



Digital Europe Programme (DIGITAL)

Call for proposals

CyberHUBs Capacity Building
(DIGITAL-ECCC-2026-DEPLOY-CYBER-10)

Version 1.0
9 December 2025

HISTORY OF CHANGES			
Version	Publication Date	Change	Page
1.0	09.12.2025	▪ Initial version.	
		▪	



CALL FOR PROPOSALS

TABLE OF CONTENTS

DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs	7
Objectives	8
Scope	8
Expected Outcomes	10
KPIs to measure outcomes and deliverables	10
Targeted stakeholders	11
Type of action and funding rate	11
Specific topic conditions	11
DIGITAL-ECCC-2026-DEPLOY-CYBER-10- CBCH — Cross-Border Cyber Hubs	11
Objectives	11
Scope	12
Expected Outcomes	14
KPIs to measure outcomes and deliverables	14
Targeted stakeholders	14
Type of action and funding rate	14
Specific topic conditions	15
Eligible participants (eligible countries)	17
Specific cases and definitions	18
Consortium composition	19
Eligible activities	20
Geographic location (target countries)	20
Due to restrictions due to security:	20
– for all topics: the proposals must relate to activities taking place in the eligible countries (see above)	20
Ethics	20
Security	20
Financial capacity	22
Operational capacity	22
Exclusion	23
Starting date and project duration	26
Milestones and deliverables	27
Form of grant, funding rate and maximum grant amount	27
Budget categories and cost eligibility rules	28
Reporting and payment arrangements	29
Prefinancing guarantees	30
Certificates	30

Liability regime for recoveries30

Provisions concerning the project implementation30

Other specificities32

Non-compliance and breach of contract32


0. Introduction

This is a call for proposals for EU **action grants** in the field of Cybersecurity under the **Digital Europe Programme (DIGITAL)**.

The regulatory framework for this EU Funding Programme is set out in:

- Regulation 2024/2509 ([EU Financial Regulation](#))¹
- the basic act (Digital Europe Regulation [2021/694](#))².

The call is launched in accordance with the 2025-2027 Work Programme³ and will be managed by the European Cybersecurity Competence Centre (ECCC).

 Please note that this call is subject to possible amendments of the 2025 - 2027 Work Programme. In case there are substantial changes, the call may be modified. All updates will be reflected in the call document.

The call covers the following **topics**:

- **DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs**
- **DIGITAL-ECCC-2026-DEPLOY-CYBER-10- CBCH — Cross-Border Cyber Hubs**

Each project application under the call must address only one of these topics. Applicants wishing to apply for more than one topic, must submit a separate proposal under each topic.

We invite you to read the **call documentation** carefully, and in particular this Call document, the Model Grant Agreement, the [EU Funding & Tenders Portal Online Manual](#) and the [EU Grants AGA — Annotated Grant Agreement](#).

These documents provide clarifications and answers to questions you may have when preparing your application:

- the [Call document](#) outlines the:
 - background, objectives, scope, outcomes and deliverables, KPIs to measure outcomes and deliverables, targeted stakeholders, type of action and funding rate and specific topic conditions (sections 1 and 2)
 - timetable and available budget (sections 3 and 4)
 - admissibility and eligibility conditions (including mandatory documents; sections 5 and 6)
 - criteria for financial and operational capacity and exclusion (section 7)
 - evaluation and award procedure (section 8)

¹ Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast) ('EU Financial Regulation') (OJ L, 2024/2509, 26.9.2024).

² Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme (OJ L 166, 11.5.2021, p. 1).

³ Adopted by the GB of ECCC in Decision No 2025/04 concerning the adoption of the [work programme for 2025-2027](#) and the financing decision for the implementation of the Digital Europe Programme.

- award criteria (section 9)
- legal and financial set-up of the Grant Agreements (section 10)
- how to submit an application (section 11).
- the Online Manual outlines the:
 - procedures to register and submit proposals online via the EU Funding & Tenders Portal ('Portal')
 - recommendations for the preparation of the application.
- the AGA — Annotated Grant Agreement contains:
 - detailed annotations on all the provisions in the Grant Agreement you will have to sign in order to obtain the grant (*including cost eligibility, payment schedule, accessory obligations, etc*).

You are also encouraged to visit the [EU Funding & Tenders Portal](#) to consult the list of projects funded previously.

1. Background

Digital transformation continues to accelerate across Europe, fundamentally reshaping economies, societies, and governance. From AI-driven automation to the rise of quantum technologies, digital systems are now deeply integrated into critical infrastructures, public services, and industrial value chains. This growing interdependence, while creating new opportunities, also exposes Europe to a rapidly evolving spectrum of cyber threats — increasingly sophisticated, transnational, and strategically motivated.

Recent geopolitical developments and the proliferation of large-scale cyber incidents have underscored the strategic importance of robust, coordinated, and sovereign cybersecurity capabilities. Cyberattacks targeting energy systems, communication networks, and democratic institutions demonstrate that resilience in cyberspace is not merely a technical concern, but a cornerstone of Europe's security, sovereignty, and trust.

To address these challenges, the **European Union** has launched a comprehensive approach under the **Cyber Solidarity Act** and the **EU Cybersecurity Strategy**, reinforcing the EU's ability to detect, prevent, and respond to cyber incidents. Within this framework, the **European Cybersecurity Competence Centre (ECCC)**, through the **Digital Europe Programme (DEP) 2025–2027 Work Programme**, is deploying key initiatives that strengthen operational capacities and promote a coordinated European cybersecurity ecosystem.

Building on the successful deployment of national and cross-border Security Operations Centres (SOCs) under previous Digital Europe work programmes, the **2026 Call 10** continues this strategic investment by supporting the establishment and consolidation of **National Cyber Hubs** and **Cross-Border Cyber Hubs**. These actions will constitute essential components of the **European Cybersecurity Alert System**, providing the backbone for joint detection, situational awareness, and coordinated response across the Union.

National Cyber Hubs will act as the primary national entities responsible for collecting, analysing, and correlating cybersecurity data, serving as reference points and gateways to national CSIRTs, ISACs, and other competent authorities. Cross-Border Cyber Hubs

will interconnect these national nodes, enabling a pan-European exchange of cyber threat intelligence (CTI), supporting real-time situational awareness, and fostering joint analysis and mitigation of threats that transcend national borders.

Together, these interconnected hubs will:

- Enhance the EU's capacity to **detect cyber threats early** and **respond swiftly** to major incidents.
- **Facilitate information sharing** and **interoperability** across Member States and sectors.
- **Integrate advanced AI and data analytics** for real-time monitoring, threat correlation, and early warning systems.
- **Support preparedness and resilience** of critical infrastructures, including emerging domains such as **submarine cable security**.
- Strengthen **collective cyber defence and solidarity**, contributing to Europe's digital sovereignty.

These actions are implemented under the **Cyber Solidarity Act** and subject to the **security restrictions of Article 12(5)** of the Digital Europe Programme Regulation, ensuring that participating entities are EU-controlled and aligned with the Union's security interests.

By consolidating and connecting Europe's Cyber Hubs, the EU is advancing towards a **resilient, trusted, and sovereign digital future**—one in which early detection, rapid response, and cross-border cooperation are at the core of a secure Digital Single Market.

2. Objectives — Scope — Expected Outcomes — KPIs to measure outcomes and deliverables — Targeted stakeholders — Type of action and funding rate — Specific topic conditions

DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs

Where a Member State decides to participate in the European Cybersecurity Alert System, it shall designate or, where applicable, establish a National Cyber Hub, a single entity acting under the authority of the Member State.

National Cyber Hubs have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cyber threats and incidents and to contribute to a Cross-Border Cyber Hub. They are capable of detecting, aggregating, and analysing data and information relevant to cyber threats and incidents, such as cyber threat intelligence, by using in particular state-of-the-art technologies, and with the aim of preventing incidents.

As already mentioned, for the following programming cycle, the emphasis is on continuation of activities initiated during past years.

Objectives

The objective is to create or strengthen National Cyber Hubs, with state-of-the-art tools for monitoring, understanding and proactively managing cyber events, in close collaboration with relevant entities such as CSIRTs, ISACs, etc. They will also, where possible, benefit from information and feeds from other Cyber Hubs in their countries and use the aggregated data and analysis to deliver early warnings to targeted critical infrastructures on a need-to-know basis. National Cyber Hubs could also consider the possibility of monitoring undersea infrastructure, such as submarine cables.

Scope

The aim is to build capacity for new or existing National Cyber Hubs, e.g. equipment, tools, data feeds, as well as costs related to data analysis, interconnection with Cross-Border Cyber Hubs, etc. This can include for example automation, analysis and correlation tools and data feeds covering Cyber Threat Intelligence (CTI) at various levels, ranging from field data to Security Information and Event Management (SIEM) data to higher level CTI. Automation is a key aspect in the efficient handling and processing of information. Where available, already established standards should be used, such as the Common Security Advisory Framework (CSAF)⁴, for security advisories or for collecting and processing cybersecurity-related messages (e.g. IntelMQ project⁵). Applications developed by Cyber Hubs/SOCs should be compatible with European standardisation projects like the EU vulnerability database (EUVD). National Cyber Hubs should also leverage state-of-the-art technology such as artificial intelligence and dynamic learning of the threat landscape and context. This also includes the use of shared cybersecurity information, to the extent possible based on existing taxonomies and/or ontologies, and hardware to ensure the secure exchange and storage of information. The operations should be built upon live network data and other training data required in the initial phases. Where relevant, consideration should be given to SMEs as the ultimate recipients of cybersecurity operational information.

A key element is the translation of advanced AI, data analytics and other relevant cybersecurity tools from research results to operational tools, and further testing and validating them in real conditions in combination with access to supercomputing facilities (e.g. to boost the correlation and detection features of cross-border platforms). Such activities are identified and proposed for financing in section 2.3, dedicated to AI for Cybersecurity, and topic 2.3.1.

Furthermore, National Cyber Hubs could also consider deploying solutions for the surveillance and protection of critical undersea infrastructure, such as submarine cables, and the detection of malicious activities around them, to improve the resilience and security of this infrastructure, which is critical for global communications. The response to such hybrid threats could also include situational awareness performed through the collection and analysis of in-situ, sea based sensor data as well as relevant

⁴ Common Security Advisory Framework (CSAF): Machine-processable format enables automated database reconciliation - https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html

⁵ IntelMQ: <https://github.com/certtools/intelmq>

satellite imagery. For such activities, operational synergies with the EU Copernicus Space Programme and in particular with its Security Service are required.

Another key role for National Cyber Hubs is to facilitate knowledge transfer and sharing, as well as support training initiatives for all needed cybersecurity roles the basis, for instance, of the European Cybersecurity Skills Framework (ECSF⁶). For example, Cyber Hubs/SOCs dealing with critical infrastructures play a key role and should benefit from the knowledge and experience acquired by or concentrated in National Cyber Hubs.

National Cyber Hubs must share information with other stakeholders in a mutually beneficial exchange of information and commit to apply to participate in a Cross-Border Cyber Hub within the next 2 years, with a view to exchanging information with other National Cyber Hubs.

To achieve this aim, a call for expression of interest⁷ will be launched to select entities in Member States that provide the necessary facilities to host and operate National Cyber Hubs. Applicants to the call for expressions of interest should describe the aims and objectives of the National Cyber Hub, describe its role and how such role relates to other cybersecurity actors, such as CSIRTs, and its potential cooperation with other public or private cybersecurity stakeholders. Applicants should also provide the detailed planning of the activities and tasks of the National Cyber Hub, the services it will offer, the way it will operate and be operationalised, and describe the duration of the activity as well as the main milestones and deliverables. They should also specify what equipment, tools and services need to be procured and integrated to build up the National Cyber Hub, its services and its infrastructure.

To support the above activities of a National Cyber Hub, the following two workstreams of activities are foreseen:

- **[Procurement]8 A Joint Procurement Action** with the Member State where the National Cyber Hub is located: this will cover the procurement of the main infrastructure, tools and services needed to build up the National Cyber Hub.
- **[Building up and running the National Cyber Hub]** A grant will also be available to cover, among others, the preparatory activities for setting up the National Cyber Hub, its interaction and cooperation with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the National Cyber Hub, e.g. using the infrastructure, tools and services purchased through the joint procurement. These will also indicate milestones and deliverables to monitor progress.

⁶ <https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework>.

⁷ Please note this is not a call for expression of interest within the meaning of Point 13 of Annex I of the Regulation (EU, Euratom) 2018/1046. The aim is to select the future contracting authorities taking part in a joint procurement.

⁸ For the topic DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs an expression of interest shall also be submitted no later than the 28 May 2026 at 17:00 Brussels time. Application forms will be available at https://cybersecurity-centre.europa.eu/funding-opportunities_en. Applications must be submitted in the correct form, duly completed and dated. They must be submitted in electronic copy on [Call for Expressions of Interest - European Cybersecurity Competence Centre and Network](#) and signed by the person authorised to enter into legally binding commitments on behalf of the applicant organisation. The electronic version must contain the pdf versions of the application and other files as described in the call for expression of interest.

Applications shall be made to both workstreams. The applications will be subject to an evaluation procedure. Grants will only be awarded to applicants that have succeeded in the evaluation of the joint procurement action.

These actions aim at creating or strengthening National Cyber Hubs, which occupy a central role in ensuring the cybersecurity of national authorities, providers of critical infrastructures and essential services. Cyber Hubs, in cooperation with other relevant national/regional entities, are tasked with monitoring, understanding and proactively managing cybersecurity threats. Cyber Hubs will have a crucial operative role in ensuring cybersecurity in the Union and will handle sensitive information.

Pursuant to Article 12(5a) of the Cyber Solidarity Act amending Article 12 of Regulation (EU) 2021/694, Article 12(5) of Regulation (EU) 2021/694 shall not apply if the conditions stipulated in Article 12(5a) are cumulatively met. The assessment of these conditions should take into account the results of the mapping of the availability of tools, infrastructure and services for the National Cyber Hubs to be carried out by the ECCC pursuant to Article 9(4) of the Cyber Solidarity Act.

The first mapping exercise is ongoing. Until the mapping is completed and in line with the relevant provisions of the Cyber Solidarity Act, participation to the calls funded under this topic will be therefore subject to the restrictions of Article 12(5), as specified in Appendix 3 of this Work Programme. These security conditions may be later amended taking into account the results of the final mapping of services carried out by the ECCC pursuant to Article 9(4) of the Cyber Solidarity Act.

Expected Outcomes

World-class National Cyber Hubs across the Union, supported by state-of-the-art technology, acting as clearing houses for detecting, gathering and storing data on cybersecurity threats, analysing this data, and sharing and reporting CTI, reviews and analyses, taking into account well-established standards for sharing and automation processes.

Threat intelligence and situational awareness capabilities and capacity building supporting strengthened collaboration between cybersecurity actors, including private and public actors.

- Targeted training courses on the basis of the ECSF to improve the capacity of cyber security roles.
- Applications for automated notification of private and public actors about compromised or insecure systems.

KPIs to measure outcomes and deliverables

Applicants should provide KPI's and metrics relevant for the action to measure progress and performance. Proposals may include the indicators listed below or those of their choice.

When applicable, baseline and target values must be provided.

- *Maturity analysis pre and post implementation to measure the change in capacity of the beneficiary(ies).*
- *Number of entities benefitting from the CyberHUB operations.*
- *Intensity of exchange of information between funded entities.*

- *Cyberthreat intelligence and situational awareness services developed.*

Targeted stakeholders

The targeted stakeholders under a) and b) above are *public bodies acting as National Cyber Hubs, as identified by Member States* linked to a “call for expression of interest to deploy and operate National CyberHUB platforms to improve the detection of cybersecurity threats and share cybersecurity data in the EU”. Actions under Proposals for grants shall complement submission for the successful applicants to this call for expression of interest.

Type of action and funding rate

Simple Grants — 50% funding rate

-  For more information on Digital Europe types of action, see *Annex 1*.

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply (*see sections 6 and 10 and Annex 2*)
- For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment (*see section 10*)
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
 - extent to which the project would reinforce and secure the digital technology supply chain in the Union*
 - extent to which the proposal can overcome financial obstacles such as the lack of market finance*
 - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*

DIGITAL-ECCC-2026-DEPLOY-CYBER-10- CBCH — Cross-Border Cyber Hubs

The former Cross-border SOC platforms were financed during previous calls and such collaboration is envisaged for the Cross-Border Cyber Hubs. They should provide new additional capacity building upon and complementing existing SOC/Cyber Hubs, Computer Security Incident Response Teams (CSIRTs), ISACs and other relevant actors.

Objectives

This action is aimed mainly at new Cross-Border Cyber Hubs. Supporting activities for the SOC/Cyber Hubs that were already launched under the previous DIGITAL work programmes

(2021-2022 and 2023-2024)⁹ could also be included when relevant to ensure collaboration with the Cross-Border Cyber Hubs.

In addition to setting up processes, tools and services for prevention, detection and analysis of emerging cyberattacks, the scope also covers the acquisition and/or adoption of common (automation) tools, processes and shared data infrastructures for the management and sharing of contextualised and actionable cybersecurity operational information across the EU. Well-established open standards for CTI sharing (e.g. MISP Standard¹⁰) or automation of advisory information (e.g. CSAF¹¹) and cybersecurity related messages (e.g. by IntelMQ) should be considered. Cross-Border Cyber Hubs could also foresee the possibility to monitor undersea infrastructure, such as submarine cables.

Scope

The Cross-Border Cyber Hubs platforms will contribute to enhancing and consolidating collective situational awareness and capabilities in detection and CTI, supporting the development of better performing data analytics, detection, and response tools, through the pooling of large amounts of data, including new data generated internally by the consortia members.

The platforms should act as a central point allowing for broader pooling of relevant data and CTI, enabling the dissemination of threat information on a large scale and among a large and diverse set of actors (e.g. CERTs/CSIRTs, ISACs, operators of critical infrastructures).

According to the Cyber Solidarity Act, the Cross-Border Cyber Hubs and the CSIRTs Network shall cooperate closely, in particular for the purpose of sharing information. To that end, they shall agree procedural arrangements on cooperation and sharing of relevant information and on the types of information to be shared.

Furthermore, Cross-Border Cyber Hubs could also deploy solutions for the surveillance and protection of critical undersea infrastructure, such as submarine cables, and the detection of malicious activities around them, to improve the resilience and security of this infrastructure, which is critical for global communications. The response to such hybrid threats could also include situational awareness performed through the collection and analysis of in-situ, sea based sensor data as well as relevant satellite imagery. For this activity, operational synergies with the EU Copernicus Space Programme and in particular with its Security Service are required.

Where the Cross-Border Cyber Hubs obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall ensure, for the purpose of common situational awareness, that relevant information as well as early warnings are provided to the authorities in the Member States and to the Commission through the

⁹ ENSOC and ATHENA consortia are already financed.

¹⁰ MISP Standard: <https://www.misp-standard.org/>.

¹¹ Common Security Advisory Framework (CSAF): Machine-processable format enables automated database reconciliation - https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html.

EU-CyCLONe and the CSIRTs network¹², without undue delay. A call for expression of interest will be launched to select entities in Member States that provide the necessary facilities to host and operate Cross-Border Cyber Hubs for pooling data on cybersecurity threats between several Member States. Applicants to the call for expressions of interest should describe the aims and objectives of the Cross-Border Cyber Hub, describe its role and how such role relates to other cybersecurity actors, and its potential cooperation with other public or private cybersecurity stakeholders. Applicants should also provide the detailed planning of the activities and tasks of the Cross-Border Cyber Hub, the services it will offer, the way they will operate and be operationalised, as well as the main milestones and deliverables. They should also specify what equipment, tools and services need to be procured and integrated to build up the Cross-Border Cyber Hub, its services and its infrastructure.

To support the above activities of a Cross-Border Cyber Hub, the following two workstreams of activities are foreseen:

- **[Procurement]¹³ A Joint Procurement Action** with the Member State participating in the Cross-Border Cyber Hub: this will cover the procurement of the infrastructure, tools and services needed to build up the Cross-Border Cyber Hub.
- **[Building up and running the Cross-Border Cyber Hub]** A grant will also be available to cover, among others, the preparatory activities for setting up the Cross-Border Cyber Hub, its interaction and cooperation with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the Cross-Border Cyber Hub, e.g. using the infrastructure, tools and services purchased through the joint procurement, personnel. These will also indicate milestones and deliverables to monitor progress.

Applications shall be made to both workstreams. The applications will be subject to an evaluation procedure. Grants will only be awarded to applicants that have succeeded in the evaluation of the joint procurement action.

These actions aim at creating or strengthening Cross-Border Cyber Hubs, which occupy a central role in ensuring the cybersecurity of national authorities, providers of critical infrastructures and essential services. As previously noted, Cyber Hubs will have a crucial operative role in ensuring cybersecurity in the Union and will handle sensitive information.

Pursuant to Article 12(5a) of the Cyber Solidarity Act amending Article 12 of Regulation (EU) 2021/694, Article 12(5) of the Regulation (EU) 2021/694 shall not apply if the conditions stipulated in Article 12(5a) are cumulatively met. The assessment of these conditions should take into account the results of the mapping of the availability of tools, infrastructure and services for the Cross-Border Cyber Hubs to be carried out by the ECCC pursuant to Article 9(4) of the Cyber Solidarity Act.

¹² As defined by Directive (EU) 2022/2555.

¹³ For the topic DIGITAL-ECCC-2026-DEPLOY-CYBER-10- CBCH — Cross-Border Cyber Hubs an expression of interest shall also be submitted no later than the 28 May 2026 at 17:00 Brussels time. Application forms will be available at https://cybersecurity-centre.europa.eu/funding-opportunities_en. Applications must be submitted in the correct form, duly completed and dated. They must be submitted in electronic copy on [Call for Expressions of Interest - European Cybersecurity Competence Centre and Network](#) and signed by the person authorised to enter into legally binding commitments on behalf of the applicant organisation. The electronic version must contain the pdf versions of the application and other files as described in the call for expression of interest.

The first mapping exercise is ongoing. Until the mapping is completed and in line with the relevant provisions of the Cyber Solidarity Act, participation to the calls funded under this topic will be therefore subject to the restrictions of Article 12(5), as specified in Appendix 3 of this Work Programme. These security conditions may be later amended taking into account the results of the final mapping of services carried out by the ECCC pursuant to Article 9(4) of the Cyber Solidarity Act.

In case of enlargement of an ongoing cross-border grant, the applicant consortium should be composed by the coordinator of the ongoing grant plus the new entities that want to join the hosting consortium of the cross-border CyberHUB. The new grant will work in close cooperation with the ongoing one.

Expected Outcomes

- World-class Cross-Border Cyber Hubs across the Union for pooling data on cybersecurity threats between several Member States, equipped with a highly secure infrastructures and advanced data analytics tools for detecting, gathering and storing data on cybersecurity threats, analysing this data, and sharing and reporting CTI, reviews and analyses.
- Sharing of Threat Intelligence between National Cyber Hubs, and information sharing agreements with competent authorities and networks, including CSIRTs.

KPIs to measure outcomes and deliverables

Applicants should provide KPI's and metrics relevant for the action to measure progress and performance. Proposals may include the indicators listed below or those of their choice.

When applicable, baseline and target values must be provided.

- *Maturity analysis pre and post implementation to measure the change in capacity of the beneficiary(ies).*
- Number of entities benefitting from the SOC's operations.
- Intensity of exchange of information between funded entities.
- Cyberthreat intelligence and situational awareness services developed.

Targeted stakeholders

The target stakeholders under a) and b) above are *Public bodies acting as National Cyber Hubs, as identified by Member States*, linked to a "call for expression of interest to deploy and operate National SOC platforms to improve the detection of cybersecurity threats and share cybersecurity data in the EU". Actions under Proposals for grants shall complement submission for the successful applicants to this call for expression of interest.

Type of action and funding rate

Simple Grants — 50% funding rate



For more information on Digital Europe types of action, see *Annex 1*.

Specific topic conditions

- For this topic, security restrictions under Article 12(5) of the Digital Europe Regulation apply (see *sections 6 and 10 and Annex 2*)
- For this topic, following reimbursement option for equipment costs applies: depreciation and full cost for listed equipment (see *section 10*)
- The following parts of the award criteria in section 9 are exceptionally NOT applicable for this topic:
 - extent to which the project would reinforce and secure the digital technology supply chain in the Union*
 - extent to which the proposal can overcome financial obstacles such as the lack of market finance*
 - extent to which the proposal addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*

3. Available budget

The estimated available call budget is **EUR 4 000 000**.

Specific budget information per topic can be found in the table below:

Topic	Topic budget
DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs	EUR 2.000.000
DIGITAL-ECCC-2026-DEPLOY-CYBER-10- CBCH — Cross-Border Cyber Hubs	EUR 2.000.000

We reserve the right not to award all available funds or to redistribute them between the call priorities, depending on the proposals received and the results of the evaluation.

4. Timetable and deadlines

Timetable and deadlines (indicative)	
Call opening:	9 December 2025
<u>Deadline for submission:</u>	<u>28 May 2026 – 17:00:00 CET</u> <u>(Brussels)</u>
Evaluation:	June - July 2026
Information on evaluation results:	July – August 2026
GA signature:	November 2026

5. Admissibility and documents

Proposals must be submitted before the **call deadline** (see *timetable section 4*).

Proposals must be submitted **electronically** via the Funding & Tenders Portal Electronic Submission System (accessible via the Topic page in the [Calls for proposals](#) section). Paper submissions are NOT possible.

Proposals (including annexes and supporting documents) must be submitted using the forms provided *inside* the Submission System (⚠ NOT the documents available on the Topic page — they are only for information).

Proposals must be **complete** and contain all the requested information and all required annexes and supporting documents:


- Application Form Part A — contains administrative information about the participants (future coordinator, beneficiaries and affiliated entities) and the summarised budget for the project (*to be filled in directly online*)
- Application Form Part B — contains the technical description of the project (*template to be downloaded from the Portal Submission System, completed, assembled and re-uploaded*)
- **mandatory annexes and supporting documents** (*templates to be downloaded from the Portal Submission System, completed, assembled and re-uploaded*):
 - detailed budget table/calculator detailed budget table/calculator: not applicable
 - CVs of core project team: not applicable
 - activity reports of last year: not applicable
 - list of previous projects: not applicable
 - ownership control declarations (including for associated partners and subcontractors): applicable
 - **Other annexes:** for Topics DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH and DIGITAL-ECCC-2026-DEPLOY-CYBER-10- CBCH — Cross-Border Cyber Hubs the appointment decision from the Member State designating the entity to act as National CyberHUB: **applicable**.

At proposal submission, you will have to confirm that you have the **mandate to act** for all applicants. Moreover, you will have to confirm that the information in the application is correct and complete and that all participants comply with the conditions for receiving EU funding (*especially eligibility, financial and operational capacity, exclusion, etc*). Before signing the grant, each beneficiary and affiliated entity will have to confirm this again by signing a declaration of honour (DoH). Proposals without full support will be rejected.

Your application must be **readable, accessible and printable** (please check carefully the layout of the documents uploaded).

Proposals are limited to maximum **70 pages** (Part B). Evaluators will not consider any additional pages.

You may be asked at a later stage for further documents (*for legal entity validation, financial capacity check, bank account validation, etc*).

 For more information about the submission process (including IT aspects), consult the [Online Manual](#).

6. Eligibility

Eligible participants (eligible countries)

In order to be eligible, the applicants (beneficiaries and affiliated entities) must:

- be legal entities (public or private bodies)
- be established in one of the eligible countries, i.e.:
 - EU Member States (including overseas countries and territories (OCTs))
 - EEA countries (Norway, Iceland, Liechtenstein)

Beneficiaries and affiliated entities must register in the [Participant Register](#) — before submitting the proposal — and will have to be validated by the Central Validation Service (REA Validation). For the validation, they will be requested to upload documents showing legal status and origin.

Other entities may participate in other consortium roles, such as associated partners, subcontractors, third parties giving in-kind contributions, etc (*see section 13*).

Please be aware that all topics of this call are subject to restrictions due to security, therefore entities must not be directly or indirectly controlled from a country that is not an eligible country. All entities¹⁴ will have to fill in and submit a declaration on ownership and control.

Moreover:

- participation in any capacity (as beneficiary, affiliated entity, associated partner, subcontractor or recipient of financial support to third parties) is limited to entities established in and controlled from eligible countries
- project activities (included subcontracted work) must take place in eligible countries (*see section geographic location below and section 10*)

¹⁴ Except for entities that are validated as public bodies by the Central Validation Service.

– the Grant Agreement may provide for IPR restrictions (see section 10).



For restrictions limiting participation to specific eligible countries:

The condition must in principle be fulfilled already at proposal submission stage (call deadline); you cannot change status during GAP — unless agreed by the granting authority.

The following participants (beneficiaries, affiliated entities, associated partners and subcontractors) will be checked by the EU. Other participants must be checked by the consortium.

For the EU checks, the participants must register in the [Participant Register](#) (i.e. have at least a draft PIC). For beneficiaries and affiliated entities, the checks will be done on the basis of the validated PIC data. For other participants, the checks will be done on the basis of publicly available information.



For ownership control restrictions:

'Control' means the possibility to exercise decisive influence on the participant, directly or indirectly, through one or more intermediate entities, 'de jure' or 'de facto'. This includes not only ownership of more than 50% (shareholding), but also any other elements and/or rights that can amount to control.

The condition must in principle be fulfilled already at proposal submission stage (call deadline); you cannot change status during GAP — unless agreed by the granting authority.

The following participants (beneficiaries, affiliated entities, associated partners and subcontractors) will be checked by the EU. Other participants must be checked by the consortium.

For the EU checks, the participants must register in the [Participant Register](#) (i.e. have at least a draft PIC). They will be required to fill in and submit an [ownership control declaration](#)* as part of the proposal (and later on be requested to submit supporting documents). Where guarantees are allowed, ineligible entities will be requested to fill in the [guarantee template](#)*, have it approved by the competent authority of their country of establishment, and submit it to the granting authority which will assess their validity.

Finally, for all the topics grants will only be awarded to applicants that have succeeded the evaluation of the joint procurement action.

For more information, see *Annex 2*.

Specific cases and definitions

Natural persons — Natural persons are NOT eligible (with the exception of self-employed persons, i.e. sole traders, where the company does not have legal personality separate from that of the natural person).

International organisations — International organisations are NOT eligible, unless they are International organisations of European Interest within the meaning of Article 2 of the Digital Europe Regulation (i.e. international organisations the majority of whose members are Member States or whose headquarters are in a Member State).

Entities without legal personality — Entities which do not have legal personality under their national law may exceptionally participate, provided that their representatives have the capacity to undertake legal obligations on their behalf, and offer guarantees for the protection of the EU financial interests equivalent to that offered by legal persons¹⁵.

EU bodies — EU bodies (with the exception of the European Commission Joint Research Centre) can NOT be part of the consortium.

Associations and interest groupings — Entities composed of members may participate as 'sole beneficiaries' or 'beneficiaries without legal personality'¹⁶. ⚠ Please note that if the action will be implemented by the members, they should also participate (either as beneficiaries or as affiliated entities, otherwise their costs will NOT be eligible).

Countries currently negotiating association agreements — Beneficiaries from countries with ongoing negotiations for participating in the programme (*see list of participating countries above*) may participate in the call and can sign grants if the negotiations are concluded before grant signature and if the association covers the call (i.e. is retroactive and covers both the part of the programme and the year when the call was launched).

EU restrictive measures — Special rules apply for entities subject to [EU restrictive measures](#) under Article 29 of the Treaty on the European Union (TEU) and Article 215 of the Treaty on the Functioning of the EU (TFEU)¹⁷. Such entities are not eligible to participate in any capacity, including as beneficiaries, affiliated entities, associated partners, subcontractors or recipients of financial support to third parties (if any).

EU conditionality measures — Special rules apply for entities subject to measures adopted on the basis of EU Regulation 2020/2092¹⁸. Such entities are not eligible to participate in any funded role (beneficiaries, affiliated entities, subcontractors, recipients of financial support to third parties, etc). Currently such measures are in place, e.g. Hungarian public interest trusts established under the Hungarian Act IX of 2021 or any entity they maintain (see [Council Implementing Decision \(EU\) 2022/2506](#), as of 16 December 2022).

For more information, see [Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment](#).

Consortium composition

For the topic DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs: only entities designated at Member State level as National SOC are allowed to apply for funding and the project should be mono-beneficiary.

For the topic DIGITAL-ECCC-2026-DEPLOY-CYBER-10- CBCH — Cross-Border Cyber Hubs: consortia shall be composed by beneficiaries from at least 3 eligible countries in case of new cross-border CyberHUBs. In case of enlargement of an ongoing cross-border grant, the new consortium should be composed by the coordinator of the ongoing grant plus the new entities that want to join the hosting consortium of the cross-border SOC.

¹⁵ See Article 200(2)(c) EU Financial Regulation [2024/2509](#).

¹⁶ For the definitions, see Articles 190(2) and 200(2)(c) EU Financial Regulation [2024/2509](#).

¹⁷ Please note that the EU Official Journal contains the official list and, in case of conflict, its content prevails over that of the [EU Sanctions Map](#).

¹⁸ Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget (OJ L 325, 20.12.2022, p. 94).

Eligible activities

Applications will only be considered eligible if their content corresponds wholly (or at least in part) to the topic description for which they are submitted.

Eligible activities are the ones set out in section 2 above.

Projects should take into account the results of projects supported by other EU funding programmes. The complementarities must be described in the project proposals (Part B of the Application Form).

Projects must comply with EU policy interests and priorities (*such as environment, social, security, industrial and trade policy, etc*). Projects must also respect EU values and European Commission policy regarding reputational matters (*e.g. activities involving capacity building, policy support, awareness raising, communication, dissemination, etc*).

Financial support to third parties is not allowed.

Geographic location (target countries)

Due to restrictions due to security:

– for all topics: the proposals must relate to activities taking place in the eligible countries (see above)

Ethics

Projects must comply with:

- highest ethical standards and
- applicable EU, international and national law (including the [General Data Protection Regulation 2016/679](#)).

Proposals under this call will have to undergo an ethics review to authorise funding and may be made subject to specific ethics rules (which become part of the Grant Agreement in the form of ethics deliverables, *e.g. ethics committee opinions/notifications/authorisations required under national or EU law*).

For proposals involving development, testing, deployment, use or distribution of AI systems, the ethics review will in particular check compliance with the principles of human agency and oversight, diversity/fairness, transparency and responsible social impact, while the experts performing the technical evaluation will assess the robustness of the AI systems (i.e. their reliability not to cause unintentional harm).

Security

Projects involving EU classified information must undergo security scrutiny to authorise funding and may be made subject to specific security rules (detailed in a security aspects letter (SAL) which is annexed to the Grant Agreement).

These rules (governed by Decision [2015/444](#)¹⁹ and its implementing rules and/or national rules) provide for instance that:

- projects involving information classified TRES SECRET UE/EU TOP SECRET (or equivalent) can NOT be funded
- classified information must be marked in accordance with the applicable security instructions in the SAL
- information with classification levels CONFIDENTIEL UE/EU CONFIDENTIAL or above (and RESTREINT UE/ EU RESTRICTED, if required by national rules) may be:
 - created or accessed only on premises with facility security clearance (FSC) from the competent national security authority (NSA), in accordance with the national rules
 - handled only in a secured area accredited by the competent NSA
 - accessed and handled only by persons with valid personnel security clearance (PSC) and a need-to-know
- at the end of the grant, the classified information must either be returned or continue to be protected in accordance with the applicable rules
- action tasks involving EU classified information (EUCI) may be subcontracted only with prior written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of information agreement with the EU (or an administrative arrangement with the Commission)
- disclosure of EUCI to third parties is subject to prior written approval from the granting authority.

Please note that, depending on the type of activity, facility security clearance may have to be provided before grant signature. The granting authority will assess the need for clearance in each case and will establish their delivery date during grant preparation. Please note that in no circumstances can we sign any grant agreement until at least one of the beneficiaries in a consortium has facility security clearance.

Further security recommendations may be added to the Grant Agreement in the form of security deliverables (*e.g. create security advisory group, limit level of detail, use fake scenario, exclude use of classified information, etc*).

Beneficiaries must ensure that their projects are not subject to national/third-country security requirements that could affect implementation or put into question the award of the grant (*e.g. technology restrictions, national security classification, etc*). The granting authority must be notified immediately of any potential security issues.

¹⁹ See Commission Decision 2015/444/EU, Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

7. Financial and operational capacity and exclusion

Financial capacity

Applicants must have **stable and sufficient resources** to successfully implement the projects and contribute their share. Organisations participating in several projects must have sufficient capacity to implement all projects.

The financial capacity check will be carried out on the basis of the documents you will be requested to upload in the [Participant Register](#) during grant preparation (*e.g. profit and loss account and balance sheet, business plan, audit report produced by an approved external auditor, certifying the accounts for the last closed financial year, etc*). The analysis will be based on neutral financial indicators, but will also take into account other aspects, such as dependency on EU funding and deficit and revenue in previous years.

The check will normally be done for all beneficiaries, except:

- public bodies (entities established as public body under national law, including local, regional or national authorities) or international organisations
- if the individual requested grant amount is not more than EUR 60 000.

If needed, it may also be done for affiliated entities.

If we consider that your financial capacity is not satisfactory, we may require:

- further information
- an enhanced financial responsibility regime, i.e. joint and several responsibility for all beneficiaries or joint and several liability of affiliated entities (*see below, section 10*)
- prefinancing paid in instalments
- (one or more) prefinancing guarantees (*see below, section 10*)

or

- propose no prefinancing
- request that you are replaced or, if needed, reject the entire proposal.

 For more information, see [Rules for Legal Entity Validation, LEAR Appointment and Financial Capacity Assessment](#).

Operational capacity

Applicants must have the **know-how, qualifications** and **resources** to successfully implement the projects and contribute their share (including sufficient experience in projects of comparable size and nature).

This capacity will be assessed together with the 'Implementation' award criterion, on the basis of the competence and experience of the applicants and their project teams, including operational resources (human, technical and other) or, exceptionally, the measures proposed to obtain it by the time the task implementation starts.

If the evaluation of the award criterion is positive, the applicants are considered to have sufficient operational capacity.

Applicants will have to show their capacity via the following information:

- general profiles (qualifications and experiences) of the staff responsible for managing and implementing the project
- description of the consortium participants

Additional supporting documents may be requested, if needed to confirm the operational capacity of any applicant.

Exclusion

Applicants which are subject to an **EU exclusion decision** or in one of the following **exclusion situations** that bar them from receiving EU funding can NOT participate²⁰:

- bankruptcy, winding up, affairs administered by the courts, arrangement with creditors, suspended business activities or other similar procedures (including procedures for persons with unlimited liability for the applicant's debts)
- in breach of social security or tax obligations (including if done by persons with unlimited liability for the applicant's debts)
- guilty of grave professional misconduct²¹ (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- committed fraud, corruption, links to a criminal organisation, money laundering, terrorism-related crimes (including terrorism financing), child labour or human trafficking (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- shown significant deficiencies in complying with main obligations under an EU procurement contract, grant agreement, prize, expert contract, or similar (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- guilty of irregularities within the meaning of Article 1(2) of EU Regulation [2988/95](#) (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- created under a different jurisdiction with the intent to circumvent fiscal, social or other legal obligations in the country of origin or created another entity with this purpose (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)

²⁰ See Articles 138 and 143 of EU Financial Regulation [2024/2509](#).

²¹ 'Professional misconduct' includes, in particular, the following: violation of ethical standards of the profession; wrongful conduct with impact on professional credibility; breach of generally accepted professional ethical standards; false declarations/misrepresentation of information; participation in a cartel or other agreement distorting competition; violation of IPR; attempting to influence decision-making processes by taking advantage, through misrepresentation, of a conflict of interests, or to obtain confidential information from public authorities to gain an advantage; incitement to discrimination, hatred or violence or similar activities contrary to the EU values where negatively affecting or risking to affect the performance of a legal commitment.

- intentionally and without proper justification resisted²² an investigation, check or audit carried out by an EU authorising officer (or their representative or auditor), OLAF, the EPPO, or the European Court of Auditors.

Applicants will also be rejected if it turns out that²³:

- during the award procedure they misrepresented information required as a condition for participating or failed to supply that information
- they were previously involved in the preparation of the call and this entails a distortion of competition that cannot be remedied otherwise (conflict of interest).

Moreover, for the topics DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs and DIGITAL-ECCC-2026-DEPLOY-CYBER-10- CBCH — Cross-Border Cyber Hubs grants will only be awarded to applicants that have succeeded the evaluation of the joint procurement action.

8. Evaluation and award procedure

The proposals will have to follow the **standard submission and evaluation procedure** (one-stage submission + one-step evaluation).

An **evaluation committee** (assisted by independent outside experts) will assess all applications. Proposals will first be checked for formal requirements (admissibility, and eligibility, see *sections 5 and 6*). Proposals found admissible and eligible will be evaluated (for each topic) against the operational capacity and award criteria (see *sections 7 and 9*) and then ranked according to their scores.

For proposals with the same score (within a topic or budget envelope) a **priority order** will be determined according to the following approach:

Successively for every group of *ex aequo* proposals, starting with the highest scored group, and continuing in descending order:


- 1) Proposals focusing on a theme that is not otherwise covered by higher ranked proposals will be considered to have the highest priority.
- 2) The *ex aequo* proposals within the same topic will be prioritised according to the scores they have been awarded for the award criterion 'Relevance'. When these scores are equal, priority will be based on their scores for the criterion 'Impact'. When these scores are equal, priority will be based on their scores for the criterion 'Implementation'.
- 3) If this does not allow to determine the priority, a further prioritisation can be done by considering the overall proposal portfolio and the creation of positive synergies between proposals, or other factors related to the objectives of the call. These factors will be documented in the panel report.
- 4) After that, the remainder of the available call budget will be used to fund projects across the different topics in order to ensure a balanced spread of the geographical and thematic coverage and while respecting to the maximum possible extent the order of merit based on the evaluation of the award criteria.

²² 'Resisting an investigation, check or audit' means carrying out actions with the goal or effect of preventing, hindering or delaying the conduct of any of the activities needed to perform the investigation, check or audit, such as refusing to grant the necessary access to its premises or any other areas used for business purposes, concealing or refusing to disclose information or providing false information.

²³ See Article 143 EU Financial Regulation [2024/2509](#).

All proposals will be informed about the evaluation result (**evaluation result letter**). Successful proposals will be invited for grant preparation; the other ones will be put on the reserve list or rejected.

All proposals will be informed about the evaluation result (evaluation result letter). Successful proposals will be invited for grant preparation; the other ones will be put on the reserve list or rejected.

 No commitment for funding — Invitation to grant preparation does NOT constitute a formal commitment for funding. We will still need to make various legal checks before grant award: *legal entity validation, financial capacity, exclusion check, etc.*

Grant preparation will involve a dialogue in order to fine-tune technical or financial aspects of the project and may require extra information from your side. It may also include adjustments to the proposal to address recommendations of the evaluation committee or other concerns. Full compliance will be a pre-condition for signing the grant.

If you believe that the evaluation procedure was flawed, you can submit a **complaint** (following the deadlines and procedures set out in the evaluation result letter). Please note that notifications which have not been opened within 10 days after sending will be considered to have been accessed and that deadlines will be counted from opening/access (see also [Funding & Tenders Portal Terms and Conditions](#)). Please also be aware that for complaints submitted electronically, there may be character limitations.

9. Award criteria

The **award criteria** for this call are as follows:

1. Relevance

- Alignment with the objectives and activities as described in section 2
- Contribution to long-term policy objectives, relevant policies and strategies, and synergies with activities at European and national level
- Extent to which the project would reinforce and secure the digital technology supply chain in the EU*
- Extent to which the project can overcome financial obstacles such as the lack of market finance*

2. Implementation

- Maturity of the project
- Soundness of the implementation plan and efficient use of resources
- Capacity of the applicants, and when applicable the consortium as a whole, to carry out the proposed work

3. Impact

- Extent to which the project will achieve the expected outcomes and deliverables referred to in the call for proposals and, where relevant, the plans to disseminate and communicate project achievements

- Extent to which the project will strengthen competitiveness and bring important benefits for society
- Extent to which the project addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects *.

**May not be applicable to all topics (see specific topic conditions in section 2).*

Award criteria	Minimum pass score	Maximum score
Relevance	3	5
Implementation	3	5
Impact	3	5
Overall (pass) scores	10	15

Maximum points: 15 points.

Individual thresholds per criterion: 3/5, 3/5 and 3/5 points.

Overall threshold: 10 points.

Proposals that pass the individual thresholds AND the overall threshold will be considered for funding — within the limits of the available budget (i.e. up to the budget ceiling). Other proposals will be rejected.

10. Legal and financial set-up of the Grant Agreements

If you pass evaluation, your project will be invited for grant preparation, where you will be asked to prepare the Grant Agreement together with the EU Project Officer.

This Grant Agreement will set the framework for your grant and its terms and conditions, in particular concerning deliverables, reporting and payments.

The Model Grant Agreement that will be used (and all other relevant templates and guidance documents) can be found on [Portal Reference Documents](#).

Starting date and project duration

The project starting date and duration will be fixed in the Grant Agreement (*Data Sheet, point 1*). Normally the starting date will be after grant signature. A retroactive starting date can be granted exceptionally for duly justified reasons— but never earlier than the proposal submission date.

Project duration:

- For topic DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs the indicative duration of the action is indicatively 36 months, other durations are not excluded.

– For topic DIGITAL-ECCC-2026-DEPLOY-CYBER-10- CBCH — Cross-Border Cyber Hubs the indicative duration of the action is indicatively 36 months, other durations are not excluded.

Extensions are possible, if duly justified and through an amendment. Only if in agreement with the ECCC.

Milestones and deliverables

The milestones and deliverables for each project will be managed through the Portal Grant Management System and will be reflected in Annex 1 of the Grant Agreement.

The following deliverables will be mandatory for all projects:

- additional deliverable on dissemination and exploitation, to be submitted in the first six months of the project

Form of grant, funding rate and maximum grant amount

The grant parameters (*maximum grant amount, funding rate, total eligible costs, etc*) will be fixed in the Grant Agreement (*Data Sheet, point 3 and art 5*).

Project budget (requested grant amount):

- for topic DIGITAL-ECCC-2026-DEPLOY-CYBER-10-NCH — National Cyber Hubs: approximatively 1 million EUR per project but other amounts are not excluded.
- for topics DIGITAL-ECCC-2026-DEPLOY-CYBER-10- CBCH — Cross-Border Cyber Hubs: indicatively between 1 and 2 million EUR per project but other amounts are not excluded.

The grant awarded may be lower than the amount requested. The minimum budget for each topic as listed above is strongly recommended.

The grant will be a budget-based mixed actual cost grant (actual costs, with unit cost and flat-rate elements). This means that it will reimburse ONLY certain types of costs (eligible costs) and costs that were *actually* incurred for your project (NOT the *budgeted* costs). For unit costs and flat-rates, you can charge the amounts calculated as explained in the Grant Agreement (*see art 6 and Annex 2 and 2a*).

The costs will be reimbursed at the funding rate fixed in the Grant Agreement. This rate depends on the type of action which applies to the topic (*see section 2*).

Grants may NOT produce a profit (i.e. surplus of revenues + EU grant over costs). For-profit organisations must declare their revenues and, if there is a profit, we will deduct it from the final grant amount (*see art 22.3*).

Moreover, please be aware that the final grant amount may be reduced in case of non-compliance with the Grant Agreement (*e.g. improper implementation, breach of obligations, etc*).

Budget categories and cost eligibility rules

The budget categories and cost eligibility rules are fixed in the Grant Agreement (*Data Sheet, point 3 and art 6*).

Budget categories for this call:

- A. Personnel costs
 - A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons
 - A.4 SME owners and natural person beneficiaries
- B. Subcontracting costs
- C. Purchase costs
 - C.1 Travel and subsistence
 - C.2 Equipment
 - C.3 Other goods, works and services
- D. Other cost categories
 - D.1 Financial support to third parties – Not applicable
 - D.2 Internally invoiced goods and services
- E. Indirect costs

Specific cost eligibility conditions for this call:

- personnel costs:
 - average personnel costs (unit cost according to usual cost accounting practices)²⁴: Yes
 - SME owner/natural person unit cost²⁵: Yes
- travel and subsistence unit costs²⁶: No (only actual costs)
- equipment costs:
 - depreciation + full cost for listed equipment (for all topics)
- other cost categories:
 - costs for financial support to third parties: not allowed
 - internally invoiced goods and services (unit cost according to usual cost accounting practices)²⁷: Yes
- indirect cost flat-rate: 7% of the eligible direct costs (categories A-D, except volunteers costs and exempted specific cost categories, if any).

²⁴ [Decision](#) of 29 June 2021 authorising the use of unit costs based on usual cost accounting practices for actions under the Digital Europe Programme.

²⁵ Commission [Decision](#) of 20 October 2020 authorising the use of unit costs for the personnel costs of the owners of small and medium-sized enterprises and beneficiaries that are natural persons not receiving a salary for the work carried out by themselves under an action or work programme (C(2020)7115).

²⁶ Commission [Decision](#) of 12 January 2021 authorising the use of unit costs for travel, accommodation and subsistence costs under an action or work programme under the 2021-2027 multi-annual financial framework (C(2021)35).

²⁷ [Decision](#) of 29 June 2021 authorising the use of unit costs based on usual cost accounting practices for actions under the Digital Europe Programme.

- VAT: non-deductible/non-refundable VAT is eligible (but please note that since 2013 VAT paid by beneficiaries that are public bodies acting as public authority is NOT eligible)
- other:
 - in-kind contributions for free are allowed, but cost-neutral, i.e. they cannot be declared as cost
 - kick-off meeting: costs for kick-off meeting organised by the granting authority are eligible (travel costs for maximum 2 persons, return ticket to Brussels and accommodation for one night) only if the meeting takes place after the project starting date set out in the Grant Agreement; the starting date can be changed through an amendment, if needed
 - project websites: communication costs for presenting the project on the participants' websites or social media accounts are eligible; costs for *separate* project websites are not eligible
 - restrictions due to security:
 - country restrictions for subcontracting costs: Yes, subcontracted work must be performed in the eligible countries
 - eligible cost country restrictions: Yes, only costs for activities carried out in eligible countries are eligible
 - other ineligible costs: No.

Reporting and payment arrangements


The reporting and payment arrangements are fixed in the Grant Agreement (*Data Sheet, point 4 and art 21 and 22*).

After grant signature, you will normally receive a **prefinancing** to start working on the project (float of normally **80%** of the maximum grant amount; exceptionally less or no prefinancing). The prefinancing will be paid 30 days from entry into force/10 days before starting date/financial guarantee (if required) – whichever is the latest.

There will be one or more **interim payments** (with cost reporting through the use of resources report).

Payment of the balance: At the end of the project, we will calculate your final grant amount. If the total of earlier payments is higher than the final grant amount, we will ask you (your coordinator) to pay back the difference (recovery).

All payments will be made to the coordinator.

 Please be aware that payments will be automatically lowered if you or one of your consortium members has outstanding debts towards the EU (granting authority or other EU bodies). Such debts will be offset by us — in line with the conditions set out in the Grant Agreement (*see art 22*).

Please also note that you are responsible for **keeping records** on all the work done and the costs declared.

Prefinancing guarantees

If a prefinancing guarantee is required, it will be fixed in the Grant Agreement (*Data Sheet, point 4*). The amount will be set during grant preparation and it will normally be equal or lower than the prefinancing for your grant.

The guarantee should be in euro and issued by an approved bank/financial institution established in an EU Member State. If you are established in a non-EU country and would like to provide a guarantee from a bank/financial institution in your country, please contact us (this may be exceptionally accepted, if it offers equivalent security).

Amounts blocked in bank accounts will NOT be accepted as financial guarantees.

Prefinancing guarantees are normally requested from the coordinator, for the consortium. They must be provided during grant preparation, in time to make the prefinancing (scanned copy via Portal AND original by post).

If agreed with us, the bank guarantee may be replaced by a guarantee from a third party.

The guarantee will be released at the end of the grant, in accordance with the conditions laid down in the Grant Agreement (*art 23*).

Certificates

Depending on the type of action, size of grant amount and type of beneficiaries, you may be requested to submit different certificates. The types, schedules and thresholds for each certificate are fixed in the Grant Agreement (*Data Sheet, point 4 and art 24*).

Liability regime for recoveries

The liability regime for recoveries will be fixed in the Grant Agreement (*Data Sheet, point 4.4 and art 22*).

For beneficiaries, it is one of the following:

- limited joint and several liability with individual ceilings — *each beneficiary up to their maximum grant amount*
 - unconditional joint and several liability — *each beneficiary up to the maximum grant amount for the action*
- or
- individual financial responsibility — *each beneficiary only for their own debts*.

In addition, the granting authority may require joint and several liability of affiliated entities (with their beneficiary).

Provisions concerning the project implementation

Security rules: see *Model Grant Agreement (art 13 and Annex 5)*

Ethics rules: see *Model Grant Agreement (art 14 and Annex 5)*

IPR rules: *see Model Grant Agreement (art 16 and Annex 5)*:

- background and list of background: Yes
- protection of results: Yes
- exploitation of results: Yes
- rights of use on results: Yes
- access to results for policy purposes: Yes
- access to results in case of a public emergency: Yes
- access rights to ensure continuity and interoperability obligations: No
- special IPR obligations linked to restrictions due to security:
 - exploitation in eligible countries: Yes
 - limitations to transfers and licensing: Yes

Communication, dissemination and visibility of funding: *see Model Grant Agreement (art 17 and Annex 5)*:

- communication and dissemination plan: Yes
- dissemination of results: Yes
- additional dissemination obligations: Yes
- additional communication activities: Yes
- special logo: Yes - both EU and European Cybersecurity Competence Centre logo

Specific rules for carrying out the action: *see Model Grant Agreement (art 18 and Annex 5)*:

- specific rules for PAC Grants for Procurement: No
- specific rules for Grants for Financial Support: No
- specific rules for blending operations: No
- special obligations linked to restrictions due to security:
 - implementation in case of restrictions due to security or EU strategic autonomy: Yes

Other specificities

Consortium agreement: Yes – in case of more than one beneficiary.

Non-compliance and breach of contract

The Grant Agreement (chapter 5) provides for the measures we may take in case of breach of contract (and other non-compliance issues).



For more information, see [AGA — Annotated Grant Agreement](#).

11. How to submit an application

All proposals must be submitted directly online via the Funding & Tenders Portal Electronic Submission System. Paper applications are NOT accepted.

Submission is a **2-step process**:

a) create a user account and register your organisation

To use the Submission System (the only way to apply), all participants need to [create an EU Login user account](#).

Once you have an EU Login account, you can [register your organisation](#) in the Participant Register. When your registration is finalised, you will receive a 9-digit participant identification code (PIC).

b) submit the proposal

Access the Electronic Submission System via the Topic page in the [Calls for proposals](#) section (or, for calls sent by invitation to submit a proposal, through the link provided in the invitation letter).

Submit your proposal in 3 parts, as follows:

- Part A includes administrative information about the applicant organisations (future coordinator, beneficiaries, affiliated entities and associated partners) and the summarised budget for the proposal. Fill it in directly online
- Part B (description of the action) covers the technical content of the proposal. Download the mandatory word template from the Submission System, fill it in and upload it as a PDF file
- Annexes (*see section 5*). Upload them as PDF file (single or multiple depending on the slots). Excel upload is sometimes possible, depending on the file type.

The proposal must keep to the **page limits** (*see section 5*); excess pages will be disregarded.

Documents must be uploaded to the **right category** in the Submission System, otherwise the proposal may be considered incomplete and thus inadmissible.

The proposal must be submitted **before the call deadline** (*see section 4*). After this deadline, the system is closed and proposals can no longer be submitted.

Once the proposal is submitted, you will receive a **confirmation e-mail** (with date and time of your application). If you do not receive this confirmation e-mail, it means your

proposal has NOT been submitted. If you believe this is due to a fault in the Submission System, you should immediately file a complaint via the [IT Helpdesk webform](#), explaining the circumstances and attaching a copy of the proposal (and, if possible, screenshots to show what happened).

Details on processes and procedures are described in the [Online Manual](#). The Online Manual also contains the links to FAQs and detailed instructions regarding the Portal Electronic Exchange System.

12. Help

As far as possible, ***please try to find the answers you need yourself***, in this and the other documentation (we have limited resources for handling direct enquiries):

- [Online Manual](#)
- Topic Q&A on the Topic page (for call-specific questions in open calls; not applicable for actions by invitation)
- [Portal FAQ](#) (for general questions).

Please also consult the Topic page regularly, since we will use it to publish call updates. (For invitations, we will contact you directly in case of a call update).

Contact

For individual questions on the Portal Submission System, please contact the [IT Helpdesk](#).

Non-IT related questions should be sent to the ECCC Applicants Direct Contact Centre (ADCC), only after consultation of the [National Coordination Centre](#), at the following email address: applicants@eccc.europa.eu

Please indicate clearly the reference of the call and topic to which your question relates (see cover page).

13. Important



IMPORTANT

- **Don't wait until the end** — Complete your application sufficiently in advance of the deadline to avoid any last minute **technical problems**. Problems due to last minute submissions (*e.g. congestion, etc*) will be entirely at your risk. Call deadlines can NOT be extended.
- **Consult** the Portal Topic page regularly. We will use it to publish updates and additional information on the call (call and topic updates).
- **Funding & Tenders Portal Electronic Exchange System** — By submitting the application, all participants **accept** to use the electronic exchange system in accordance with the [Portal Terms & Conditions](#).
- **Registration** — Before submitting the application, all beneficiaries, affiliated entities and associated partners must be registered in the [Participant Register](#). The participant identification code (PIC) (one per participant) is mandatory for the Application Form.
- **Consortium roles** - When setting up your consortium, you should think of organisations that help you reach objectives and solve problems.

The roles should be attributed according to the level of participation in the project. Main participants should participate as **beneficiaries** or **affiliated entities**; other entities can participate as associated partners, subcontractors, third parties giving in-kind contributions. **Associated partners** and third parties giving in-kind contributions should bear their own costs (they will not become formal recipients of EU funding). **Subcontracting** should normally constitute a limited part and must be performed by third parties (not by one of the beneficiaries/affiliated entities). Subcontracting going beyond 30% of the total eligible costs must be justified in the application.

- **Coordinator** — In multi-beneficiary grants, the beneficiaries participate as consortium (group of beneficiaries). They will have to choose a coordinator, who will take care of the project management and coordination and will represent the consortium towards the granting authority. In mono-beneficiary grants, the single beneficiary will automatically be coordinator.
- **Affiliated entities** — Applicants may participate with affiliated entities (i.e. entities linked to a beneficiary which participate in the action with similar rights and obligations as the beneficiaries, but do not sign the grant and therefore do not become beneficiaries themselves). They will get a part of the grant money and must therefore comply with all the call conditions and be validated (just like beneficiaries); but they do not count towards the minimum eligibility criteria for consortium composition (if any). If affiliated entities participate in your project, please do not forget to provide documents demonstrating their affiliation link to your organisation as part of your application.
- **Associated partners** — Applicants may participate with associated partners (i.e. partner organisations which participate in the action but without the right to get grant money). They participate without funding and therefore do not need to be validated.
- **Consortium agreement** — For practical and legal reasons it is recommended to set up internal arrangements that allow you to deal with exceptional or unforeseen circumstances (in all cases, even if not mandatory under the Grant Agreement). The consortium agreement also gives you the possibility to redistribute the grant money according to your own consortium-internal principles and parameters (for instance, one beneficiary can reattribute its grant money to another beneficiary). The consortium agreement thus allows you to customise the EU grant to the needs inside your consortium and can also help to protect you in case of disputes.

- **Balanced project budget** - Grant applications must ensure a balanced project budget and sufficient other resources to implement the project successfully (*e.g. own contributions, income generated by the action, financial contributions from third parties, etc*). You may be requested to lower your estimated costs, if they are ineligible (including excessive).
- **Completed/ongoing projects** — Proposals for projects that have already been completed will be rejected; proposals for projects that have already started will be assessed on a case-by-case basis (in this case, no costs can be reimbursed for activities that took place before the project starting date/proposal submission).
- **No-profit rule** — Grants may NOT give a profit (i.e. surplus of revenues + EU grant over costs). This will be checked by us at the end of the project.
- **No cumulation of funding/no double funding** — It is strictly prohibited to cumulate funding from the EU budget (except under 'EU Synergies actions'). Outside such Synergies actions, any given action may receive only ONE grant from the EU budget and cost items may under NO circumstances be declared under two EU grants; projects must be designed as different actions, clearly delineated and separated for each grant (without overlaps).
- **Combination with EU operating grants** — Combination with EU operating grants is possible, if the project remains outside the operating grant work programme and you make sure that cost items are clearly separated in your accounting and NOT declared twice (see [AGA — Annotated Grant Agreement, art 6.2.E](#)).
- **Multiple proposals** — Applicants may submit more than one proposal for *different* projects under the same call (and be awarded funding for them).
Organisations may participate in several proposals.
BUT: if there are several proposals for *very similar* projects, only one application will be accepted and evaluated; the applicants will be asked to withdraw the others (or they will be rejected).
- **Resubmission** — Proposals may be changed and re-submitted until the deadline for submission.
- **Rejection** — By submitting the application, all applicants accept the call conditions set out in this Call document (and the documents it refers to). Proposals that do not comply with all the call conditions will be rejected. This applies also to applicants: All applicants need to fulfil the criteria; if any one of them doesn't, they must be replaced or the entire proposal will be rejected.
- **Cancellation** — There may be circumstances which may require the cancellation of the call. In this case, you will be informed via a call or topic update. Please note that cancellations are without entitlement to compensation.
- **Language** — You can submit your proposal in any official EU language (project abstract/summary should however always be in English). For reasons of efficiency, we strongly advise you to use English for the entire application. If you need the call documentation in another official EU language, please submit a request within 10 days after call publication (for the contact information, see *section 12*).

- **Transparency** — In accordance with Article 38 of the [EU Financial Regulation](#), information about EU grants awarded is published each year on the [Europa website](#).

This includes:

- beneficiary names
- beneficiary addresses
- the purpose for which the grant was awarded
- the maximum amount awarded.

The publication can exceptionally be waived (on reasoned and duly substantiated request), if there is a risk that the disclosure could jeopardise your rights and freedoms under the EU Charter of Fundamental Rights or harm your commercial interests.

- **Data protection** — The submission of a proposal under this call involves the collection, use and processing of personal data. This data will be processed in accordance with the applicable legal framework. It will be processed solely for the purpose of evaluating your proposal, subsequent management of your grant and, if needed, programme monitoring, evaluation and communication. Details are explained in the [Funding & Tenders Portal Privacy Statement](#).

Annex 1**Digital Europe types of action**

The Digital Europe Programme uses the following actions to implement grants:

Simple Grants

Description: Simple Grants (SIMPLE) are a flexible type of action used by a large variety of topics and can cover most activities. The consortium will mostly use personnel costs to implement action tasks, activities with third parties (subcontracting, financial support, purchase) are possible but should be limited.

Funding rate: 50%

Payment model: Prefinancing – (x) interim payment(s) – final payment

SME Support Actions

Description: SME Support Actions (SME) are a type of action primarily consisting of activities directly aiming to support SMEs involved in building up and the deployment of the digital capacities. This type of action can also be used if SMEs need to be in the consortium and make investments to access the digital capacities.

Funding rate: 50% except for SMEs where a rate of 75% applies

Payment model: Prefinancing – (x) interim payment(s) – final payment

Coordination and Support Actions (CSAs)

Description: Coordination and Support Actions (CSAs) are a small type of action (a typical amount of 1-2 Mio) with the primary goal to support EU policies. Activities can include coordination between different actors for accompanying measures such as standardisation, dissemination, awareness-raising and communication, networking, coordination or support services, policy dialogues and mutual learning exercises and studies, including design studies for new infrastructure and may also include complementary activities of strategic planning, networking and coordination between programmes in different countries.

Funding rate: 100%

Payment model: Prefinancing – (x) interim payment(s) – final payment

Grants for Procurement

Description: Grants for Procurement (GP) are a special type of action where the main goal of the action (and thus the majority of the costs) consist of buying goods or services and/or subcontracting tasks. Contrary to the PAC Grants for Procurement (see *below*) there are no specific procurement rules (i.e. usual rules for purchase apply), nor is there a limit to 'contracting authorities/entities'. Personnel costs should be limited in this type of action; they are in general used to manage the grant, coordination between the beneficiaries, preparation of the procurements.

Funding rate: 50%

Payment model: Prefinancing - second prefinancing (to provide the necessary cash-flow to finance the procurements) – payment of the balance

PAC Grants for Procurement

Description: PAC Grants for Procurement (PACGP) are a specific type of action for procurement in grant agreements by 'contracting authorities/entities' as defined in the EU Public Procurement Directives (Directives 2014/24/EU , 2014/25/EU and 2009/81/EC) aiming at innovative digital goods and services (i.e. novel technologies on the way to commercialisation but not yet broadly available).

Funding rate: 50%

Payment model: Prefinancing - second prefinancing (to provide the necessary cash-flow to finance the procurements) – payment of the balance

Grants for Financial Support

Description: Grants for Financial Support (GfS) have a particular focus on cascading grants. The majority of the grant will be distributed via financial support to third parties with special provisions in the grant agreement, maximum amounts to third parties, multiple pre-financing and reporting obligations.

Annex 5 of the model grant agreements foresees specific rules for this type of action regarding conflict of interest, the principles of transparency, non-discrimination and sound financial management as well as the selection procedure and criteria.

In order to assure the co-financing obligation in the programme, the support to third parties should only cover 50% of third party costs.

Funding rate: 100% for the consortium, co-financing of 50% by the supported third party

Payment model: Prefinancing - second prefinancing (to provide the necessary cash-flow to finance sub-grants) – payment of the balance

Lump Sum Grants

Description: Lump Sum Grants (LS) reimburse a general lump sum for the entire project and the consortium as a whole. The lump sum is fixed ex-ante (at the latest at grant signature). on the basis of a methodology defined by the granting authority (either on the basis of a detailed project budget or other pre-defined parameters). The lump sum will cover all the beneficiaries' direct and indirect costs for the project. The beneficiaries do not need to report actual costs, they just need to claim the lump sum once the work is done. If the action is not properly implemented only part of the lump sum will be paid.

Funding rate: 100%/50%/50% and 75% (for SMEs)

Payment model: Prefinancing – (x) interim payment(s)– final payment

Framework Partnerships (FPAs) and Specific Grants (SGAs)

FPAs

Description: FPAs establish a long-term cooperation mechanism between the granting authority and the beneficiaries of grants. The FPA specifies the common objectives (action plan) and the procedure for awarding specific grants. The specific grants are awarded via identified beneficiary actions (with or without competition).

Funding rate: no funding for FPA

SGAs

Description: The SGAs are linked to an FPA and implement the action plan (or part of it). They are awarded via an invitation to submit a proposal (identified beneficiary action). The consortium composition should in principle match (meaning that only entities that are part of the FPA can participate in an SGA), but otherwise the implementation is rather flexible. FPAs and SGAs can have different coordinators ; other partners of the FPA are free to participate in an SGA or not. There is no limit to the amount of SGAs signed under one FPA.

Funding rate: 50%

Payment model: Prefinancing – (x) interim payment(s) – final payment

Annex 2**Eligibility restrictions under Articles 12(5) and (6) and 18(4) of the Digital Europe Regulation****Security restrictions Article 12(5) and (6)**

If indicated in the Digital Europe Work Programme, and if justified for security reasons, topics can exclude the participation of legal entities *established* in a third country or DEP associated country, or established in the EU territory but *controlled* by a third country or third country legal entities (including DEP associated countries)²⁸.

This restriction is applicable for SO1 (High Performance Computing), SO2 (Artificial Intelligence) and SO3 (Cybersecurity), but at different levels.

- In the case of SO3, the provision is implemented in the strictest way. When activated, only entities established in the EU AND controlled from the EU will be able to participate; entities from associated countries (which are normally eligible) can NOT participate — unless otherwise provided in the Work Programme.
- In SO1 and SO2, entities established in associated countries and entities controlled from non-EU countries may participate, if they comply with the conditions set out in the Work Programme (usually:
 - for the associated countries: be formally associated to Digital Europe Programme and receive a positive assessment by the Commission on the replies to their associated country security questionnaire.
 - for the participants: submission of a guarantee demonstrating that they have taken measures to ensure that their participation does not contravene security or EU strategic autonomy interests).



EEA countries (and participants from EEA countries) are exempted from these restrictions (and additional requirements) because EEA countries benefit from a status equivalent to the Member States.

In order to determine the ownership and control status, participants²⁹ will be required to fill in and submit an [ownership control declaration](#)* as part of the proposal (and later on be requested to submit supporting documents) (see [Guidance on participation in EU restricted calls with ownership and control restrictions](#)*).

In addition, where a guarantee is required, the participants will also have to fill in the [guarantee template](#)*, approved by the competent authorities of their country of establishment, and submit it to the granting authority which will assess its validity.

The activation of these restrictions will also make a number of specific provisions in the Grant Agreement applicable, such as country restrictions for eligible costs, country restrictions for subcontracting, and special rules for implementation, exploitation of results and transfers and exclusive licensing of results.

Thus:

²⁸ See Article 12(5) and (6) of the Digital Europe Regulation [2021/694](#).

²⁹ Beneficiaries and affiliated entities, associated partners and subcontractors — except for entities that are validated as public bodies by the Central Validation Service.

- participation in any capacity (as beneficiary, affiliated entity, associated partner, subcontractor or recipient of financial support to third parties) is also limited to entities established in and controlled from eligible countries
- project activities (included subcontracted work) must take place in eligible countries
- the Grant Agreement provides for specific IPR restrictions.

Strategic autonomy restrictions Article 18(4)

If indicated in the Digital Europe Work Programme, calls can limit the participation to entities *established* in the EU, and/or entities established in third countries associated to the programme for EU strategic autonomy reasons³⁰.

The activation of these restrictions will make a number of specific provisions in the Grant Agreement applicable, such as country restrictions for eligible costs, country restrictions for subcontracting, and special rules for implementation, exploitation of results and transfers and exclusive licensing of results.

 For more information, see [Guidance on participation in EU restricted calls with ownership and control restrictions](#)*.

³⁰ See Article 18(4) of the Digital Europe Regulation [2021/694](#).