

SIG AI • GÉANT Project

AI Guidelines for the Project

Magdalena Rzaca

GDPR Coordinator, GEANT Project

A practical story about using AI with confidence, clarity, and human accountability.

From principles to daily practice

A clear operating standard for project participants, work packages, and leaders.

Responsible AI use is not a blocker to innovation — it is how innovation becomes trustworthy.



Why this matters

The real question is not “Should we use AI?”

It is “How do we use it responsibly inside the project?”

AI is already present in analytics, generative tools, decision support, and third-party services.

The risk is not only technical failure. It is also privacy leakage, misleading output, unfairness, weak oversight, and avoidable reputational damage.

The purpose of the guidelines is simple: enable useful AI while keeping the project lawful, transparent, safe, and professional.

Goal: move fast on value, not fast into risk.



These guidelines create one shared baseline for design, development, testing, procurement, integration, and use of AI tools.

Every AI use needs accountability

The framework keeps human judgment at the center.



1

Human Oversight Owner

Each AI use case has a named owner who approves, monitors, and can intervene or stop the use.

2

GDPR Coordinator

Consult early when personal data is involved and support risk or assessment documentation when triggers apply.

3

Project participants and WP leads

Use AI responsibly, keep records, escalate incidents, and maintain an AI Use Register entry for each use.

The seven principles

What trustworthy AI looks like in practice

The guidelines turn broad ethics into concrete design and usage rules.

01 Lawfulness and ethics

Comply with law, uphold fairness, and protect fundamental rights.

02 Transparency

Disclose AI use, label synthetic content, and explain purpose and limitations.

03 Human oversight

Critical decisions always keep meaningful human review.

04 Data responsibility

Use lawful, accurate, proportionate, and protected data; reduce bias.

05 Security and safety

Address vulnerabilities, harmful output, and incidents promptly.

06 IP and attribution

Respect licenses, third-party rights, and disclosure obligations.

07 Continuous improvement

Review, learn, and adapt with law, standards, and project feedback.

Bottom line: AI can be innovative, but it must remain explainable, reviewable, and safe to use.

Everyday use: prompt responsibly

Most AI risk starts with ordinary behavior

The safest habits are simple, repeatable, and easy to teach.

Do this

- Use the minimum data necessary
- Verify outputs before sharing or using them
- Keep prompts respectful, fair, and non-misleading
- Treat outputs as possibly wrong and possibly sensitive

Avoid this

- Do not enter personal, confidential, or proprietary content unless explicitly authorised
- Do not upload whole datasets or unnecessary identifiers
- Do not share externally until reviewed and cleared



External tools are convenient — but they are not a free pass on privacy, confidentiality, or quality.

Before higher-impact AI goes live

Run the right risk check at the right moment.



1

Always do a documented risk check

Before use that involves personal data or could affect individuals.

2

Trigger a DPIA or equivalent when needed

Especially for profiling with effects, large-scale sensitive data, monitoring, or other high-impact contexts.

3

Document five things

Data and sources, purpose and necessity, risks, transparency, oversight, and mitigations.

4

Escalate uncertainty early

If in doubt, involve the GDPR Coordinator before proceeding.

Good AI governance is not a one-time approval

It becomes real through records, training, reviews, and careful tool onboarding.

Third-party AI tools need minimum checks before adoption: confirm contractual terms, perform security due diligence, satisfy data protection requirements where relevant, and record the tool in the AI Use Register.

Logs should also be maintained — enough for security investigation, auditability, and data protection duties, while still respecting minimisation and retention.

1

Register

Keep an AI Use Register entry with purpose, owner, tool, data categories, sources, risk level, and mitigations.

2

Train

Each participant is encouraged to build and run AI training in their work package.

3

Review

Update the guidelines at least annually, or sooner if law or technology changes materially.

Takeaway

A simple standard for the project

Helpful AI. Clear ownership. Human accountability.

The cheat sheet in one line:

Inform Tell users and stakeholders when AI is involved.

Assign Name an oversight owner for every AI use case.

Check Run risk checks and DPIAs when triggers apply.

Record Maintain the AI Use Register and relevant logs.

Review Verify outputs, train people, and improve continuously.

If it could materially affect people, data, or trust — slow down, document it, and keep a human in control.

