Argus

Security, Privacy & AI

Last updated October 21, 2026

When you connect Argus, you are handing us the most important channel in your business: the conversations with the people who pay you. Those messages hold your customers' names, addresses, and phone numbers, your prices, and your reputation. We treat that trust as the foundation of everything we build. This page sets out, in plain language, how we protect your data, what we will and will never do with it, and how we use AI responsibly on your behalf.

Never sold, never advertised to

We do not sell your data or your customers' data, and we never use it for advertising.

Never used to train AI

Your mail, calls, and documents are not used to train our models or our AI providers' models.

Encrypted everywhere

Your data is encrypted in transit and at rest.

Independently assessed

Verified by Google, including an annual third-party CASA security assessment.

You stay in control

You decide what the AI may send on its own, and you can disconnect or delete at any time.

No quiet access

Our staff cannot browse your account. Support access is controlled, time-limited, and recorded.

Our principles

- **Collect only what the job needs.** We ask for the narrowest mailbox, calendar, and phone permissions that let Argus do its work, and each one maps to a feature you can see.
- **Use it only for you.** Your data exists in Argus to answer your customers and run your front office. It is never repurposed for anyone else.

- **Keep you in charge.** Automated behaviour can be reviewed, paused, or switched off, and your data can be exported or deleted on request.
- **Say what we do, and do what we say.** This page describes how we operate today. When that changes, this page changes with it.

Security

Infrastructure and encryption

- Argus is hosted with a leading cloud provider in the United States, in isolated environments that are not exposed to the public internet beyond what the service requires.
- All data is encrypted in transit and at rest. The credentials that connect us to your mailbox receive an additional layer of encryption.
- System credentials are held in a managed, encrypted secret store — never in source code.
- Data is backed up automatically.

Account protection

- Most customers sign in with Google or Microsoft, so we never see or store those passwords. Any password we do hold is stored only in strongly hashed form.
- Sessions are short-lived and can be revoked.
- Each account's data is kept strictly separate from every other account's.
- Team members get role-based access, limited to what their job requires.

How our own staff access data

Nobody at Argus has a standing window into your account. When we need to see what you see — usually because you have asked for help — access must be justified, is granted only for a limited time, and is recorded against the named person who used it. Access to production systems is restricted to the few people who need it.

Secure development and operations

- Connections from our integration partners are verified before we act on them.
- We follow established web security practices, including protections against common attacks and abuse.
- Changes are reviewed and tested automatically before release, and we continuously monitor the software we depend on for known vulnerabilities.

Independent assessment

Because Argus works inside Gmail, Google requires us to pass its **Cloud Application Security Assessment (CASA)**, carried out by an independent, Google-authorised security lab and renewed every year. We have completed that assessment and our app is verified by Google.

If something goes wrong

No system is perfectly secure, and we do not pretend otherwise. What we promise is vigilance and candour: if a security incident affects your information, we will investigate it immediately, contain it, and notify you — and any regulator the law requires — without undue delay, telling you what happened and what we are doing about it.

Privacy

What we will never do

- Sell your data or your customers' data.
- Use it for advertising, or pass it to advertisers, data brokers, or resellers.
- Use it to train artificial intelligence models — ours or anyone else's.
- Let people read your mail, except with your permission, where security or the law requires it.

Our use of data from Google adheres to the Google API Services User Data Policy, including its Limited Use requirements, and we hold data from Microsoft to the same standard.

Your customers' privacy, too

The homeowners and businesses who contact you never signed up for Argus — you did. We act as your service provider for their information, handle it only to serve them on your behalf, and route any request from them to see or delete their data.

Trusted providers

We work with a small number of established providers for hosting, AI processing, telephony, and payments. Each is contractually bound to use your data solely to provide their service to us. Card details go directly to our payment processor and never touch our systems. The full list is in our Privacy Policy.

How long we keep it, and how to delete it

- We keep your conversations and lead history while your account is active, so the assistant has the context it needs to serve your customers well.
- Disconnect a mailbox and we stop accessing it immediately. You can also revoke our access directly from your Google or Microsoft account settings at any time.
- Close your account and we delete your data within 30 days, keeping only what the law requires for accounting.
- You can delete individual leads, documents, and messages yourself whenever you like, or ask us for a copy of everything we hold about you.

Responsible AI

AI is what lets Argus answer your customers in minutes, day or night. We think that power comes with obligations, and we have built the product around them.

Your data trains nothing

Our AI providers process your content solely to return a result to us, under terms that prohibit training their models on it. We do not train models of our own on your mail, your customers' messages, or your calls.

You decide how much it does on its own

Whether a reply is sent automatically or held for your approval is your choice, and you can change it at any time. Sensitive conversations are held for a person to review.

It speaks from your facts, and asks when it doesn't know

The assistant answers from information you have provided or approved. When a customer asks something it cannot answer, it brings the question to you rather than guessing.

It never pretends to be human

If a caller or customer asks whether they are dealing with an AI, the assistant tells them the truth. It never claims to be a person.

Everything is visible

Every message the assistant drafts or sends, every call it answers, and every appointment it books is recorded in your account, so you can always see exactly what was said in your name.

Questions or concerns

If you have a question about how we handle your data, need a security questionnaire completed, or believe you have found a security vulnerability, please write to us at elliott@meetargus.io. Security reports are read by a person and answered promptly.

For the full legal detail, see our Privacy Policy and Terms of Service.

Argus Intelligence Inc.
3317 Pinot Court, Marietta, GA 30062