Trax – Privacy Policy

1. Introduction

Astral Technologies, SLU ("we", "our", "us") publishes the Android application **Trax** (the "App"), whose purpose is to help track —and optionally, gather evidence of— stays in jurisdictions and their length for personal tax residency monitoring (the "Purpose"). This Privacy Policy explains, in plain language, how data is obtained, used, stored, and controlled within the App. For the purposes of this Privacy Policy, "you" or "your" refers to the individual end user of the App.

Summary: The App works entirely offline; it processes data needed for its Purpose only on your device and never sends it to us or others. Your data may only leave your device if you manually export it or your device's system backup copies it.

Scope: This Privacy Policy applies exclusively to the App. 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

In order to satisfy its Purpose, the App processes the following data locally on your device:

- **Precise location**: Location events containing your device's geographic coordinates, obtained from *Global Navigation Satellite System* (GNSS) sources such as GPS, and the associated timestamp. Location events are obtained (1) manually, on your request or (2) automatically, according to your tracking preferences.
- **Jurisdiction history**: History of visited countries, including entry and exit dates for each visit and total duration of the stay. Such information is either declared by you manually or inferred from the recorded location events.
- **Selfie pictures** (optional): Pictures may be manually taken by the user to evidence device possession (e.g. selfie taken with a device camera) when capturing the current location. No facial recognition or biometric template creation is performed.
- **Device attestations** (optional): Location events may be digitally signed using hardware-backed keys. Cryptographic signatures and related system integrity metadata are used to evidence device integrity when capturing the current location. No remote integrity verification takes place.
- **Settings and preferences**: Local configuration of the App (home jurisdiction, tax residency thresholds, tracking preferences, etc.)
- **Diagnostic information**: Technical logs used for troubleshooting.

Such data processing is carried out on the basis of our legitimate interests in providing the App's functionality (Art. 6(1)(f) GDPR).

3. 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.

Because your data is processed only within your device, requests to exercise such rights are normally fulfilled directly by you within the App using the App's own functionality.

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

4. Data retention

All App data remains only on your device until you manually reset/delete the data using the App's own functionality or uninstall the App entirely.

If you voluntarily e-mail us an export or 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.

5. Data security and privacy

Your data is stored inside the App's private storage managed by your device's operating system, and is further protected by the device's encryption and lock screen. Therefore, to safeguard your data we recommend that you maintain appropriate security measures on your device, keeping the operating system updated and free of malware.

The App does not request Internet or network access permissions and is designed to operate fully offline; it does not send your data to us. We do not maintain servers, back-end databases, or cloud storage. There is no remote attack surface related to your personal data.

The only two ways your data can leave your device are:

- **Manual exports**: Using the App's export functionality you can generate a single file containing all your data and choose whether to share it. Both creation and sharing are entirely user-initiated.
- **System backups**: If you have enabled system-wide device backups, e.g., Android backup to a Google Account, the operating system may include the App's data in such device backups. That backup process is controlled solely by the operating system and its provider, and is subject to that provider's privacy policy, not this Privacy Policy. You can disable or manage system backups in your device settings.

6. 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.

7. 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.

8. 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.