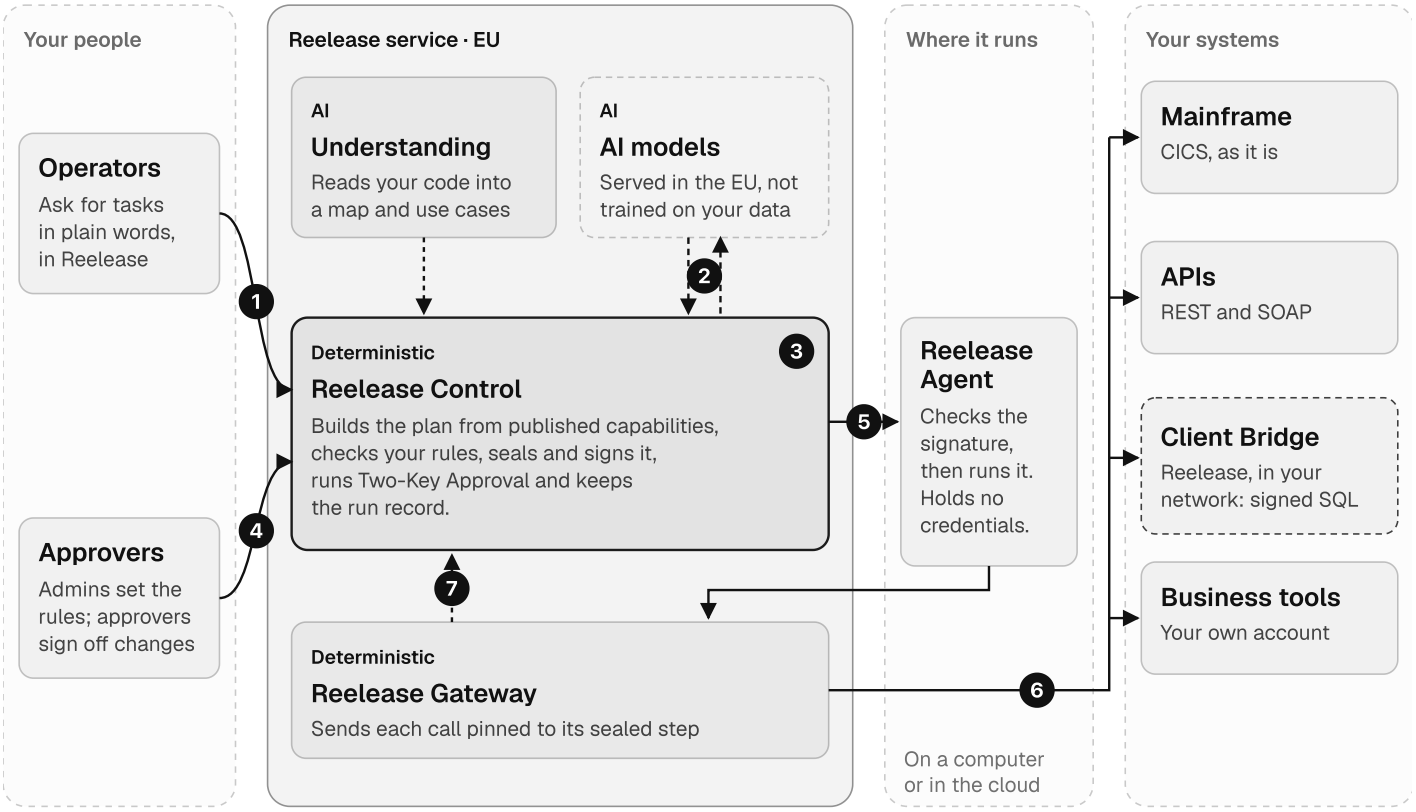
Reelease security fact sheet

Reelease is the control layer between AI and your systems: agents that start with no permissions, the approvals you define and a run record for every run. This fact sheet brings together the architecture and the facts a vendor review asks for.

Fact sheet date: 17 November 2026



1. **Ask.** An operator asks in plain language.
2. **Propose.** The model suggests a plan.
3. **Seal.** Rules validate each step; the plan is signed.
4. **Approve.** Changes wait for Two-Key Approval.
5. **Execute.** The agent verifies the signature and runs.
6. **Call.** Your system receives the sealed call.
7. **Record.** Each step lands in the run record.

Checking, sealing, approving and recording are done by Reelease, without the model.

The Reelease service runs on Google Cloud in Madrid, with its encrypted database in Frankfurt. Connection credentials are stored encrypted in Reelease and used only for the sealed call.

QUESTION	SHORT ANSWER

QUESTION	SHORT ANSWER
Control of every run	
What permissions does a new agent have?	A new agent starts with no permissions: least privilege by default. An admin turns on each capability.
Who approves sensitive steps?	You decide which steps wait for a person and who approves: human-in-the-loop approval on the steps you choose.
Can the agent skip the rules?	Rules are guardrails the agent cannot skip: what the system forbids, no agent can allow.
How do you stop an agent?	Any member with full access to the platform and the agent can suspend it at once. Only an admin can resume it.
A run record for every run	
What does each run leave behind?	Every run leaves a run record, the complete audit trail of the task: who launched it, every step, every approval and every action.
Can it be exported and kept?	It can be exported and is kept even if the agent is deleted, with retention periods per system and legal hold.
Are permission changes recorded?	Every permission change is recorded with who, when and why.
Identity and credentials	
How do people sign in?	A work account for each person. Second factor on every plan, mandatory for your whole team if you choose.
Can I use my identity provider?	On Pilot, Pro and Enterprise, sign-in through your identity provider (SSO): Microsoft Entra ID, Google Workspace, Okta or any other OpenID Connect provider.
What happens when someone leaves?	Removing someone revokes their access, accounts and computers.
Where are credentials kept?	Credentials are stored encrypted (AES-256) and never reach the operator's computer.
Data	
Is my data copied?	Your data is queried, not copied: the agent looks up what it needs at run time.
What is stored, and how?	The configuration, the knowledge of your systems and the record of every run are stored encrypted.
What happens to the code I provide?	The code you provide for analysis is read in a temporary workspace, and a ZIP is kept for 8 days at most.
Where is my data?	EU data residency: with our service, your systems' information stays in the European Union, with services in Madrid and the database in Frankfurt.
AI models	
Who chooses the model?	You choose the model for each system and each agent: the ones Reelease offers, your own provider or an open-weight model on your own servers.
Is my data used for training?	No AI provider trains its models on what the agent reads.
What if the model isn't available?	If the chosen model isn't available, the task stops: it never switches to another provider.
Where do Reelease's models run?	The models Reelease offers run inside the European Union.
Where Reelease runs and where the agent works	
Where does Reelease run?	Reelease runs as a service in Madrid, in your cloud, on-premises or in isolated mode. Isolated mode is air-gapped: no outbound connection at all.
How is each cloud run isolated?	In the cloud, each run works in its own disposable space, with no internet access and no access to other runs.
And on the operator's computer?	On the operator's computer, the Reelease Agent works in an isolated folder for each run. The desktop is used only with the operator's consent.

QUESTION	SHORT ANSWER

Compliance

Which regulations does it help with?	Reelease is designed to help you comply with GDPR, the EU AI Act, DORA and NIS2. **EU AI Act** Arts. 12, 14 and 26 **DORA** Arts. 9 and 28 to 30 **GDPR** Arts. 5, 28 and 32 **NIS2** Art. 21
Who carries out the assessment?	The compliance assessment is yours. You get the product's controls, the traceability of every run and the documentation to carry it out.
And in the public sector?	Public sector: each body applies Spain's National Security Framework (ENS), and Reelease can run on your premises if you need it.

Reporting an issue and response times

How do I report a security issue?	If you find a security issue, write to security@reelease.io with the steps to reproduce it. We confirm receipt and keep you informed until it is resolved.
How fast does support respond?	First response from support: on Pilot, urgent requests within 4 business hours and everything else within 1 business day; on Pro, in under 1 hour; on Enterprise, by contract.
During what hours?	Hours are Monday to Friday, 9:00 to 18:00 Madrid time, excluding Spanish national holidays. These are first response targets; a contractual SLA is available on Enterprise.

Legal texts

Data processing agreement Subprocessors Privacy policy Legal information