

Dutch cybersecurity software company seeks coordinator and partners for a Digital Europe project (under CYBER-11-EULEG) on automated compliance audits (CRA, NIS2, GDPR)

Summary

Profile type

Research & Development Request Netherlands

Company's country

POD reference

RDRNL20260928033

Profile status

PUBLISHED

Type of partnership

**Research and development
cooperation agreement**

Targeted countries

• All countries

Contact Person

[Enrico FRANZIN](#)

Term of validity

28 Sep 2026**28 Sep 2027**

Last update

28 Sep 2026

General Information

Short summary

A Dutch SME offering and expanding continuous IT security and compliance platform is building a consortium for the Digital Europe call CYBER-11-EULEG (deadline 14 January 2027) to fully automate audits against EU legislation such as the Cyber Resilience Act, NIS2 and GDPR. A coordinator is sought, as well as partners with regulatory and audit expertise, AI Act validation competence, and end users acting as launching customers and beta testers.

Full description

The client is a Dutch, privately owned software company with more than ten years of experience in cybersecurity. Its multi-tenant platform continuously detects IT risks, manages vulnerabilities, monitors web applications and cloud environments, and maps findings to more than 25 compliance frameworks, including ISO 27001, GDPR, NIS2 and DORA. The platform is delivered through more than 100 managed service providers (MSPs) and is used by over 1,000 organisations in healthcare, government, finance and other sectors. The company has been ISO 27001 certified for eight years and holds the ECSO (European Cyber Security Organisation) label.

New EU legislation, in particular the Cyber Resilience Act (CRA) and the NIS2 Directive, places significant compliance obligations on organisations and manufacturers, many of them SMEs. Compliance audits today are largely manual, costly and point-in-time. This creates a shortage of audit capacity and leaves organisations uncertain about their compliance status between audits.

The client has already developed a substantial set of building blocks for automated audits against GDPR, CRA, NIS2 and other standards. The proposed project will extend these into a fully automated audit solution covering audit planning, evidence collection from technical sources, assessment against legal and normative requirements, and audit reporting. AI components will support interpretation and reporting; the solution itself must therefore comply with the EU AI Act.

The client is now initiating an international consortium for the Digital Europe Programme call DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG and has already found an interested German partner.

As an SME focused on technology development, the client does not wish to take on the coordinator role and is therefore looking for an experienced organisation to coordinate the proposal and project. Under a research and development cooperation agreement, the consortium will develop, validate and pilot the solution in several EU countries, turning it into an interoperable European tool for regulatory compliance.

Advantages and innovations

- Continuous compliance instead of point-in-time audits. The solution checks compliance continuously against legal requirements, while traditional audits are manual, periodic and costly. Organisations can see their compliance status at any moment and need less scarce auditor capacity.
- Direct link between technical evidence and legal requirements. Findings from vulnerability scans, configuration checks and monitoring are mapped automatically to specific articles and controls of the CRA, NIS2, GDPR and DORA. Existing tools mostly handle either technical security or documentation-based compliance, not both.
- Built on a proven platform. The project starts from a platform that is already on the market, maps findings to more than 25 frameworks and is used by over 1,000 organisations. This lowers the technical risk of the project and speeds up piloting.
- Direct route to wide uptake. Through a network of more than 100 managed service providers, the results can reach many SMEs across Europe without extra effort. SMEs are the group that struggles most with the new obligations.

Technical specification or expertise sought

- Project coordination: an organisation with proven experience in preparing and coordinating EU-funded projects (preferably Digital Europe or Horizon Europe) in the field of cybersecurity, able to lead proposal writing, consortium management and reporting to the European Cybersecurity Competence Centre (ECCC).
- Regulatory and audit expertise: in-depth knowledge of the CRA, NIS2, GDPR, DORA and related standards (e.g. ISO 27001, IEC 62443), combined with practical experience in audit plans, audit scheduling and audit reporting. Typical profiles: audit firms, certification or conformity assessment bodies, and legal or compliance consultancies.
- AI Act compliance validation: capacity to assess and validate that the AI components meet AI Act requirements (risk classification, transparency, human oversight, technical documentation). Typical profiles: research organisations, universities, or specialised AI governance and testing labs.
- Launching customers and pilot sites: organisations subject to NIS2 or the CRA, such as manufacturers of connected products, essential or important entities, or MSPs, willing to beta test the solution in real environments and provide structured feedback.

Stage of development

Under development

Sustainable Development goals

- **Goal 16: Peace and Justice Strong Institutions**
- **Goal 9: Industry, Innovation and Infrastructure**
- **Goal 8: Decent Work and Economic Growth**

IPR Status

No IPR applied

IPR Notes

Partner Sought

Expected role of the partner

Partners sought:

- Type of partner: R&D institutions, universities, industry, SMEs, certification or conformity assessment bodies; also sector associations, cluster organisations or national cybersecurity bodies.
- Role of partner: one partner will act as project coordinator. Other partners contribute regulatory content and audit methodology, validate AI Act compliance, or provide pilot environments and end-user feedback.
- Requirements: established in an EU Member State or a country eligible under the Digital Europe Programme, and able to meet the security requirements of Article 12(5) of the Digital Europe Regulation.

Type of partnership

Research and development cooperation agreement

Type and size of the partner

- **SME 50 - 249**
- **University**
- **Big company**
- **R&D Institution**
- **SME 11-49**

Call Details

Framework program

Digital Europe

Call title and identifier

DIGITAL-ECCC-2027-DEPLOY-CYBER-11-EULEG – Strengthening EU cybersecurity capacities and capabilities in line with legislative requirements

Submission and evaluation scheme

Deadline of call submission is January 14th, 2027

Anticipated project budget

3-5 Million Euro

Coordinator required

Yes

Deadline for EoI

Deadline of the call

15 Nov 2026

14 Jan 2027

Project duration in weeks

156

Web link to the call

Project title and acronym

Dissemination

Technology keywords

- 01003009 - Data Protection, Storage, Cryptography, Security
- 01006005 - Network Technology, Network Security
- 01003003 - Artificial Intelligence (AI)
- 01003020 - Building Automation Software

Targeted countries

- All countries

Market keywords

- 02007025 - Consulting services
- 02006009 - Other computer services
- 02007016 - Artificial intelligence related software

Sector groups involved

- Digital