Astronort Data Protection Assurance

Sam Minnée • CTO • Version 1.3 • 1 May 2024

In order for Astronort to provide its service, we require that you send us sensitive documents such as strategic plans, management reports, and board reports. It is therefore critical that you have confidence in how we take care of your data.

This document describes what we will do with documents that you provide us, and how we will ensure that we safeguard their confidentiality.

Who will have access to your documents?

- "**Astronort Personnel"** are the 3 founders: Diana Minnée, Rebecca Wrightson, and Sam Minnée.
- The "**Astronort Engineer"** is Sam Minnée.
- Astronort Personnel may read both the documents you provide us and the reports generated, in order to assess & improve the quality of the reports.
- All Astronort Personnel who will be given access to your documents will be named in an NDA we sign with you.

Where will we store your documents?

- We will receive documents (**"Customer Documents"**) via a **"Shared Cloud Folder"** in either Dropbox, Google Drive, or iCloud Drive at your preference,

and retain them on a shared drive for the duration of our access to them. We recommend that this is done with a folder under your control and shared with us.

- We expect that the Shared Cloud Folder will be shared with the Astronort Engineer for the duration of our work with you. Selected documents may be shared with the Astronort Personnel if necessary to review & improve the quality of our reports. All such access will be granted only through appropriately hardened devices and Astronort cloud accounts.

What third-parties will you send our information to?

Linode

- Our production infrastructure run's on Akamai's Linode service in California. Their Master Service Agreement and Data Processing Addendum is available online. The infrastructure is hardened according to our Cloud Infrastructure Hardening Standard.
- Customer Documents will be transferred to this service. We create "**Derivative Content"** summarising, transforming, filtering and analysing the documents you provide. This content will be stored on the production infrastructure, and selected documents may be copied back to the Shared Cloud Folder.

OpenAI

We use OpenAI's LLMs for processing information you provide to us. This usage is covered by OpenAI's terms.

- OpenAI terms clearly state that they own neither the input material nor the output it generates.
- We only send your information OpenAI via OpenAI APIs, which means that it is treated in clause 3(c) of their terms as "API Content". **They will NOT use your information as training data**, avoiding the risk of your data being used to generate ChatGPT responses.

RunPod

We use a custom model that we have developed, hosted on cloud hosting provider, RunPod, to analyse each page of uploaded PDFs.

- RunPod's compliance & security information is available online

Development environments

- The Astronort Engineer's laptop, appropriately hardened, is used as a development environment for our product.
- When improving the system to perform better with your documents, Customer Documents may temporary be transferred to a development machine for processing, and deleted after processing has been document.

Who can access the systems we connect to?

- The Astronort portal is available to authenticated users, with password authentication.
- Each organisation's data is stored in a separate database. In the near future, each of these databases will be separately encrypted with their own secrets keys, unlocked when authorised users log in.
- The portal will comply with our Multi-tenant Security Standard to ensure that each customer can only access their information.
- The portal will be built according our Secure Development Standard that covers security risks such as SQL Injection and XSS.

How will access by our personnel be secured?

- We protect any device that can access Astronort cloud accounts. Every such mobile & laptop devices is hardened according to our Device Hardening Standard to limit the risk of allowing access to your data if their device is compromised.
- Every Astronort cloud account complies with our Cloud Account Hardening Standard.
- Every member of the Astronort Team have their mobile & laptop devices hardened according to our Device Hardening Standard to limit the risk of

allowing access to your data if their device is compromised.

How do you test and monitor your systems?

Testing

- Changes to systems are developed without access to customer data.
- Automated tests are developed alongside changes. Prior to any changes being placed on the production platform, the tests must pass in a pre-production environment.
- Automated testing of the multi-tenant isolation is considered essential.

Monitoring

- Detailed logs of system access are kept
- The Astronort Engineer is alerted about warnings & errors and investigates them

Removal of data

Should you wish to stop working with us, we will remove your data from our systems.

- Customer Documents will be deleted.
- All Derivative Content will also be deleted.
- Customer Documents and Derivative Content can be expunged from backups on request.

Other points

- Our security contact is security@astronort.com

Supporting documents (available on request)

Device Hardening Standard

Cloud Account Hardening Standard

Cloud Infrastructure Hardening Standard

Multi-tenant Security Standard

Secure Development Standard