ANASTASIIA ANDRIIEVSKA
RISE RESEARCH INSTITUTES OF SWEDEN

Pitch

SecureAI

HORIZON-CL3-2026-02-CS-ECCC-02

Contacts: anastasiia.andriievska@ri.se | michael.popoff@ri.se | rickard.brannvall@ri.se

SecureAI – idea & RISE role

Topic focus: security, privacy and robustness of AI models and systems

Project idea: integrated SecureAI assurance framework (test + verify + comply)

Objectives: robustness & attack detection, privacy-enhancing AI (PETs), compliance evidence (AI Act/GDPR)

Deliverables: technical components + test/verification framework + practical compliance tool

Validation: 2–3 use cases in sensitive / regulated environments

RISE role: coordinator candidate (or partner) with Swedish pilots and strong EU networks

Track record: AI Factory Mimer, TEF Health AI/CitCom, EUHARPOCRATES, LeakPro (and more)

Desired partners

We are looking for:

- Applied/academic excellence: adversarial ML, robust training, PETs/crypto, verification & evaluation
- Industry/SMEs: tooling, integration, secure deployment, monitoring/mitigation
- End-users: government/public sector and enterprises for pilots & requirements
- Legal/standardisation: AI Act/GDPR, standards, exploitation

Current list of partner organisations (may change):

2 SMEs in privacy enhancing technologies, a cybersecurity company, 2 applied research and 2 academic partners + pilot/infrastructure links: MIMER AI Factory, TEF CitCom

Call(s) of interest: HORIZON-CL3-2026-02-CS-ECCC-02 (SecureAI)