ALETEO

Privacy Policy

Effective Date: November 27, 2025

1. Introduction

Aleteo ("we," "us," or "our") is committed to protecting your privacy and ensuring the security of your personal data. This Privacy Policy explains how we collect, use, disclose, and protect your information when you use our mobile application and related services (the "Service").

We process personal data in accordance with the General Data Protection Regulation (GDPR) and other applicable European data protection laws. Please read this Privacy Policy carefully to understand our practices regarding your personal data.

2. Data Controller

Aleteo is the data controller responsible for your personal data. Our contact details are:

Email: team@aleteo.net

Note: Aleteo is in the process of formal company registration. Full legal entity details, including registered address and company registration number, will be provided upon completion of registration.

3. Data We Collect

3.1 Data from Companion Users

We collect the following categories of data from Companion Users (older adults using the AI companion):

Conversation Data:

- Voice recordings (audio) of conversations with the AI Companion
- Transcribed text from conversations
- Conversation frequency, duration, and timing
- Conversation topics and content

Analyzed Patterns:

- Sentiment and emotional state indicators

- Cognitive markers (vocabulary diversity, word-finding patterns, narrative coherence, memory recall patterns)
- Speech patterns (rhythm, processing speed, attention signals)
- Mood trends and emotional resilience markers
- Social engagement indicators

Personal Information ("Core Facts Memory"):

- Important personal information you choose to share
- Preferences and interests
- Family history and relationships
- Life experiences and memories
- Personalization preferences

Technical Data:

- App usage patterns and interaction frequency
- Device information (device type, operating system)
- Log data and error reports

3.2 Data from Guardian Users

We collect the following data from Guardian Users (family members and caregivers):

- Account credentials (email, password)
- Contact information
- Relationship to the Companion User
- Dashboard access logs and activity
- Alert and notification preferences

3.3 Special Category Data

Some data we process may constitute special category data under GDPR, including health-related information that may be revealed through conversations and cognitive pattern analysis. We process this data only with your explicit consent and for the purposes described in this Privacy Policy.

4. Purposes of Data Processing

We process your personal data for the following purposes:

4.1 Primary Purposes

- Providing the conversational AI companion service
- Personalizing conversations based on your preferences and history
- Detecting and analyzing cognitive and emotional patterns
- Generating insights and reports for authorized Guardian Users
- Providing early indicators of potential changes in cognitive or emotional state
- Improving conversation quality through personalization

4.2 Service Improvement

- Analyzing usage patterns to improve the Service
- Developing new features and functionalities
- Training and improving our AI models using anonymized data
- Conducting research to enhance cognitive assessment accuracy

4.3 Communication

- Sending service-related notifications
- Responding to your inquiries and support requests
- Providing alerts to Guardian Users (as configured)

5. Legal Basis for Processing

We process your personal data based on the following legal grounds under GDPR:

Consent (Article 6(1)(a)): For processing voice recordings, conversation content, and special category health data. You provide explicit consent when you register for and use the Service.

Contract Performance (Article 6(1)(b)): Processing necessary to provide you with the Service as described in our Terms and Conditions.

Legitimate Interests (Article 6(1)(f)): For service improvement, security, and fraud prevention, where our interests do not override your fundamental rights.

For special category data (health-related information), we rely on your explicit consent under Article 9(2)(a) of GDPR.

6. Data Sharing and Disclosure

6.1 Guardian Users

With your explicit authorization, we share conversation analysis, sentiment patterns, cognitive marker summaries, and other insights with your designated Guardian Users through the Guardian Dashboard. You control what information is shared through granular privacy settings.

6.2 Third-Party Service Providers

We engage trusted third-party service providers to help us deliver the Service:

- Cloud hosting providers for data storage and processing
- Commercial speech recognition API providers for voice-to-text conversion
- Large language model (LLM) API providers for AI conversation capabilities
- Real-time voice network providers for audio transmission
- Email service providers for notifications

All third-party processors are bound by data processing agreements and are required to protect your data in accordance with GDPR.

6.3 Data We Do NOT Share

We do NOT share your personal data with:

- Advertising networks or ad tech companies
- Data brokers
- Social media platforms
- Insurance companies (unless explicitly requested by you)

6.4 Legal Requirements

We may disclose your data if required by law, court order, or government request, or if necessary to protect our rights, safety, or property, or the rights, safety, or property of others.

7. International Data Transfers

Your data is primarily processed within the European Union. However, some of our third-party service providers may process data in the United States or other countries outside the EU/EEA.

When we transfer personal data outside the EU/EEA, we ensure appropriate safeguards are in place, including:

- European Commission adequacy decisions for the recipient country
- Standard Contractual Clauses (SCCs) approved by the European Commission
- Binding Corporate Rules where applicable
- Other legally recognized transfer mechanisms under GDPR Chapter V

You may request information about the specific safeguards applied to transfers of your data by contacting us.

8. Data Retention

We retain your personal data for as long as your account is active and as necessary to provide you with the Service. After you delete your account or request data deletion:

- Most personal data will be deleted within 90 days
- Some data may be retained longer if required by law or for legitimate business purposes (e.g., financial records, legal disputes)
- Anonymized and aggregated data that cannot identify you may be retained indefinitely for research and service improvement

You may request deletion of your data at any time by contacting us or using the account settings in the application.

9. Your Rights Under GDPR

Under the General Data Protection Regulation, you have the following rights regarding your personal data:

Right of Access: You can request a copy of the personal data we hold about you.

Right to Rectification: You can request that we correct any inaccurate or incomplete personal data.

Right to Erasure ("Right to be Forgotten"): You can request that we delete your personal data in certain circumstances.

Right to Restriction: You can request that we restrict the processing of your personal data in certain circumstances.

Right to Data Portability: You can request to receive your personal data in a structured, commonly used, machine-readable format.

Right to Object: You can object to processing based on legitimate interests or for direct marketing purposes.

Right to Withdraw Consent: Where processing is based on consent, you can withdraw your consent at any time.

Right to Lodge a Complaint: You can lodge a complaint with a supervisory authority (e.g., CNIL in France, or your local data protection authority).

To exercise any of these rights, please contact us at team@aleteo.net. We will respond to your request within 30 days.

10. Data Security

We implement appropriate technical and organizational measures to protect your personal data against unauthorized access, alteration, disclosure, or destruction. These measures include:

- Encryption of data in transit and at rest
- Secure authentication mechanisms
- Access controls limiting who can access your data
- Regular security assessments and monitoring
- Audit logging of data access
- Employee training on data protection

While we strive to protect your personal data, no method of transmission over the Internet or electronic storage is 100% secure. We cannot guarantee absolute security.

11. Guardian Dashboard and Data Sharing

11.1 Authorization

Guardian Users can only access the Guardian Dashboard if explicitly authorized by the Companion User or if they hold legal guardianship. Companion Users control which Guardian Users have access and what level of information they can view.

11.2 Information Available to Guardians

Depending on your settings, Guardian Users may access:

- Conversation analysis summaries (not full transcripts unless specifically configured)
- Sentiment patterns and emotional trends
- Cognitive marker summaries
- Mood and engagement level reports
- Alerts for significant changes in patterns

11.3 Your Control

You can modify Guardian access permissions, revoke access, or exclude specific information from sharing at any time through the application settings.

12. Children's Privacy

The Service is designed for older adults and is not intended for use by children under 16 years of age. We do not knowingly collect personal data from children under 16. If we become aware that we have collected personal data from a child under 16, we will take steps to delete that information.

13. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices or for legal, operational, or regulatory reasons. We will notify you of material changes by posting the updated Privacy Policy in the application and/or sending you an email notification at least 30 days before the changes take effect.

We encourage you to review this Privacy Policy periodically. Your continued use of the Service after the effective date of the revised Privacy Policy constitutes your acceptance of the changes.

14. Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us at:

Email: team@aleteo.net

You also have the right to lodge a complaint with a supervisory authority. In France, the supervisory authority is the Commission Nationale de l'Informatique et des Libertés (CNIL). You may also contact the supervisory authority in your country of residence.