

# Connected toys or consumer IoT use-case partner sought for mobile application software supply-chain cybersecurity pilot as part of a Horizon Europe project (HORIZON-CL3-2026-02-CS-ECCC-01- Cybersecurity of software supply chains of mobile applications)

## Summary

Profile type

**Research & Development Request Bulgaria**

Company's country

POD reference

**RDRBG20260723010**

Profile status

**PUBLISHED**

Type of partnership

**Research and development cooperation agreement**

Targeted countries

- **Belgium**
- **Hungary**
- **Bulgaria**
- **Estonia**
- **Ireland**
- **Greece**
- **Austria**
- **Czechia**
- **Denmark**
- **France**
- **Germany**
- **Finland**
- **Croatia**
- **Cyprus**
- **New Zealand**
- **Albania**
- **Egypt**
- **Spain**
- **Sweden**
- **Canada**
- **Israel**

- Ukraine
- North Macedonia
- Lithuania
- Poland
- Tunisia
- Italy
- South Korea
- Slovenia
- Moldova
- Norway
- Luxembourg
- Kosovo
- Faroe Islands
- Latvia
- Malta
- Bosnia and Herzegovina
- Georgia
- Iceland
- Türkiye
- Netherlands
- United Kingdom
- Armenia
- Switzerland
- Slovakia
- Serbia
- Montenegro

Contact Person

[\*\*Enrico FRANZIN\*\*](#)

Term of validity

**23 Jul 2026****23 Jul 2027**

Last update

**23 Jul 2026**

## General Information

Short summary

A Bulgarian organization (foundation) is a project partner in a Horizon Europe proposal and will lead the work

package on validation and pilot testing. The consortium is seeking a formal use-case partner for a pilot sector to provide a real connected-device and consumer mobile application context, co-define the use case, support evaluation of the project results and participate in selected validation activities, without a requirement for software development.

#### Full description

The project is being prepared as a Horizon Europe proposal in the civil security and cybersecurity area, under the call HORIZON-CL3-2026-02-CS-ECCC-01 – Cybersecurity of software supply chains of mobile applications. It addresses the growing cybersecurity risks linked to mobile application software supply chains, where apps often depend on third-party libraries, SDKs, APIs, cloud services, updates and external software components. These dependencies may create vulnerabilities affecting security, privacy, trust, resilience and user safety, especially when mobile applications are connected to consumer devices and IoT ecosystems.

The project will research, develop and validate approaches for improving the security and resilience of software supply chains for mobile applications. The work is expected to focus on methods, tools, processes and validation practices that help identify, assess and mitigate cybersecurity risks across the mobile app lifecycle. The aim is to ensure that the project outputs are technically robust and practically applicable in real operational and market contexts.

The consortium already includes technical and use-case partners, including use cases from Bulgaria and Spain. To broaden EU coverage and demonstrate applicability in another country and sector, one additional use-case partner is sought for a third pilot sector, preferably outside Bulgaria and Spain.

The partner must be established in an EU Member State or Horizon Europe Associated Country and must not be controlled by an ineligible third country, in line with the security requirements of the call. These conditions are important due to the civil security and cybersecurity nature of the topic.

The call submission deadline is 15 September 2026. Due to the short preparation timeframe, an expression of interest is needed as soon as possible, and by 8 August 2026 at the latest, together with confirmation of eligibility and PIC registration or an existing PIC number. The indicative budget for this partner is approximately EUR 50,000–80,000, depending on the final scope of activities and effort allocation. The expected project duration will follow the final Horizon Europe proposal and consortium planning, with the partner mainly involved in use-case definition, validation and pilot-related activities.

### Advantages and innovations

### Technical specification or expertise sought

No software development is expected from the use-case partner. Its main contribution will be sector knowledge, access to a realistic connected-device/mobile app context and validation feedback, helping the consortium test whether the developed approaches can be applied in a real consumer IoT environment.

### Stage of development

### Sustainable Development goals

- **Goal 9: Industry, Innovation and Infrastructure**

### IPR Status

### IPR Notes

## Partner Sought

### Expected role of the partner

The requested partner should be a producer of connected toys or a company offering connected consumer devices / IoT products supported by a consumer mobile application. A child-safety angle is a strong advantage, particularly where the device, mobile app and software components raise issues related to cybersecurity, privacy, trust, data protection, software updates, user safety or responsible digital interaction.

The expected partner will have a small, formal and clearly defined role. The organisation will co-define the use case, provide real-life context related to its product and/or application, support assessment of project results and participate in selected validation and pilot activities. The expected involvement includes one or two working meetings and feedback on the relevance, usability and applicability of the project outcomes from an operational and market perspective.

### Type of partnership

### Type and size of the partner

**Research and development cooperation agreement**

- **Big company**
- **SME 11-49**
- **SME 50 - 249**

## Call Details

---

Framework program

**Horizon Europe**

Call title and identifier

**HORIZON-CL3-2026-02-CS-ECCC-01- Cybersecurity of software supply chains of mobile applications**

Submission and evaluation scheme

Anticipated project budget

Coordinator required

**No**

Deadline for EoI

**8 Aug 2026**

Deadline of the call

**15 Sep 2026**

Project duration in weeks

Web link to the call

Project title and acronym

## Dissemination

---

Technology keywords

- **01003025 - Internet of Things**
- **01003009 - Data Protection, Storage, Cryptography, Security**

Market keywords

- **02007007 - Applications software**
- **07004008 - Other consumer products**





Targeted countries

- Belgium
- Hungary
- Bulgaria
- Estonia
- Ireland
- Greece
- Austria
- Czechia
- Denmark
- France
- Germany
- Finland
- Croatia
- Cyprus
- New Zealand
- Albania
- Egypt
- Spain
- Sweden
- Canada
- Israel
- Ukraine
- North Macedonia
- Lithuania
- Poland
- Tunisia
- Italy
- South Korea
- Slovenia
- Moldova
- Norway
- Luxembourg

Sector groups involved

- Digital



- Kosovo
- Faroe Islands
- Latvia
- Malta
- Bosnia and Herzegovina
- Georgia
- Iceland
- Türkiye
- Netherlands
- United Kingdom
- Armenia
- Switzerland
- Slovakia
- Serbia
- Montenegro