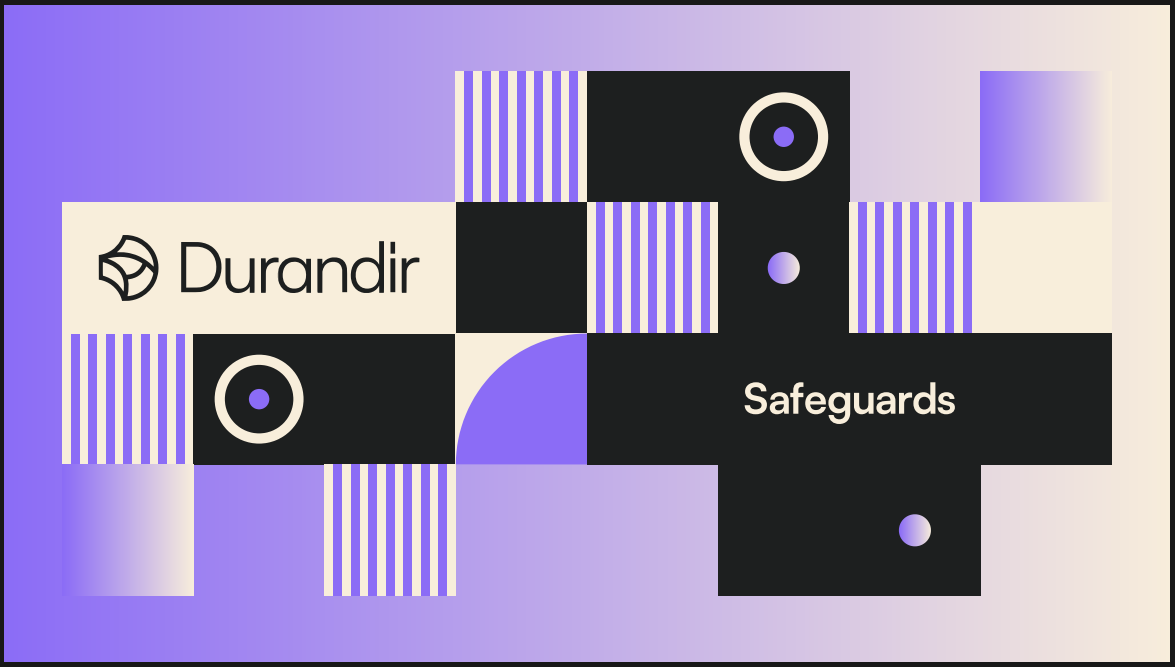
Safeguards



Published	Nov 13, 2026
Category	Security

Every request to a Durandir product is checked against a set of safeguards before any work begins.

A safeguard is a rule that decides whether a request can go ahead. It looks at two things: what is being asked, and whether your account is allowed to ask for it. If the answer is no, the request stops before anything runs, and the product tells you why.

Safeguards let Durandir products be powerful investigation tools without becoming tools for harm. They put two commitments into practice: we comply with the law that governs artificial intelligence, and we keep sensitive capabilities in the hands of the people authorised to use them.

How safeguards work

- They act first. Every request is checked before processing starts. A stopped request runs no tool and produces no answer.
- They are the same everywhere. The same rules apply in every product, whichever AI provider or model your account uses.
- They are enforced by Durandir. Our own services apply them, so they behave the same on every device and installation.

- They judge the request, not the wording. Rephrasing a request does not change the outcome.
- They are never silent. You are always told which safeguard applied and why.

Why a request can be stopped

A request is stopped for one of two reasons: the law does not allow it, or it needs a capability your account does not have.

Regulation

The EU Artificial Intelligence Act (Regulation (EU) 2024/1689) prohibits AI practices that pose an unacceptable risk to fundamental rights. Among them, Article 5 prohibits biometric categorisation systems that infer sensitive characteristics of a person, such as their sexual orientation, political opinions or religious beliefs.

Durandir applies the same principle to every request, whatever the source of the data: our products do not infer this kind of information about a specific person. A request to determine someone's sexual orientation, for example, is stopped.

Cybersecurity

Some capabilities are dual-use: the techniques that help defend a system can also be used to attack it. Durandir reserves them for accounts with Cyber or Government access, which we grant to organisations after reviewing their intended use. On any other account, a request that needs one of these capabilities is stopped.

Access levels

Every Durandir account has one access level. Durandir assigns it, and it applies across all Durandir products.

- Standard: the general capabilities of each product. Regulatory safeguards and cybersecurity restrictions apply.
- Cyber: everything in Standard, plus the cybersecurity capabilities. Regulatory safeguards apply.
- Government: the full set of capabilities, for eligible public bodies under a separate agreement. Its use remains subject to the legal framework that governs each organisation.

When a request is stopped

The product shows a Request stopped notice. It names the reason, regulation or cybersecurity, and links to this page. Nothing else happens: no action is taken and no answer is given.

A stopped request is not the same as an ignored one. Some products set aside messages that fall outside their purpose, such as a question unrelated to an investigation. Those show a Request ignored notice and can simply be rephrased. A Request stopped notice always comes from a safeguard and always states its reason.

Questions about your access

If you think a request was stopped by mistake, or you want a different access level, open Support in Durandir Platform and choose the product concerned.