Informativa sul Trattamento dei Dati Personali e sulla Privacy

Applicazione MedReminder

Ultima modifica: 2 maggio 2025

Indice

1 Introduzione

Benvenuto in MedReminder (di seguito "App"), l'applicazione che ti aiuta a gestire la tua terapia farmacologica. Per utilizzare le funzionalità dell'App è necessaria la registrazione.

La tua privacy è molto importante per noi. La presente informativa descrive come **MedReminder S.r.l.** (di seguito "MedReminder" o "noi"), in qualità di Titolare del Trattamento, raccoglie, utilizza e protegge i tuoi dati personali quando utilizzi la nostra App, in conformità al Regolamento UE 2016/679 (GDPR).

2 Titolare del Trattamento

Il Titolare del trattamento dei tuoi dati personali è:

- **Denominazione:** MedReminder S.r.l.
- **Sede Legale:** Via Roma 41, 24040 Madone - (BG), Italia
- **Partita IVA:** IT12345678901
- **Email dedicata alla privacy:** privacy@medreminder.it
- **PEC:** medreminder@pec.it

Il nostro Responsabile della Protezione dei Dati (DPO) è Giovanni Brignoli, contattabile all'indirizzo brignoli.giovanni.06@itisdalmine.edu.it.

3 Tipologie di Dati Personali Trattati

Raccogliamo diverse categorie di dati personali per fornirti i servizi dell'App:

- **Dati identificativi e di contatto:** Poiché la registrazione è obbligatoria per utilizzare l'App, raccogliamo il tuo indirizzo email e una password da te scelta per l'autenticazione. Potremmo raccogliere anche un nome utente o nickname da te fornito.
- **Dati relativi alla salute (Categoria Particolare di Dati):** Per utilizzare la funzione principale del calendario farmaci, tratteremo i dati che inserirai volontariamente, quali:
  - Nomi dei farmaci che assumi.
  - Orari e giorni programmati per l'assunzione.

  Questi dati sono considerati "dati relativi alla salute" ai sensi del GDPR e richiedono una protezione specifica e il tuo consenso esplicito.
- **Dati relativi all'utilizzo dell'App:**

- Farmaci cercati tramite la funzione di ricerca (interfacciata con le API pubbliche AIFA).
- Domande poste all'Assistente AI (basato esclusivamente sui foglietti illustrativi).

- **Dati relativi agli abbonamenti (se applicabile):** Informazioni relative al piano di abbonamento sottoscritto (gratuito o a pagamento) e allo stato dei pagamenti (ma *non* i dati completi della carta di credito/debito, vedi Sezione 7).
- **Dati Tecnici:** Durante l'utilizzo dell'App, potremmo raccogliere automaticamente alcuni dati tecnici necessari per garantire il corretto funzionamento e la sicurezza, come tipo di dispositivo, versione del sistema operativo, indirizzo IP (temporaneamente per motivi di sicurezza e diagnostica), log di errori anonimi. Non raccogliamo identificativi pubblicitari univoci del dispositivo.
- **Dati di Localizzazione:** L'App **non** raccoglie dati relativi alla tua posizione geografica.

4 Finalità del Trattamento e Base Giuridica

Trattiamo i tuoi dati personali per le seguenti finalità e sulla base delle seguenti basi giuridiche:

- **a) Registrazione, Autenticazione e Fornitura Funzionalità Principali (Calendario Farmaci):**
  - *Finalità:* Permetterti di creare e gestire il tuo account, registrare i farmaci, impostare orari di assunzione e ricevere notifiche promemoria.
  - *Dati Trattati:* Dati identificativi (email, password criptata), Dati relativi alla salute (nomi farmaci, orari).
  - *Base Giuridica:*
    - Dati identificativi: Esecuzione di un contratto (Art. 6.1.b GDPR) – la fornitura del servizio richiesto, subordinato alla registrazione.
    - Dati relativi alla Salute: **Consenso Esplicito** (Art. 9.2.a GDPR), richiesto tramite azione positiva inequivocabile (es. spunta di una casella dedicata e non preselezionata durante la configurazione iniziale o al primo inserimento di un farmaco), dopo aver preso visione dell'informativa. Senza questo consenso, non potrai inserire dati nel calendario.
- **b) Funzionalità Ricerca Farmaci e Download Foglietto Illustrativo (via API AIFA):**
  - *Finalità:* Consentirti di cercare informazioni ufficiali sui farmaci e scaricare i foglietti illustrativi tramite le API pubbliche AIFA.

- *Dati Trattati:* Termini di ricerca farmaco.
- *Base Giuridica:* Esecuzione di un servizio da te richiesto (Art. 6.1.b GDPR). AIFA agisce come titolare autonomo.

- **c) Funzionalità Assistente AI:**
  - *Finalità:* Fornire risposte informative basate esclusivamente sul contenuto del foglietto illustrativo del farmaco selezionato. L'AI non fornisce diagnosi o pareri medici.
  - *Dati Trattati:* Testo della domanda.
  - *Base Giuridica:*
    - Domande generiche: Esecuzione di un servizio da te richiesto (Art. 6.1.b GDPR).
    - Domande che *potrebbero* rivelare dati relativi alla salute: **Consenso Esplicito** (Art. 9.2.a GDPR), richiesto al primo utilizzo della funzione.

- **d) Gestione Abbonamenti e Pagamenti (per funzioni Premium):**
  - *Finalità:* Gestire la sottoscrizione ai piani a pagamento, processare i pagamenti e adempiere agli obblighi fiscali e contabili.
  - *Dati Trattati:* Dati relativi all'abbonamento, dati necessari alla transazione (gestiti dal fornitore terzo, vedi Sez. 7), dati di fatturazione.
  - *Base Giuridica:* Esecuzione di un contratto (Art. 6.1.b GDPR) per la fornitura dei servizi premium e Adempimento di obblighi legali (Art. 6.1.c GDPR) per la gestione fiscale e contabile.

- **e) Manutenzione Tecnica e Sicurezza dell'App:**
  - *Finalità:* Garantire il corretto funzionamento, sicurezza e integrità dell'App e dei dati, diagnosticare problemi, prevenire accessi non autorizzati.
  - *Dati Trattati:* Dati Tecnici (inclusi IP temporanei).
  - *Base Giuridica:* Legittimo interesse del Titolare (Art. 6.1.f GDPR) a garantire la sicurezza e l'efficienza del servizio.

- **f) Analisi Statistiche Aggregate e Vendita a Terzi per Ricerca e Sostenibilità:**
  - *Finalità:* Elaborare statistiche aggregate e completamente anonime sui farmaci più cercati e sulle tipologie di informazioni più richieste al chatbot, per migliorare l'App e vendere tali dati anonimi a enti terzi (es. istituti di ricerca, aziende farmaceutiche) esclusivamente per finalità di ricerca, analisi di mercato e farmacovigilanza, contribuendo alla sostenibilità economica dell'App.

- *Dati Trattati:* Dati di utilizzo resi **completamente anonimi** tramite processi irreversibili. **Non vengono mai condivisi i tuoi dati personali identificativi o sanitari specifici con terzi per questa finalità.**
- *Base Giuridica:* **Legittimo interesse** del Titolare (Art. 6.1.f GDPR) allo sviluppo del servizio, alla ricerca e alla sostenibilità economica, bilanciato con l'uso esclusivo di dati aggregati e totalmente anonimi. Hai il diritto di opporti (vedi Sez. 10).

5 Natura del Conferimento dei Dati e Conseguenze del Rifiuto

- Il conferimento dei **dati identificativi** (email, password) è **obbligatorio** per la registrazione e l'utilizzo dell'App. Il mancato conferimento impedisce l'uso del servizio.
- Il conferimento dei **Dati relativi alla Salute** per la funzione Calendario è facoltativo ma basato sul tuo **consenso esplicito**. Il mancato consenso impedisce l'utilizzo di tale funzionalità.
- Il conferimento dei dati per le funzioni Ricerca/Download e Assistente AI è necessario per poter utilizzare tali funzioni.
- Il conferimento dei dati per la gestione degli abbonamenti a pagamento è necessario per accedere alle funzionalità premium.
- Il trattamento dei dati tecnici è necessario per il funzionamento e la sicurezza dell'App.
- Il trattamento per finalità statistiche e di vendita di dati anonimi si basa sul nostro legittimo interesse e puoi opporti.

6 Modalità di Trattamento e Conservazione dei Dati

I tuoi dati personali sono trattati con strumenti elettronici e automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti, nel rispetto dei principi GDPR.

- **Dati Account e Calendario (inclusi dati salute):** Conservati sui server sicuri di Supabase (Francoforte, Germania - UE) finché il tuo account è attivo. In caso di cancellazione dell'account da parte tua, i dati verranno eliminati entro 30 giorni, salvo diversi obblighi legali (es. conservazione fatture per 10 anni) o necessità di difesa in giudizio. In caso di inattività prolungata (24 mesi senza accessi), potremmo contattarti prima di procedere alla cancellazione.
- **Query Assistente AI:** Processate e non conservate in modo riconducibile all'utente dopo la sessione, se non in forma anonima per analisi aggregate.

- **Ricerche Farmaci (API AIFA):** Non conserviamo cronologia ricerche associata all'utente identificabile.
- **Dati Pagamento:** Non conserviamo i dati completi della tua carta. Ci affidiamo a un fornitore esterno certificato (vedi Sez. 7). Conserviamo solo informazioni sulla transazione e sull'abbonamento per finalità contrattuali e fiscali.
- **Dati Tecnici:** Log IP conservati per un breve periodo (es. 7 giorni) per sicurezza, altri dati tecnici anonimizzati conservati per periodi più lunghi (es. 12 mesi) per analisi.
- **Dati Aggregati e Anonimi:** Essendo anonimi, non sono soggetti a limiti di conservazione legati all'identificabilità.

Adottiamo specifiche misure di sicurezza (vedi Sez. 8) per proteggere i tuoi dati.

7 Trattamento Dati di Pagamento (Funzionalità Premium)

Se decidi di sottoscrivere un piano di abbonamento a pagamento per le funzionalità premium dell'App, la gestione dei pagamenti viene affidata a un fornitore esterno specializzato e certificato secondo i più elevati standard di sicurezza del settore (PCI-DSS). Attualmente ci avvaliamo di:

Stripe Payments Europe, Ltd. (con sede in Irlanda)

- Quando effettui un pagamento, inserisci i dati della tua carta di credito/debito direttamente sui sistemi sicuri di Stripe. **MedReminder S.r.l. non raccoglie, non tratta e non conserva i dati completi della tua carta di pagamento.**
- Riceviamo da Stripe solo le informazioni strettamente necessarie a confermare l'avvenuta transazione, gestire il tuo stato di abbonamento (attivo/scaduto) e adempiere agli obblighi fiscali (es. identificativo della transazione, importo, data, tipo di piano).
- Stripe agisce come Titolare autonomo del trattamento per i dati di pagamento che raccoglie direttamente da te. Ti invitiamo a consultare l'informativa privacy di Stripe sul loro sito web per maggiori dettagli: https://stripe.com/it/privacy
- La base giuridica per il trattamento dei dati relativi alla transazione da parte nostra è l'esecuzione del contratto (Art. 6.1.b GDPR) e l'adempimento di obblighi legali (Art. 6.1.c GDPR).

8 Sicurezza dei Dati

La sicurezza dei tuoi dati, in particolare quelli relativi alla salute, è una nostra priorità assoluta. Adottiamo misure tecniche e organizzative adeguate per proteggere i dati da accessi non autorizzati, perdita, distruzione o modifica illecita, conformemente all'Art. 32 del GDPR. Queste misure includono, tra le altre:

- **Crittografia della Password:** La tua password di accesso all'App è conservata utilizzando algoritmi di hashing sicuri (SHA256) che la rendono non leggibile anche per noi.

- **Crittografia dei Dati Sensibili:** I dati relativi alla salute inseriti nel calendario farmaci sono crittografati sia a riposo (at rest) sui server del nostro database Supabase, sia durante la trasmissione (in transit) tra l'App e i server.

- **Comunicazioni Sicure (HTTPS):** Tutte le comunicazioni tra l'App e i nostri server, inclusi i server Supabase e il server AI, nonché le chiamate alle API AIFA, avvengono esclusivamente tramite protocollo HTTPS, che garantisce la crittografia dei dati in transito.

- **Accesso Controllato:** L'accesso ai dati personali da parte del nostro personale è strettamente limitato in base ai ruoli e alle necessità operative ("principio del minimo privilegio") e soggetto a obblighi di riservatezza.

- **Infrastruttura Sicura:** Ci affidiamo a fornitori (come Supabase) che garantiscono elevati standard di sicurezza fisica e logica per i loro data center all'interno dell'UE.

- **Pseudonimizzazione/Anonimizzazione:** Adottiamo tecniche di anonimizzazione robuste per i dati destinati ad analisi statistiche e vendita (finalità 4.f), come descritto.

- **Procedure di Backup e Ripristino:** Disponiamo di procedure per il backup regolare dei dati e il loro ripristino in caso di incidenti.

- **Monitoraggio e Test:** Effettuiamo monitoraggi e test periodici per verificare l'efficacia delle misure di sicurezza.

Nonostante il nostro impegno, nessun sistema è infallibile. In caso di violazione dei dati personali (Data Breach), attueremo le procedure previste dal GDPR per la notifica all'Autorità Garante e, se necessario, agli utenti interessati.

9 Destinatari dei Dati

I tuoi dati personali potranno essere comunicati a:

- Personale autorizzato di MedReminder S.r.l.
- Fornitori di servizi tecnici (Responsabili del Trattamento ex Art. 28 GDPR):
  - Supabase Inc. (Database hosting - Francoforte, UE).
  - Stripe Payments Europe, Ltd. (Gestione pagamenti premium - Irlanda, UE).

- Agenzia Italiana del Farmaco (AIFA) (Titolare autonomo, per le sole chiamate API da te attivate).
- Enti terzi acquirenti di dati **aggregati e anonimi** (per finalità 4.f).
- Autorità giudiziarie o amministrative (solo se obbligatorio per legge).

I tuoi dati personali identificativi e sanitari **non saranno diffusi né ceduti a terzi per loro finalità di marketing.**

10 Trasferimento Dati all'Estero

I tuoi dati personali sono trattati e conservati su server ubicati all'interno dell'Unione Europea (Francoforte, Germania per Supabase; Irlanda per Stripe). Non effettuiamo trasferimenti dei tuoi dati personali identificativi o sanitari al di fuori dello Spazio Economico Europeo (SEE).

11 I Tuoi Diritti Privacy

In qualità di interessato, hai il diritto di esercitare i diritti previsti dagli articoli 15-22 del GDPR:

- Diritto di **Accesso**.
- Diritto di **Rettifica**.
- Diritto alla **Cancellazione** (Diritto all'Oblio).
- Diritto di **Limitazione** del Trattamento.
- Diritto alla **Portabilità** dei Dati (per dati trattati su base consenso/contratto con mezzi automatizzati).
- Diritto di **Opposizione** (al trattamento basato su legittimo interesse).
- Diritto di **Revoca del Consenso** (per dati sanitari e uso AI, senza pregiudicare trattamenti precedenti).
- Diritto di non essere sottoposto a **decisioni automatizzate** significative.

Puoi esercitare i tuoi diritti inviando una comunicazione scritta a privacy@medreminder.it. Potremmo chiederti informazioni aggiuntive per verificare la tua identità. Risponderemo entro un mese (prorogabile di due mesi per complessità).

12 Diritto di Proporre Reclamo

Se ritieni che il trattamento violi il GDPR, hai diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali (www.gpdp.it) o all'autorità di controllo del tuo Stato membro.

13 Processi Decisionali Automatizzati e Profilazione

Confermiamo che l'App **non** effettua profilazione degli utenti né processi decisionali basati unicamente sul trattamento automatizzato che producano effetti giuridici o incidano in modo significativo sulla tua persona. L'Assistente AI fornisce solo informazioni contestuali basate sul foglietto illustrativo.

14 Modifiche all'Informativa Privacy

Ci riserviamo il diritto di aggiornare questa Informativa. Qualsiasi modifica sostanziale sarà notificata tramite l'App o via email (se fornita). Ti invitiamo a consultarla periodicamente.