Vertiza — Privacy Policy

LAST UPDATED
20 October 2026

Vertiza Effective date: 14 October 2026 · Last updated: 20 October 2026 This Privacy Policy explains how ME Film Studios LLC ("we", "us") collects, uses, stores and protects information when you use Vertiza, our AI assistant service (the "Service"), through the Vertiza app or through our website, and when you connect a third-party account (such as a Google or Microsoft account) to your assistant. We built Vertiza to work for you, not to trade in your data. We do not sell personal information, and we do not use the data you connect to train general-purpose AI models.

1. Who we are and how to contact us

Vertiza is provided by ME Film Studios LLC. For any question about this policy or about your data, write to **info@stellorient.com**.

2. What Vertiza does

Vertiza is a private AI assistant assigned to a specific person or team. It answers messages, drafts documents, keeps notes and reminders, and, only when you connect the relevant account, reads and acts on your email, files and calendar so it can help you with them. Each assistant works only for the person or team it was assigned to. Data connected by one person is never made available to another person's assistant. In a shared team space, messages are visible to the members of that space, and each message shows who wrote it.

3. Information we collect

Information you give us directly

- Messages, voice notes, files, photos and documents you send to your assistant.
- Your name and the contact details you choose to share.
- Preferences, corrections and instructions you give your assistant (for example, "don't use emojis" or "always confirm the currency").

Information about your devices

- The devices you add to your account (for example, "iPhone · Safari"), when each was added and last used, and which one is your main device.
- If you turn on notifications, a push subscription for that device. By default the lock screen shows only who wrote to you, not the message. Notifications are encrypted so that the push services that deliver them cannot read them.

Information from accounts you connect (optional) If you choose to connect an account, your assistant may access it with your explicit authorization:

- **Google:** Gmail (read messages, and compose and send messages when you ask), Google Drive (list, search, read, create, rename, move and share files when you ask), Google Calendar (read and create events when you ask).
- **Microsoft:** Outlook email, calendar and files, with the same kinds of actions, only when you ask.

You choose what to connect. Each connection is authorized by you through the provider's own consent screen, and you can revoke it at any time (see Section 8). **Information generated while your assistant works**

- Conversation history with your assistant.
- Notes your assistant keeps to remember your preferences and ongoing matters.
- Transcriptions of audio you send.
- Technical logs needed to keep the Service running (timestamps, error messages, message identifiers). We mask known secret formats, such as passwords and access tokens, in logs.

Billing information

- If you pay for the Service, your payment is processed by our payment provider. We receive your subscription status and billing details, never your full card number.

Our website

- stellorient.com uses no cookies and no analytics. The demo form opens your own email program; the website itself stores nothing.

4. How we use information

We use your information only to:

- provide the Service you requested and answer your messages;
- perform the actions you ask for in accounts you connected (for example, draft a reply to an email or create a calendar event);
- remember your preferences so you don't have to repeat them;
- manage your subscription and devices;
- keep the Service secure, detect failures and fix them;
- comply with the law.

We do not use your information for advertising, and we do not sell it, rent it or share it with data brokers.

5. Google user data and the Limited Use requirements

Our use and transfer of information received from Google APIs adheres to the Google API Services User Data Policy, including the Limited Use requirements. Specifically:

- We only use Google user data to provide and improve the user-facing features of the assistant you connected the account to.
- We do not transfer Google user data to third parties except as necessary to provide those features (see Section 6), as required by law, or with your explicit consent.
- We do not use Google user data for advertising.
- Our administrators can technically reach the systems where this data is stored, because they operate them. We do not read Google user data except with your explicit consent for a specific message or file, when necessary for security purposes (such as investigating abuse), to comply with applicable law, or when the data is aggregated and anonymized for internal operations.
- We do not use Google user data to develop, improve or train generalized artificial intelligence or machine-learning models.

6. Service providers (sub-processors)

To provide the Service we rely on a small number of providers that process data on our behalf, under contractual confidentiality and security obligations:

Google user data is shared with these providers only to the extent needed for the feature you asked for (for example, the text of one email so your assistant can draft a reply). It is never shared for a provider's own purposes.

7. Where and how we store data; retention

Service data is stored on servers in the United States, protected by firewalls and access controls. Access tokens for connected accounts are stored on our servers, readable only by the assistant that needs them and by authorized administrators.

- Conversation history and notes are kept while your assistant is active, so it can keep helping you.
- Connected-account tokens are kept until you disconnect the account or the Service ends.
- When you remove a device from your account, its notifications are deleted.
- Files sent in the app's chat are deleted from the delivery server after 7 days. Some temporary files (for example, audio after transcription) are deleted as soon as they are processed.
- Backups are encrypted and retained for a limited rolling period.
- When your Service ends, we delete your working data within 30 days, keeping only what we must retain by law (for example, invoices and signed agreements).

8. Your choices and rights

- Disconnect an account at any time by asking your assistant, or by removing Vertiza from your Google account permissions (myaccount.google.com/permissions) or your Microsoft account permissions. Disconnecting deletes the stored token for that account.

- Remove any device from your account in the app's Settings, or from your account area at app.stellorient.com/mi-cuenta.
- See, correct or delete your data: write to info@stellorient.com. We will respond within 30 days.
- Ask your assistant to forget a note or preference at any time.

Depending on where you live, you may have additional rights under laws such as the California Consumer Privacy Act or Colombia's Ley 1581 de 2012. We honor those rights on request.

9. Security

We use encryption in transit (TLS), encrypted notifications that push services cannot read, encrypted backups, masking of known secret formats in logs, approval from you before any irreversible action your assistant takes on your behalf (sending an email, sharing a file, deleting a document), new devices approved from a device you already use, and continuous monitoring. No system is perfectly secure. If we learn of a breach affecting your data, we will notify you without undue delay.

10. Children

Vertiza is a business tool and is not directed to children under 13. We do not knowingly collect information from children.

11. Changes to this policy

We will post any changes on this page and update the "Last updated" date. If a change materially affects how we use your data, we will also tell you directly.

12. Contact

Vertiza · ME Film Studios LLC · info@stellorient.com

Copy of the document published at https://stellorient.com/privacy/