Digital Europe: partners sought for AI-powered cybersecurity toolkit for small and medium enterprises

Summary

Profile type	Company's country	POD reference
Research & Development Request	**Lithuania**	**RDRLT20261103008**
Profile status	**Type of partnership**	**Targeted countries**
PUBLISHED	**Research and development cooperation agreement**	**• All countries**
Contact Person	**Term of validity**	**Last update**
Enrico FRANZIN	**4 Nov 2026** **4 Nov 2027**	**4 Nov 2026**

General Information

Short summary

A Lithuanian university with expertise in cybersecurity, digital forensics and artificial intelligence (AI) is building a consortium for the Digital Europe Programme call on cybersecurity capacities of small and medium-sized enterprises (SMEs). The project will integrate mature AI tools into one software-as-a-service toolkit for risk assessment, early warning and incident response, and validate it with SMEs in several countries.

Full description

Small and medium-sized enterprises are frequent targets of cyberattacks, but most have little or no dedicated security staff and limited ability to adopt AI-based protection. The project aims to close this gap with a modular toolkit that guides an SME from an authorised baseline of its assets and risks to prioritised actions, guided incident handling and a final reassessment of its cyber preparedness.

Programme conditions: the call is “Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions” (DIGITAL-ECCC-2027-DEPLOY-CYBER-11-AI4SME), an SME Support Action under the Digital Europe Programme. The expected EU contribution is EUR 3-5 million per project. Funding covers 75% of eligible costs for qualifying SME beneficiaries and 50% for other beneficiaries. Project duration is 36 months. Security restrictions under Article 12(5) of the programme regulation apply. Participants, associated partners and subcontractors must be established in, and not controlled from outside, eligible EU or EEA countries.

Timescales: expressions of interest by [EOI deadline to be confirmed]; call deadline 14 January 2027, 17:00 CET.

Partners roles will be defined in later stage.

Advantages and innovations

Main innovative elements:

-A single guided pathway from an authorised asset and risk baseline, through prioritised actions and incident handling, to a final reassessment of preparedness;
-AI-assisted incident reporting that leads non-expert staff step by step through incident descriptions, response instructions and notification drafts;
-A function that helps SMEs assess their own AI tools for data leakage, prompt injection and misconfiguration, a risk that most existing SME security offers do not cover;

Technical specification or expertise sought

The coordinator is looking for partners from the EU and eligible European Economic Area (EEA) countries who can contribute one or more of the following types of expertise, technology or access.

1. Cybersecurity and AI technology companies (SMEs)

2. Pilot SMEs

3. Organisations with direct access to SMEs

4. National incident reporting and support bodies

5. Training providers
Eligibility conditions for all partners

Establishment in an eligible EU or EEA country, and direct and indirect control only from eligible countries. These checks also cover associated partners and subcontractors.
Compliance with the security restrictions under Article 12(5) of the Digital Europe Programme regulation.
A valid participant identification code (PIC).

Stage of development

Concept stage

Sustainable Development goals

- **Goal 8: Decent Work and Economic Growth**

IPR Status

No IPR applied

IPR Notes

Partner Sought

Expected role of the partner

Selected partners will join the consortium as funded beneficiaries or as pilot participants, depending on their type.

Type of partnership

Research and development cooperation agreement

Type and size of the partner

- **SME <=10**
- **SME 11-49**
- **SME 50 - 249**
- **University**
- **Big company**
- **R&D Institution**
- **Other**

Call Details

Framework program

Digital Europe

Call title and identifier

Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions (DIGITAL-ECCC-2027-DEPLOY-CYBER-11-AI4SME), SME Support Action

Submission and evaluation scheme

Single-stage submission and evaluation procedure via EU F&T. Proposals submitted as a complete single-stage application (Part A administrative forms, Part B technical proposal narrative, and Part C key performance indicators).

Anticipated project budget

Coordinator required

Yes

Deadline for EoI

Deadline of the call

30 Nov 2026

Project duration in weeks

27 Jan 2027

Web link to the call

Project title and acronym

Dissemination

Technology keywords

- **01006005 - Network Technology, Network Security**
- **01004016 - Analysis Risk Management**
- **01003003 - Artificial Intelligence (AI)**

Market keywords

- **02006009 - Other computer services**
- **02006003 - Computer training services**

Targeted countries

- **All countries**

Sector groups involved

- **Digital**