The questions you were going to ask anyway.

The awkward ones, answered before you have to send them.

SECURITY AT A GLANCE

If a developer sent you this page, start here. Every answer below is one we confirm in writing, in our DPA, sub-processor list or your security questionnaire.

YOUR DATA

DATA SENT OUT
Your prompts, the files the agent reads for a task, and the session history of that task.

PROCESSED BY
Open-weight models on inference providers located in the EU, through Melious. No fallback outside the EU.

INFERENCE RETENTION
Zero. Prompts and code are processed in memory and not logged. Our inference partner is bound to this by contract.

STORED BY ZOOID
Account details, session history and logs, in EU data centres, encrypted in transit (TLS) and at rest. Kept until you delete them, per session or all at once. Session history can contain code excerpts and diffs.

MODEL TRAINING
Never. Not by us and not by our inference partner. The companies that make the models never receive your data.

INCIDENTS
If a breach affects your data, we notify you within 48 hours of becoming aware, so you have time for GDPR's 72-hour deadline.

CONTROL AND ACCOUNTABILITY

VENDOR
Zooid, based in Gent, Belgium. European-owned, with no US parent and no US subsidiary.

GDPR ROLE
Zooid acts as your processor under Article 28. You stay the controller. We sign a DPA.

SUB-PROCESSORS
EU-based only. You get the full list with locations, advance notice of any change, and the right to object.

AGENT PERMISSIONS
Runs on the developer's machine with that developer's access. Every file read, edit and command is shown, and gated actions wait for approval.

CERTIFICATIONS
No ISO 27001 or SOC 2 report yet. Our controls follow ISO 27001 Annex A, and certification is on our roadmap.

SECURITY CONTACT
Luigi, co-founder and security officer. security@zooid.app reaches Luigi directly, not a ticket queue.

STRAIGHT ANSWERS

01 The demo shows DeepSeek. Does our code go to China?

No. Open-weight means we run the model itself, on EU hardware, through Melious. DeepSeek, Mistral, Alibaba and the other model makers never receive a request, a prompt or a line of your code. They published the model; they are not in the loop.

02 No ISO 27001 yet. Why should we trust you?

Fair question. Our controls follow ISO 27001 Annex A, and certification is on our roadmap. Until then, we are still working through the full mapping ourselves, so tell us which controls your review depends on and we will show you how they are handled today.

03 What happens if something goes wrong?

If a breach affects your data, you hear from us within 48 hours of us becoming aware, with what happened, what was affected and what we are doing about it. That leaves you time for your own 72-hour GDPR notification.

04 We found a vulnerability. Where do we report it?

Email security@zooid.app. It reaches Luigi directly. We do not threaten researchers who report in good faith, and we will tell you when it is fixed.

JURISDICTION — STORED IN THE EU IS NOT THE SAME AS SAFE FROM US LAW

01 Can a US court order reach your data?

US-BASED PROVIDER, EVEN IN AN EU REGION

Yes. Since 2018 the CLOUD Act lets US authorities compel US providers to disclose data in their possession, custody, or control, even when it is stored in the EU.

ZOOID

No. There is no US parent or US subsidiary to serve that order on, and our sub-processors are European companies too.

02 Does an EU data centre protect you?

US-BASED PROVIDER, EVEN IN AN EU REGION

Not on its own. In June 2025, Microsoft France told the French Senate under oath that it could not guarantee EU customer data would never be handed to US authorities.

ZOOID

It does when the owner is European too. EU servers, run by EU companies, under EU law only.

03 Which law decides on foreign requests?

US-BASED PROVIDER, EVEN IN AN EU REGION	ZOOID
Both, and they conflict. US law can compel disclosure, while GDPR Article 48 only recognises foreign orders based on an international agreement.	EU law only. A foreign authority has to go through a mutual legal assistance treaty and a European court.

04 What about US intelligence surveillance?

US-BASED PROVIDER, EVEN IN AN EU REGION	ZOOID
US providers fall under US intelligence laws such as FISA Section 702. Those powers are why the EU's top court struck down Privacy Shield in Schrems II (2020).	Section 702 cannot compel EU companies to hand anything over, and only EU companies process your prompts and code.

05 Is the legal basis for transfers stable?

US-BASED PROVIDER, EVEN IN AN EU REGION	ZOOID
Transfers rely on the EU–US Data Privacy Framework, the third attempt after Safe Harbor and Privacy Shield were struck down. Its validity is now on appeal at the EU Court of Justice.	Not needed. Nothing is transferred to the US, so there is no transfer mechanism to depend on, or to lose.

security@zooid.app · Zooid, Gent, Belgium

A plain-language summary, not legal advice.

Sources: US CLOUD Act (2018), 18 U.S.C. § 2713 · GDPR Article 48 · CJEU C-311/18, Schrems II (2020) · EU General Court T-553/23, Latombe (2025), on appeal as C-703/25 P · French Senate inquiry hearing, 10 June 2025