



# Trustlead Privacy Policy

**Last update :** 01/06/2026

Welcome to the Trustlead Mobile Application (the "App"). At Trustlead, your privacy is a top priority. This Privacy Policy explains how we collect, process, and protect your personal data when you use our App to record, transcribe, and integrate your voice notes with CRMs and instant messaging platforms. We are committed to handling your data transparently and securely.

This Privacy Policy applies to all personal data processed by Trustlead, its employees, and authorized third-party providers.

For inquiries regarding this Privacy Policy, you can contact us at [dpo@trustlead.co](mailto:dpo@trustlead.co).

## ▼ 1. Collection and Use of Personal Data

Data we collect:

- **Voice Recordings and Transcriptions:** Audio recordings captured via the App using the device's near-field microphone. Recordings are processed locally on the user's device and are never transmitted to or stored on Trustlead's servers or AI models. Only the resulting transcription is transmitted for processing.
- **Phone Call Metadata:** When users access the voice assistant via phone call, Trustlead collects call metadata (date, time, duration) and the user's professional phone number. No call audio is recorded or stored.

- CRM and Messaging Integration Data: Information shared with connected CRMs (e.g., contact details, structured notes) or instant messaging platforms (e.g., message metadata).
- Business Intelligence Integration Data: Data exchanged with connected BI tools (e.g., dashboards, reporting data).
- Knowledge Base Documents: Files uploaded by administrators (PDF, Excel, etc.) which may contain personal data belonging to third parties. Trustlead processes these documents solely to provide its services and acts as a data processor in this context.
- Account Information: Name, email address, and other details required to create and manage your account.
- Billing Information: Company name, billing contact name, email address, and billing address, collected for invoicing purposes.
- Device Information: Data about your device, including IP address, operating system, and app usage statistics.

## ▼ 2. Use of Personal Data

The personal data collected are used:

### Trustlead service offer

To provide transcription services, convert voice notes into structured data, and enable integration with CRMs, messaging platforms, and BI tools.

**Privacy by design:** Voice recordings are stored exclusively on the user's device and are never uploaded to Trustlead's servers or AI models. Trustlead uses near-field microphone detection to capture only the user's voice, excluding surrounding sounds and third-party conversations.

- **Data categories:** Transcription data, CRM/messaging platform integration data, BI integration data, knowledge base documents.
- **Legal basis:** Contractual necessity.
- **Retention period:** Transcriptions are retained for a maximum period of 12 months from the date of creation, unless deleted earlier by the user. Users

are notified prior to automatic deletion. Voice recordings are stored exclusively on the user's device and are not subject to Trustlead's retention policy.

## Phone Assistant Feature

To enable users to access the voice assistant by calling a dedicated phone number.

- **Data categories:** Professional phone number of the user, call metadata (date, time, duration).
- **Legal basis:** Contractual necessity.
- **Retention period:** Call metadata retained for 3 months.

## Customer support

To respond to support requests and communicate with our customers.

- **Data categories :** customer account information (name, email address), and any data voluntarily shared by the user in the context of their support request.
- **Legal basis :** legitimate interests to provide effective customer service
- **Retention period :** Duration of the account and 3 years after deactivation

## Service improvement

To analyze app usage, improve transcription accuracy, and optimize features.

- **Data categories :** app usage data, feature interaction logs, anonymized performance metrics
- **Legal basis:** Legitimate interests in improving our services.
- **Retention period:** Duration of account and 2 years after deletion.

## Marketing and Communication

To send promotional materials, updates about new features, and newsletters.

- **Data categories:** Email address, app usage preferences.

- **Legal basis:** Consent or legitimate interests, depending on the context.
- **Retention period:** Until the user unsubscribes or requests deletion.

## Compliance with Legal Obligations

To comply with legal and regulatory requirements, such as data retention laws.

- **Data categories:** Account and usage records.
- **Legal basis:** Legal obligations.
- **Retention period:** As required by law.

## Security and Fraud Prevention

To ensure app security and detect fraudulent activities.

- **Data categories:** Device information, app usage logs.
- **Legal basis:** Legitimate interests in ensuring app security.
- **Retention period:** 3 months.

## Invoicing and Payment Processing

To generate invoices and process payments for Trustlead services.

- **Data categories:** Company name, billing contact name, email address, billing address, transaction details.
- **Legal basis:** Legal obligation (accounting law) and contractual necessity.
- **Retention period:** 10 years, in accordance with French accounting regulations (Code de commerce, Art. L.123-22).

## ▼ 3. Sharing of Personal Data

We only share personal data under the following circumstances:

- **With our employees:** Authorized employees have access to the collected data, limited to what is necessary for their roles
- **With service providers:** Third-party providers assist in delivering our services. Categories include:

- **Hosting and infrastructure:**
  - **Ionos SE:** Server hosting. Servers located in Germany (Berlin, EU). Retains all data processed by Trustlead for the duration defined by customers.
  - **Supabase:** Database hosting. Servers located in France (Paris, EU). Retains all data stored by Trustlead for the duration defined by customers.
- **Artificial intelligence:**
  - **Mistral AI (default):** AI processing of transcripts, summaries, and templates. Servers located in France (Paris, EU). **No data retention (0 days), only processing.**
  - **Microsoft Azure (option):** AI processing of transcripts, summaries, and templates. Servers located in Sweden (EU). **No data retention (0 days), only processing.**
- **Payment gateway:**
  - **Qonto:** Invoice generation and financial transaction processing. Data treated: billing contact information (company name, contact name, email address, billing address). Servers located in the European Union. Retention: as required by applicable accounting and tax law (10 years in France).
- **Marketing and CRM:**
  - **Hubspot:** Customer relationship management. Data treated: account and contact information.
- **Performance and Security:**
  - **Datadog, Inc.:** Security logging (user ID, email addresses). Servers located in Germany (Frankfurt, EU). Retention: 15 days.
  - **PostHog:** Mobile application monitoring (touch events, HTTP calls without payload, errors). Servers located in Germany (Frankfurt, EU). Retention: 21 days. Activated based on your consent.

- **In case of legal obligation:** Personal data may be disclosed if required by law or to comply with a legal request.

## International Data Transfers

All Trustlead service providers currently process data within the European Union. Should this change, Trustlead will ensure appropriate safeguards are in place (including SCCs under Article 46 GDPR) and will update this Policy accordingly.

## ▼ 4. Data Security

We implement appropriate technical and organizational security measures to protect your personal data against loss, misuse, unauthorized access, disclosure, alteration or destruction.

We implement encryption of data in transit and at rest on our servers, including transcription data and integration payloads.

For more details, ask for our Trustlead Security WhitePaper by contacting [dpo@trustlead.co](mailto:dpo@trustlead.co)

## ▼ 5. Your rights

Under applicable data protection laws, you have the following rights:

- **Right to Information:** As outlined in Articles 13 and 14 of the GDPR.
- **Right of Access:** Access your personal data at any time (Article 15 of the GDPR).
- **Right to Rectification:** Correct inaccurate, incomplete, or outdated personal data (Article 16 of the GDPR).
- **Right to Restriction:** Restrict the processing of personal data under certain conditions (Article 18 of the GDPR).
- **Right to Erasure:** Request the deletion of personal data (Article 17 of the GDPR).

- **Right to File a Complaint:** File a complaint with a supervisory authority (in France, the CNIL) if data processing violates applicable regulations (Article 77 of the GDPR).
- **Post-Mortem Directives:** Set instructions for managing personal data after death (Article 40-1 of French data protection law).
- **Right to Withdraw Consent:** Withdraw consent for data processing at any time (Article 7 of the GDPR).
- **Right to Data Portability:** Receive personal data in a standard machine-readable format and transfer it to another entity (Article 20 of the GDPR).
- **Right to Object:** Object to data processing for legitimate reasons or for defending legal claims (Article 21 of the GDPR).

To exercise your rights or for any questions regarding this Policy, contact our Data Protection Officer at [dpo@trustlead.co](mailto:dpo@trustlead.co).

## ▼ 6. Changes to the Privacy Policy

We may update this Privacy Policy periodically. Updates will be published on this page with the updated date. We encourage you to review this page regularly to stay informed about our privacy practices.