e ridurne gli effetti. La notifica all'autorità di controllo e la comunicazione agli interessati restano a cura del Titolare, salvo diverso accordo scritto.

9. Richieste degli interessati

1. Se un interessato si rivolge direttamente al Responsabile per esercitare i propri diritti, il Responsabile inoltra la richiesta al Titolare senza ritardo, e comunque entro 5 giorni lavorativi, e non risponde nel merito senza istruzioni del Titolare.
2. L'applicazione consente al Titolare di consultare, correggere, esportare e cancellare i dati dei propri pazienti. Per le richieste che il Titolare non può soddisfare in autonomia, il Responsabile presta assistenza.

10. Verifiche

1. Su richiesta, il Responsabile fornisce al Titolare le informazioni necessarie a dimostrare il rispetto di questo Accordo, compresa la documentazione resa disponibile dai sub-responsabili e dai fornitori di infrastruttura (certificazioni, attestazioni, rapporti di audit indipendenti, relazioni di conformità e altra documentazione idonea e pertinente).
2. Se le informazioni del punto 1 non sono sufficienti a dimostrare il rispetto di questo Accordo, oppure in caso di violazione dei dati o di richiesta di un'autorità di controllo, il Titolare, direttamente o tramite un revisore indipendente vincolato alla riservatezza, può svolgere un'ispezione, con un preavviso scritto di almeno 30 giorni e non più di una volta per anno solare. L'ispezione si svolge di norma da remoto, in orario lavorativo, senza accesso ai dati di altri clienti e senza compromettere la sicurezza del servizio. I costi sono a carico del Titolare.

3. Per quanto riguarda infrastrutture, sistemi o servizi gestiti da sub-responsabili o fornitori terzi, la verifica è effettuata, ove possibile, sulla base della documentazione resa disponibile dagli stessi, comprese certificazioni, attestazioni, rapporti di audit indipendenti, relazioni di conformità e altra documentazione idonea e pertinente.
4. Qualora tale documentazione non sia sufficiente rispetto alle specifiche circostanze della verifica, il Responsabile coopera, nei limiti dei propri poteri contrattuali e delle informazioni legittimamente accessibili, al fine di fornire gli ulteriori elementi ragionevolmente necessari, fermo restando il rispetto delle condizioni di sicurezza, riservatezza e accesso stabilite dai relativi sub-responsabili o fornitori.

11. Durata, restituzione e cancellazione dei dati

1. Questo Accordo resta in vigore finché il Responsabile tratta dati per conto del Titolare.
2. Per tutta la durata del contratto il Titolare può esportare in autonomia tutti i propri dati dall'account principale (Impostazioni → Account): tabelle in formato XML, immagini diagnostiche e documenti in archivio ZIP.
3. Alla fine del rapporto, su richiesta del Titolare, il Responsabile cancella tutti i dati secondo la procedura descritta nell'Allegato 2: distruzione dell'account e dei dati collegati entro 7 giorni dalla conferma del Titolare, cancellazione delle copie nei backup e negli snapshot entro i successivi 7 giorni, conferma scritta via email. I log di accesso e sicurezza seguono i tempi di conservazione indicati nell'Allegato 2 (sezione 5).
4. Se il contratto cessa senza una richiesta del Titolare (per esempio per mancato pagamento o mancato rinnovo dell'abbonamento), il Responsabile conserva i dati per 90 giorni, per consentire al Titolare di regolarizzare la posizione o di esportarli, e poi li cancella con la stessa procedura, dandone comunicazione al Titolare.
5. Il Responsabile conserva oltre questi termini solo i dati che deve tenere per obbligo di legge, per il tempo strettamente necessario e con le stesse garanzie di riservatezza.

12. Responsabilità

Ciascuna parte risponde dei danni causati dalla violazione dei propri obblighi ai sensi dell'art. 82 del GDPR. Per il resto si applicano le limitazioni di responsabilità previste dai Termini del servizio, nei limiti consentiti dalla Normativa sulla protezione dei dati.

13. Modifiche all'Accordo

1. Gli aggiornamenti dell'Allegato 2 e dell'Allegato 3 seguono le sezioni 5 e 6.
2. Le altre modifiche di questo Accordo sono comunicate al Titolare con almeno 30 giorni di preavviso. Se il Titolare non le accetta, può recedere dal servizio senza penali prima della loro entrata in vigore.

14. Legge applicabile e foro

1. Questo Accordo è regolato dalla legge applicabile ai Termini del servizio, fermo restando il rispetto del GDPR e delle norme nazionali di protezione dei dati applicabili a ciascuna parte.
2. Per le controversie è competente il foro indicato nei Termini del servizio. Restano salvi i diritti degli interessati e la competenza delle autorità di controllo ai sensi della Normativa sulla protezione dei dati.

Allegato 1 — Descrizione del trattamento

Voce	Descrizione
Natura e finalità	Fornitura del software gestionale Open Kanino in modalità SaaS per studi odontoiatrici: agenda e appuntamenti, cartella clinica e diario clinico, piani di cura, preventivi, fatturazione e pagamenti, archivio di immagini e documenti, comunicazioni ai pazienti (email, SMS, WhatsApp) attivate dallo studio, invio dei dati di spesa al Sistema Tessera Sanitaria su istruzione dello studio, assistenza tecnica
Operazioni	Raccolta, registrazione, organizzazione, conservazione, consultazione, modifica, estrazione, trasmissione su istruzione del Titolare, cancellazione e distruzione
Categorie di interessati	Pazienti (compresi minori), loro familiari, tutori o rappresentanti; titolari, dipendenti e collaboratori dello studio; fornitori, laboratori odontotecnici e altri contatti dello studio
Categorie di dati personali	Dati anagrafici e codice fiscale; dati di contatto; appuntamenti; dati amministrativi, di fatturazione e di pagamento; firme apposte sui documenti; dati di accesso degli utenti dello studio
Categorie particolari di dati (art. 9 GDPR)	Dati relativi alla salute: anamnesi, diario clinico, piani di cura e prestazioni, immagini diagnostiche e documenti clinici
Durata	Per tutta la durata del contratto e fino alla cancellazione dei dati prevista dalla sezione 11
Luogo di conservazione	Unione Europea — data center DigitalOcean di Amsterdam (Paesi Bassi)