Our data handling principles

What protects every conversation Ava handles.

Encryption and access control

Data is encrypted in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent), with keys rotated regularly. Access follows least privilege, multi-factor authentication protects privileged operations, and every admin action is logged.

Governance and assurance

The platform's information security framework is aligned with ISO 27001, ISO 9001 and Cyber Essentials Plus, with annual control assessments and policies reviewed every year.

Monitoring and testing

Infrastructure and applications are monitored continuously, independent penetration testing takes place at least once a year, and a formal incident response plan is backed by 24/7 monitoring.

UK GDPR and your role

Ava is set up to support UK GDPR, EU GDPR and the Data Protection Act 2018. You remain the data controller, and your data is processed only on your instructions and for agreed purposes.

Responsible use of AI

Your call data is never used to train or improve generic AI models. It's processed only to run your own Ava setup, and AI components are assessed for security and data handling before use.

Retention, deletion and hosting

Your data is kept separate from other customers, retained only as long as needed, then securely deleted or anonymised. It's hosted on secure public cloud infrastructure, with data residency options.

This is a summary for evaluation purposes, not a formal audit report or attestation. Certification and audit details are available on request; please confirm current status as part of your own due diligence.

Frequently asked questions

The questions business owners and IT partners ask us most.

Do callers know they're speaking to AI?

Yes. Ava introduces herself as an AI assistant at the start of every call. Transparency is part of every setup as standard.

Who is the data controller?

You are. Wicomms and our platform provider act as processors, handling your callers' information only to deliver the service you've asked for.

Is our call data used to train AI?

No. Your data is never used to train or improve generic language models.

How is data protected?

Encrypted in transit and at rest, with least-privilege access, multi-factor authentication for privileged operations, and logged admin activity.

Where is it hosted?

On secure, compliant public cloud infrastructure from leading providers such as AWS, Google Cloud and Microsoft Azure, with data residency options available.

Who else processes our data?

A small number of vetted providers support hosting, AI processing and telephony, all bound by Data Processing Agreements with equivalent safeguards.

How long is data kept?

Only as long as it's needed for the service, such as call summaries and reporting. Retention can be set to suit your business, then data is deleted or anonymised.

What happens if we leave?

Your data is deleted or returned in line with your contract and legal obligations.

What if there's a security incident?

A formal incident response plan covers escalation and communication, with 24/7 monitoring. You'll be told where the law requires it.

What do we need to do on our side?

Keep access to your call summary emails secure, use multi-factor authentication on your email, and tell us if your team changes so we can update routing.