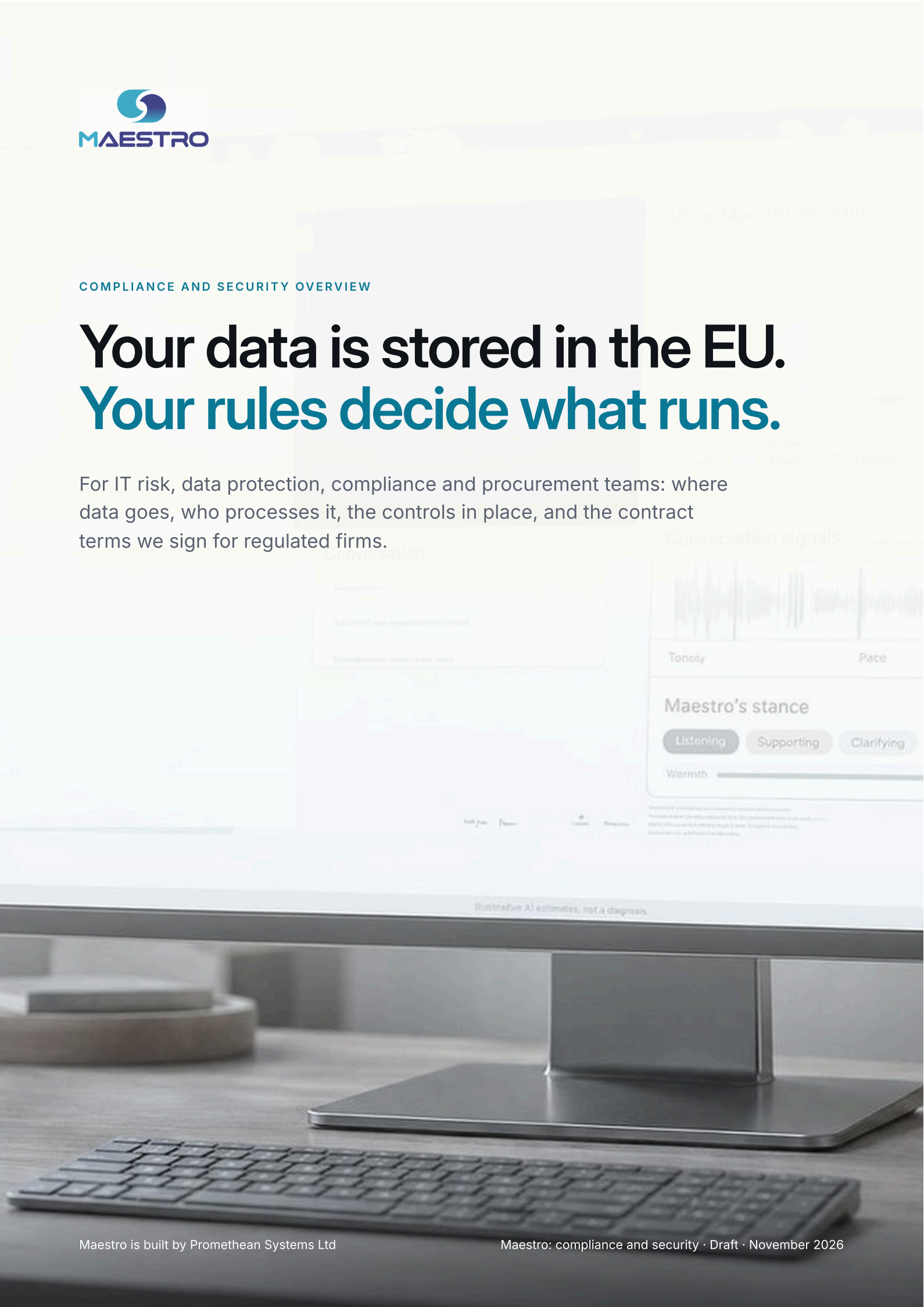
MAESTRO

COMPLIANCE AND SECURITY OVERVIEW

Your data is stored in the EU. Your rules decide what runs.

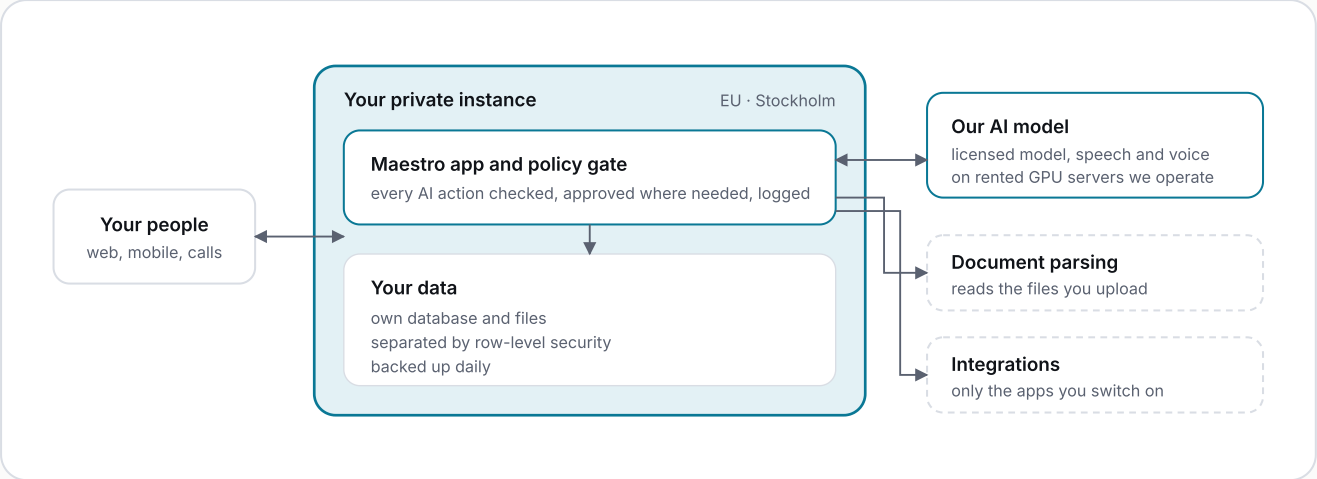
For IT risk, data protection, compliance and procurement teams: where data goes, who processes it, the controls in place, and the contract terms we sign for regulated firms.



WHERE YOUR DATA GOES

One private instance per customer, stored in the EU.

Each customer gets its own application and database. The AI is our own licensed model, run on GPU servers we rent and operate, not an outside AI provider's service.



SUBPROCESSORS

SUBPROCESSOR	WHAT IT DOES	WHERE
Amazon Web Services	Hosting, database, file storage, logs and backups	EU (Stockholm, Sweden)
Vast.ai	Rented GPU servers for our AI model, embeddings and voice	Varies by server
Unstructured	Parsing of uploaded documents	United States
Pipedream	Integrations you authorise	United States

As listed in Schedule 4 of our Terms of Service. Transfers outside the UK or EEA use the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses. We give 30 days' notice of any new subprocessor, and you can object.

EVERY ACTION GOVERNED

The AI acts inside your rules, and leaves a receipt.

1	2	3	4	5	6
Request	**Classify**	**Policy**	**Approve**	**Run**	**Receipt**
A person asks, or a workflow runs	Risk, reversibility, data sensitivity	Your rules decide what may run	A person signs off when required	With that user's permissions	An audit record of what ran

SECURITY AND DATA PROTECTION

What your IT risk and data protection teams will check.

Sign-in and access	Two-factor sign-in your admins can make mandatory. Roles, permissions, teams, an access inspector and break-glass access.
Separation	Your own application instance and database, plus row-level security in the database.
Encryption	TLS 1.3 in transit. Encryption at rest.
Infrastructure	Defined as code. No public database access, no inbound SSH, secrets held in a managed secrets store.
Roles under GDPR	You are the controller of your content; we are your processor, under Article 28 terms.
No training on your data	Your content is never used to train AI models without your written agreement.
Calls	Live audio and video are processed during the call and not stored afterwards. Tone signals adapt the assistant's speech and are never used to profile anyone.
Breaches	We tell you within 48 hours of becoming aware of a personal data breach, or 24 hours under the enterprise data processing agreement.
Backups and recovery	Daily backups kept for 30 days. Recovery time and recovery point objectives of 24 hours.
Leaving	Export your data in a common format, then we delete or return it, as you choose.

BUILT FOR YOUR RULEBOOK

We sign the terms your regulator expects.

Regulated firms have to push their own rules down to their suppliers. We add them to your contract, so your third-party risk file is complete.

DORA
EU financial entities

- Data locations and service levels
- Audit and access rights
- Incident help and notification
- Exit plan and data return

UK outsourcing
PRA SS2/21, FCA SYSC 8

- Due-diligence information
- Sub-outsourcing control
- Continuity and exit
- Facts for your supplier register

UK and EU GDPR
Every customer

- Article 28 data processing terms
- Subprocessor list with notice
- Deletion and data-subject requests

EU AI Act
AI used in the EU

- People told they are talking to an AI
- No emotion reading of your staff
- Human oversight on consequential actions

CONTRACT DOCUMENTS

Terms of Service v1.1
The contract, with service level and data processing schedules

Order form
Plan, price, users, timeline and contacts

Enterprise data processing agreement
Optional, prevails over Schedule 4

Enterprise service levels
Optional, with service credits

DORA and UK outsourcing addendum
For financial firms and outsourcing arrangements

ASSURANCE

We are a young company and say so plainly.

IN PLACE	**ICO registration** CSN9976644
PLANNED	**Penetration test** Independent, then yearly
PLANNED	**Cyber Essentials** UK government-backed baseline
ROADMAP	**ISO 27001 or SOC 2** Shared under NDA

Security policies and answers to your security questionnaire are available on request.