THE TRUST PACK

IT and procurement, answered in writing.

Where your files sit, what leaves the building, what we answer for in writing, who works on your system, and the company's facts. Last updated 18 October 2026.



Your files can stay in your office.

On one machine you own, where no vendor's cloud holds them.



Our AI's mistakes are ours to fix.

The person you name is told, and the fix is proved on twenty past jobs.



You can stop, and keep everything.

At the end of any month. Every account and every line of code is in your company's name.

Tested on twenty of your own past jobs before it goes live, and kept working as AI changes.

IN THIS PACK

Your files and security

What we answer for

Our own AI policy

What you own

What is in writing first

The company

Your files and security.

Where does it run?

On your own machine, in your office.

What leaves the building?

Three things, each one shown to you.

What is encrypted?

The whole disk, all the time.

Who can get in?

Your people, us for support, nobody else.

What does it write down?

Every step, in a log you own.

Does any model learn from our files?

Only your own, with your written yes.

Does anything reach another client?

No. Agentec is its own company.

Which data laws does it meet?

Yours, gone through and written down first.

What if something goes wrong?

You hear it from your own system first.

Which certificates do you hold?

Not ISO 27001 or SOC 2, yet.

What changes for a larger firm?

The same rules, sized to you.

Where does it run?

On one machine you own, in your office, if you choose it. Not in our cloud, not in anybody's cloud. The record, the workflow, the documents and the models that read your mail are built to run on that box, on your network. No vendor data centre holds your files, so there is no vendor data centre for your client to audit.

The machine is small: about the size of a thick book, drawing under 200 watts. It needs a cooled room and a small battery, and it is set to come back on by itself after a power cut.

If you would rather not have a machine, the AI agents can run in accounts in your firm's own name instead, with the same log, the same yes and the same stop switch. We tell you plainly what that changes about where your files sit before anything is built.

Where this stands today. The first four answers say how the machine is built to work, and on install day we prove each one in front of you and write the receipt into your log. Our own machine runs our own AI work: six kinds of it were checked on 22 September 2026, and that story is on our work page.

What leaves the building?

Three things, by design. On install day we show you each one.

A heartbeat, once an hour, going up. It says the box is alive, which versions it runs, how many jobs ran, how many are waiting, how many errors, the disk and the temperature. It carries no name, no document and no line of any job.

Signed updates, on a schedule, coming down. Each one is a sealed package checked against our signature before it is allowed to run, locked to one exact version. The box is built to run its own health checks after an update and to put itself back on the previous version if they fail.

The nightly backup, going out already sealed. It is encrypted on the box before it leaves, to storage in your own country, so the storage holds bytes nobody can read without your key.

Nothing else leaves on its own. Messages your AI agents send and receive on WhatsApp, mail or SMS go through those services, as they do today, and your proposal names each one.

What is encrypted?

If the machine were carried out of your office, nothing on it could be read.

One catch: an encrypted disk normally needs somebody to type a password when it starts, and a box that waits for a person at three in the morning stays down. So the key is sealed into a small security chip on the machine's own board, and the chip only hands it back when the same machine starts with the same startup files. Lift the disk out and put it in another machine and it opens nothing. One written recovery phrase exists for the day the board itself has to be replaced, and it never sits on our side.

On install day we prove both halves in front of you and write both receipts into your log. We pull the power at the wall and watch the box come back on its own. Then we start it once with a tampered startup file and watch it refuse.

Who can get in?

Your people, on your office network, and on a private network for phones outside the office. Nothing is exposed to the open internet.

Us, only for support, over that same private network. Every support session is recorded on your box, by your box, and the recording is yours. Nothing is ever downloaded from your machine.

Nobody else. Nobody outside the names in your proposal, no model vendor and no analytics company. The models run on your box, so there is no third party reading your mail to answer a question about it.

What does it write down?

Every step records what it read, which tool or model ran, what came back, how long it took, and who, if anyone, said yes. That record is yours, and it is what makes an audit a morning's reading instead of a project.

It can be kept for longer than the rules ask, and a copy can go to your own monitoring.

Does any model learn from our files?

With the machine, the models run on the box itself, so no model vendor reads your files at all. Without the machine, we tell you plainly which provider reads what before anything is built, and it is written down.

Does anything reach another client?

Agentec keeps every client's work apart: separate accounts, separate machines, separate logs. Nothing learned on your work is carried to another client's.

Which data laws does it meet?

India's data protection rules, and when they bite. The Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025. From May 2027 they ask every company that holds people's data to give a plain notice of what it collects and why, and to keep its logs for a year. A breach goes to the Data Protection Board in full no later than 72 hours after learning of it. What we build is made to meet them: the log stays on your own machine for as long as the rules ask, and the alert reaches the person you name at once, so your report can go in on time.

When we meet, we go through what your own law asks of you, India's DPDP Act, Singapore's PDPA, the UK GDPR or any other.

What if something goes wrong?

India's CERT-In directions of April 2022 give a company six hours from noticing an incident to report it, so the alert reaches you first, from your own system. Out of the support hours your agreement sets, an AI agent that stops stays stopped, and your team works the old way until we are back. What happens when an AI agent gets a job wrong is on our page of what we answer for.

Which certificates do you hold?

What we can show you now. This page and the trust pack, in writing and dated. Our own AI policy, in writing. Our own machine at work, with the six kinds of AI work checked on it on 22 September 2026. The audit that checks every automation on our own machines each night, and the guards that watch them, both on our work page with their dated counts.

What changes for a larger firm?

For a firm of thousands, the proposal sets each of these out in writing before anything is built.

Where it runs. In your own cloud account or your own data centre, sized to your load, where one machine in one office is too small. Two machines with failover, where you choose machines.

Who gets in. Through your own single sign on, so access follows the joiners and leavers you already manage.

Recovery. The recovery point is the last nightly backup. The recovery time is never quoted from a brochure.

What we answer for.

Your yes, our answer →

Your yes covers what you saw. We answer for the work under it.

Stop, tell, fix →

A failing AI agent stops itself, you are told,
the fix is proved, and we write it down.

People, by name →

Who works on your system, who signs, and who you escalate to.

Our own AI policy →

What our AI agents may do alone, and what always waits for a person.

What we won't build →

Five things we turn down, whoever asks.

The terms →

The price in writing, AI said plainly, and the exit.

Our own AI policy.

It binds the AI agents we run for you and our own. As it stands on 13 October 2026.

MAY DO ALONE	ALWAYS WAITS FOR A PERSON
✓ Read	⏸ Spending money
✓ Sort	⏸ Signing
✓ Draft	⏸ Filing with an authority
✓ Check	⏸ Deleting a record
✓ File	⏸ Any message outside the rules

What you own.

- Every account and every line of code is in your company's name from day one.
- Your data, rules, prompts, templates and logs stay yours.
- The systems we build for you, and the machine if you choose one.
- If either of us stops, everything comes to you as plain files with a written guide any developer can follow.

What is in writing first.

Each of these is in your hands, in writing, before anything is built.

The scope, the plan and the price	In a written proposal, before you commit to anything: one fixed price, before any work.
Who works on your system	By name, with what each has built, and who may reach it for support.
Who else handles your data	With the machine in your office, nobody. In accounts in your firm's name, each provider is named, with what it reads.
Support and incidents	The support hours, what your own system does at night and at weekends, and how you hear from us.
Changes and reviews	How a change is asked for and tested on your own past jobs before it reaches live work, and a review each quarter.

The company.

Company	Agentec Intelligence Private Limited
CIN	U63999KA2026PTC225775
Registered	Bengaluru, Karnataka, India
GST	Registered in Karnataka since 23 September 2026
Founder	Eashan Gupta
Write to	hello@agentec.cloud
Online	agentec.cloud/trust