Comms – Privacy Policy

1. Introduction

Astral Technologies, SLU ("we", "our", "us") publishes **Comms** (the "App"), a messaging and calling application for iOS, Android, Windows, macOS, Linux and the web. The App connects to a Comms server that an organization runs for its members (the "Server"). This Privacy Policy explains what data the App handles, where it goes, and who controls it. For the purposes of this Privacy Policy, "you" or "your" refers to the individual end user of the App.

Summary: The App sends your data only to the Server you sign in to, which your organization operates, not us. Messages, files, voice messages, reactions, polls, locations and calls are end-to-end encrypted, so the Server cannot read them. We receive no data from the App, and it contains no analytics, advertising or tracking.

Scope: This Privacy Policy applies exclusively to the App. The organization operating your Server decides how the Server keeps and uses your data, and is responsible for it (the controller, under the GDPR). The Server may disclose its own privacy policy ("Server Privacy Policy") to the App, which will display it when you connect. Otherwise, ask the organization for it. Where we operate a Server ourselves, for our own team or for testing, we are that organization. For information about data collected when you visit our website(s) or communicate with us, see our global Privacy Policy at: https://astral.tech/privacy.

2. Your data

On your device. The App stores your messages, files, contacts, settings and encryption keys, so that it works offline.

On the Server. The App sends to the Server what it needs to provide its functionality:

- **Account and profile**: Username, full name, display name, about text, profile pictures, and, if you add them, email address and phone number. Other users of the Server can see them.
- **Credentials**: Your password, which the Server stores only as a hash, and your two-factor authentication secret, if you turn it on.
- **Devices**: Each signed-in device's name, platform, App version, public keys and push notification token, and when it was last seen.
- **Encrypted content**: Your messages, media, files, reactions, polls and locations, all encrypted with *message keys* generated on the chat participants' devices. Your message keys are backed up to the Server, encrypted with your *recovery key*, which the Server never sees. Calls pass encrypted through the Server.

- **Metadata**: Which conversations you are in, group names, topics and profile pictures, who sent each message to which conversation and when, sizes, read markers, typing indicators, mentions and call participation. The Server also sees your IP address when you connect. On the web, your browser may also send additional metadata such as its name, version, device operating system and architecture and your preferred languages.

3. Third parties

The App contains no third-party analytics, advertising or tracking code. It reaches services other than the Server only in these cases:

- **Push notifications**: The Server sends notifications through Apple Push Notification service, Firebase Cloud Messaging (Google) on Android, or your browser's push service on the web. Notifications carry the message encrypted, with identifiers such as the conversation's, never names or readable content. On Android, Google's Firebase Messaging library registers your device with Google for this.
- **Link previews**: When you send a link, your device fetches the page to make a preview, so the website sees your IP address. On the web, the Server fetches it instead. Recipients never contact the website. You can turn link previews off in the App's settings.
- **Locations**: When you share a location, your device fetches the map image through the Server, from the map service the Server uses (OpenStreetMap by default). The Server and that service can see which area the map shows.
- **Video codec**: On Windows and Linux, the App may download Cisco's OpenH264 video codec from Cisco when it first needs it.
- **Crash reports**: If you allow your device to share diagnostics with app developers, Apple or Google may make crash reports available to us, which contain technical data about the crash and your device, and could contain traces of your data. We use them only to fix the App, on the basis of our legitimate interests (Art. 6(1)(f) GDPR).

4. Your rights

Depending on where you live (for example the EU/EEA, UK, certain US states, Brazil, Canada and other jurisdictions), you may have legal rights over personal data, such as to access it, correct it, delete it, export it, object to certain processing, restrict processing, or lodge a complaint with a supervisory or regulatory authority.

You can exercise such rights within the App using the App's own functionality, for instance to edit your profile, delete your messages or unlink your devices. Where applicable, the App will transmit such

requests to the Server. For other requests about data on the Server, contact the organization operating it.

We do **not** “sell” or “share” personal information (CCPA/CPRA definitions) and we do not perform automated decision-making or profiling about you.

5. Data retention

The App’s data on your device remains until you sign out or uninstall the App.

If you voluntarily e-mail us a diagnostic file, you can request its deletion at any time; we delete support copies within 30 days after resolving your request, or sooner upon request.

The organization operating the Server decides the data retention practices relevant to your data on the Server. Please refer to their Server Privacy Policy.

6. Data security

Message keys are end-to-end encryption keys, created on the chat participants’ devices. Your *recovery key* decrypts the encrypted backup of your message keys on the Server, so that a new device can read your past messages. We cannot recover any encryption keys for you, so keep your recovery key safe. If the organization running the Server completes your account setup on your behalf, issuing your recovery key, assume that end-to-end encryption is not guaranteed.

The App’s data on your device is protected as follows:

- **Mobile** (Android, iOS): Protected by the operating system’s encryption and your choice of lock screen. The App keeps it out of device backups and phone-to-phone transfers.
- **Desktop** (Linux, Windows, macOS): Protected by your choice of disk encryption such as BitLocker or FileVault, anti-malware and lock screen. Your computer’s own backups may include it.
- **Web**: Protected by the mobile or desktop operating system as indicated above. Your web browser keeps it in its storage, or only in memory if you choose not to keep data on that browser during sign-in.

In all cases, we recommend that you maintain appropriate security measures on your device, keeping the operating system updated and free of malware in order to safeguard your data in the App.

The App enforces encryption in transit for all its communication with the Server.

The organization operating the Server decides the data security practices relevant to your data on the Server. Please refer to their Server Privacy Policy.

7. Children's privacy

The App is not directed to children or minors. We do not knowingly receive data from individuals under 13 (or any higher age threshold requiring parental authorization in your jurisdiction). If a minor's data is sent to us in a support request, we will delete it.

8. Policy changes

We may update this Privacy Policy to reflect internal or legal changes. The date in the header of this document will change, and significant changes will be announced within the App before they take effect. Continued use after an update indicates acceptance of the revised Privacy Policy.

9. Contact information

If you have any questions about this Privacy Policy or need assistance to exercise your rights, please contact us at:

> **Astral Technologies, SLU**
> Carrer de l'Obac 8, 5-1
> AD700 Escaldes-Engordany
> Andorra

Or by email at: privacy@astral.tech

If you are in the EU/EEA or UK and believe we have not resolved a privacy concern, you can lodge a complaint with the Andorran Data Protection Agency (APDA) or your local supervisory authority.