



ECCC 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Digital Europe Programme (DIGITAL)

Call for proposals

Strengthening the Cybersecurity Ecosystem
(DIGITAL-ECCC-2025-DEPLOY-CYBER-08)

Version 1.0
12 June 2025



HISTORY OF CHANGES			
Version	Publication Date	Change	Page
1.0	12.06.2021	▪ Initial version.	
		▪	



CALL FOR PROPOSALS

Table of Contents

0. Introduction	5
1. Background	6
2. Topic description and conditions	7
DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PublicPQC — Transition to post-quantum Public Key Infrastructures	7
Objectives	7
Scope	7
Expected Outcome	9
KPIs to measure outcomes and deliverables	9
Targeted stakeholders	10
Type of action and funding rate	10
Specific topic conditions	10
DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC — Enhancing the NCC Network	10
Objectives	10
Scope	11
Expected Outcome	13
KPIs to measure outcomes and deliverables	14
Targeted stakeholders	15
Type of action and funding rate	15
Specific topic conditions	15
DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH — Dedicated action to reinforce hospitals and healthcare providers	15
Objectives	15
Scope	16
Expected Outcome	16
KPIs to measure outcomes and deliverables	17
Targeted stakeholders	17
Type of action and funding rate	17
Specific topic conditions	17
3. Available budget	18
4. Timetable and deadlines	18
5. Admissibility and documents	19
6. Eligibility	20
Eligible participants (eligible countries)	20
Specific cases and definitions	20

Consortium composition	21
Eligible activities.....	22
Geographic location (target countries).....	22
Ethics.....	22
Security.....	23
7. Financial and operational capacity and exclusion	24
Financial capacity	24
Operational capacity	24
Exclusion	25
8. Evaluation and award procedure	26
9. Award criteria.....	27
10. Legal and financial set-up of the Grant Agreements.....	28
Starting date and project duration	28
Milestones and deliverables.....	28
Form of grant, funding rate and maximum grant amount.....	29
Budget categories and cost eligibility rules.....	29
Reporting and payment arrangements.....	31
Prefinancing guarantees	31
Certificates	32
Liability regime for recoveries	32
Provisions concerning the project implementation.....	32
Other specificities	33
Non-compliance and breach of contract	33
11. How to submit an application.....	33
12. Help	34
13. Important	36
Annex 1	39
Annex 2	42


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-2025-DEPLOY-CYBER-08-PublicPQC — Transition to post-quantum Public Key Infrastructures**
- **DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC - Enhancing the NCC Network**
- **DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH - Dedicated action to reinforcing hospitals and healthcare providers**

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)

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.

- evaluation and award procedure (section 8)
- 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 reshape our lives—how we live, work, communicate, and interact with both the environment and each other. The increasing reliance on digital technologies and infrastructures brings immense opportunities, even though also significant vulnerabilities. Recent global disruptions, including the COVID-19 pandemic and Russia's war of aggression against Ukraine, have laid bare the critical dependencies and risks inherent in a hyperconnected digital world. These events reaffirm the strategic need for Europe to secure its digital sovereignty and reduce reliance on external technologies and infrastructures.

Cyber threats are becoming increasingly sophisticated and persistent, posing serious challenges not only to the economy and public services but also to the fundamental values and democratic institutions of the European Union. As such, reinforcing Europe's cybersecurity posture remains a top priority.

The third Work Programme (WP) on Cybersecurity under the Digital Europe Programme 2025–2027 outlines a series of targeted actions to strengthen the EU's cybersecurity ecosystem and enhance its resilience in line with the EU Cybersecurity Strategy and the ECCC Strategic Agenda.

This call focuses on three key areas:

- **Transition to Post-Quantum Public Key Infrastructures (PKI):** As quantum computing continues to evolve, the threat it poses to classical encryption methods becomes more immediate. This action supports the different actors involved in the Public Key Infrastructures (PKI) ecosystems and supply and value chains, who all have a unique set of diverse needs and interdependencies, such as Certificate Authorities (CAs), intermediate CAs, end-users in different domains, and vendors.
- **Enhancing the National Coordination Centre (NCC) Network:** The NCCs play a pivotal role in supporting the implementation of cybersecurity projects, fostering collaboration between public authorities, industry, and academia.

Strengthening the NCC network will reinforce national capacities, facilitate knowledge sharing, and improve coordination at the National and EU level. Actions included in this call document will support the objectives to deploy and support the National Coordination Centres (NCCs).

- **Dedicated Action to Reinforce Hospitals and Healthcare Providers:** The healthcare sector remains one of the most targeted by cyberattacks. This action will aim at strengthening the cybersecurity of hospitals and healthcare providers. The goal is to ensure that they can effectively detect, monitor, and respond to cyber threats, particularly ransomware, which pose significant risks, thereby enhancing the resilience of the European healthcare system.

All topics under this call are subject to Article 12(5) of the [Digital Europe Programme Regulation](#).

These initiatives collectively aim to build a more secure and resilient digital Europe—capable of withstanding future threats while promoting trust, innovation, and the safeguarding of European values in the digital age.

2. Topic description and conditions

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PublicPQC — Transition to post-quantum Public Key Infrastructures

Objectives

The aim of this call is to tackle the challenges of an effective integration of PQC algorithms in Public Key Infrastructures (PKIs), which offers efficient migration strategies and strong business continuity guarantees.

The call targets the different actors involved in the PKI ecosystems and supply and value chains, who all have a unique set of diverse needs and interdependencies, such as Certificate Authorities (CAs), intermediate CAs, researchers, end-users in different domains, and vendors.

Scope

Proposals shall target activities on the following subjects:

- design of digital signature combiners and key encapsulation mechanism combiners.
- the testing of deployment of certificates in protocols that use those certificates.
- the development of novel protocols for Automatic Certificate Management and revocation and of novel protocols for (privacy-friendly) certificate-transparency.
- the development of methods and tools that can be used by experts across various PKI domains, including all aspects of key management of asymmetric systems.

Proposals should carefully consider the requirements and constraints, such as security level, performance and business continuity, in a broad range of applications relevant for critical societal sectors and processes (such as governmental services, telecom, banking, smart homes, e-Health, automotive, and other sectors).

Proposals should address functions such as key establishment, digital signatures, and secure communication protocols that require careful adaptation with post-quantum counterparts to ensure resilience against threats posed by quantum-capable adversaries.

Proposals should safeguard compatibility with existing legacy systems. To achieve this, a transition to PKIs that support both pre-quantum and post-quantum cryptography should be addressed. The proposed systems should be able to seamlessly interact with legacy systems by disabling the post-quantum component as needed while preventing downgrade attacks. Relying solely on PQC solutions in this intermediate transition phase could introduce security risks given that the security analysis of the cryptosystems and of their implementations is not as mature as for their pre-quantum counterparts. Proposals should therefore use combinations of PQC solutions and established pre-quantum solutions, making sure to provide strongest-link security, meaning that the system remains secure as long as at least one of the components of the combination is secure.

For certificates for protocols that support negotiation, such as X.509 certificates for the Transport Layer (TLS), the use of post-quantum key exchange has already been demonstrated and can be implemented in a decentralised manner. Many other protocols need to be migrated, and this process will be more complex when old and new configurations must coexist. Moreover, for applications in IoT, smartcards, identity documents and others, the migration strategies defined for the core use cases of X.509 may well not work.

Proposals should develop clear procedures to effectively guide the various stakeholders involved in PKIs across different usage domains through the transition process.

Effective consortia should comprise a diverse range of actors along the entire PKI chain, encompassing expertise in areas such as software development, hardware implementation, cryptographic research, standardisation, policy, and application deployment, as well as organisations that can provide user case studies and real-world applications.

Activities should include some or all of the following:

- Identification of requirements necessary to implement hybrid certificates.
- Development of approaches and techniques for constructing cryptographic combiners for different protocols.
- Testing of the combiners for issuance of new certificates for the different applications, taking into consideration the need to balance the growth of key, signature, and ciphertext sizes, which can lead to compatibility issues with standards, such as PKI certificates, revocation mechanisms, (privacy-friendly) certificate transparency mechanisms, the use of different cryptographic protocols across certificate chains, the applications requirements, such as security level, time-constraints in signing and verification steps, communication/computational and storage overhead, and hardware optimisation requirements.
- Development of and/or further improvement of open-source libraries.
- Development of novel protocols for Automatic Certificate Management and revocation, and of novel protocols for (privacy-friendly) certificate-transparency. Support to standardisation activities.
- Development of recipes for the design and deployment of the new PKIs, with analysis that depends on each component of a given PKI.

- Tests on specialised uses of X.509 certificates other than the core cases using TLS, such as roots of trust, device integrity, firmware signing, and others.
- Design, improvement and testing of X.509 alternatives, such as, among others, Merkle tree ladders, the GNU Name System, older proposals such as SPKI and SDSI and the use of key encapsulation mechanisms for on-demand authentication in place of signatures.
- Awareness and training activities for stakeholders with different profiles, emphasising the interdependencies in the transition and facilitating a broader understanding of the technical standards amongst PKI users.

Participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, this topic is subject to Article 12(5) of Regulation (EU) 2021/694.

Expected Outcome

- New combiners ensuring that cryptographic schemes provide at least 128-bit security against quantum adversaries.
- Experimental evaluation on hybrid certificates in several standard protocols that use those certificates, also considering options for different cryptographic algorithms at the root Certification Authority level and at the other levels, in terms of security, performance, and backward compatibility. The impact of such certificates in protocols should be tested via open-source libraries.
- New and/or improved open-source libraries for certificate requests, issuance, validation, revocation and (privacy-friendly) certificate transparency.
- Clear procedures taking into account all aspects of key management: requirements for signature generation, in terms of the software and hardware used to create signatures as well as the secure storage and handling of private keys to maintain their authenticity and confidentiality, signature validation, with specification of the data required for verifying signatures and outlining the conditions necessary for a successful signature verification process, signature life-cycle process, and validity status of signatures.
- Test and evaluation of uses of X.509 certificates other than their core uses.
- Tests and evaluation of alternatives to X.509 certificates.
- Awareness activities and training courses.

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.

- Number of cybersecurity and/or tools deployed;
- Number of digital signature combiners and key encapsulation mechanism combiners designed;
- Number of novel protocols for Automatic Certificate Management developed;
- Number of new and/or improved open-source libraries for certificate;

- Number of tests and evaluation of uses of X.509 certificates other than their core uses;
- Number of awareness activities and training courses;
- Number and type of standardisation activities and contributions to them.

Targeted stakeholders

This topic targets in particular stakeholders involved in the Public Key Infrastructures (PKIs) chain, Certificate Authorities (CAs), intermediate CAs and other entities with a focus on cryptography and its standardization activities. The topic targets also other actors in PKI chain and entities that can provide use-case studies and real-world applications for deployment.

Submissions from consortia, despite not mandatory, is strongly advised.

Type of action and funding rate

Simple Grants — 50% funding rate

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 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-2025-DEPLOY-CYBER-08-NCC — Enhancing the NCC Network

Objectives

The National Coordination Centres (NCCs) set up by the Regulation (EU) 2021/887 are designed to work together through a network and to contribute to achieving the objectives of the regulation and to foster the Cybersecurity Competence Community in each Member State, by contributing to the acquisition of the necessary capacity. National Coordination Centres can also support priority areas such as the implementation of EU legislation (Directive (EU) 2022/2555, the proposed Cyber Resilience Act and the Cybersecurity Act).

The objective of this topic is to support the operation of the NCCs and to enable them to support the cybersecurity community, including SMEs, for the uptake and dissemination of state-of-the-art cybersecurity solutions and strengthen cybersecurity capacities. This could also be achieved by using Financial Support for Third Parties

(FSTPs)⁴. Based on the financing received in previous years and on the different operational start dates in the Member States, this activity aims to continue providing support for NCCs.

In this regard, it is important to stress that individual NCC can choose from the list of activities and deliverables included in this topic depending on their interest and mandate. There is no obligation for NCCs to execute all actions.

This topic also considers providing support for the uptake of EU cybersecurity technologies and products, commercialisation and scale-up of the European cybersecurity start-up/SME ecosystem, in collaboration and complementarity with the European and ongoing national and regional initiatives, such as accelerator and incubation programmes and technology transfer programmes. Such a strategy should also include support for scale-ups, considering the use of public procurement and private investment.

An essential aspect of this action is to create a framework for the emergence of such incubators and accelerators in the Member States, based on best practices and considering the specific needs and requirements arising from EU legislation (such as the Cyber Resilience Act, NIS 2 Directive).

In addition, this topic could contribute to cybersecurity awareness. It is becoming increasingly important to inform and educate EU citizens on cybersecurity topics in their daily use of digital technologies. Cybersecurity awareness helps individuals and organisations to identify threats and take appropriate action. By promoting awareness, the likelihood of incidents and data breaches can be reduced. Within this topic, NCCs are encouraged to build upon ongoing initiatives, including for example the ones from the EC and ENISA, to improve the awareness of EU citizens, businesses and organisations about cybersecurity risks and threats and to support Europe-wide actions to increase the number of students in cybersecurity courses, students engaged in cybersecurity research activities and students and young professionals choosing a career in cybersecurity.

Furthermore, European companies are innovative and develop highly competitive products, but the still underdeveloped Digital Single Market confines most of these companies (especially SMEs and start-ups) to their home country. A platform that can open the European market for small and medium-sized enterprises would also act as a springboard into international markets. This platform will ensure the competitiveness of European cybersecurity solutions. As such, this topic could also support the EU market's growth in cybersecurity products and services by providing a platform on which European SMEs and start-ups can post their (market-ready) products and solutions and on which businesses, public authorities and private individuals can search for the best solution for their needs, regardless of the country.

Scope

The National Coordination Centre should carry out, depending on their decision, one or more of the following tasks:

- acting as contact points at the national level for the Cybersecurity Competence Community to support the ECCC in achieving its objectives and missions.
- providing expertise and actively contributing to the strategic tasks of the ECCC, taking into account relevant national and regional challenges for cybersecurity in different sectors and deliver tasks supporting the implementation of the Cyber skills Academy.

⁴ For the use of FSTPs, the GB will prepare a dedicated procedure before the launch of the call.

- promoting, encouraging and facilitating the participation of civil society and industry, in particular start-ups and SMEs, academic and research communities and other actors at Member State level in cross-border projects and cybersecurity actions funded through all relevant Union programmes.
- providing technical assistance to stakeholders by supporting stakeholders in their application phase for projects managed by the ECCC, and in full compliance with the rules of sound financial management, especially on conflicts of interests. This should be done in close coordination with the relevant NCPs set up by the Member States.
- seeking to establish synergies with relevant activities at national, regional and local levels, such as addressing cybersecurity in national policies on research, development and innovation in the area of those policies stated in the national cybersecurity strategies. Where relevant, implementing specific actions for which grants have been awarded by the ECCC, including through the provision of financial support to third parties in accordance with Article 204 of the Financial Regulation under the conditions specified in the grant agreements concerned, in particular aimed at strengthening the uptake and dissemination of state-of-the-art cybersecurity solutions (notably by SMEs).
- supporting the scaling-up of start-ups by finding other funding to implement existing projects.
- promoting and disseminating the relevant outcomes of the work of the Network and the ECCC at national, regional or local level.
- assessing requests for becoming part of the Cybersecurity Competence Community by entities established in the same Member State as the NCC.
- advocating and promoting involvement by relevant entities in the activities arising from the ECCC, the Network of National Coordination Centres, and the Cybersecurity Competence Community, and monitoring, as appropriate, the level of engagement with actions awarded for cybersecurity research, developments and deployments.
- Supporting the Cybersecurity Competence Community registration (on platforms such as ATLAS) and contributing to the development of suitable community management tools.

In addition, this action aims to promote safer digital behaviours, grow talents and attract more youth to cybersecurity careers; the NCCs could also, depending on their national context, carry out one or more of the following tasks:

- Provide support to innovative ideas towards market-readiness.
- Promote cybersecurity awareness, best practices, and careers in schools, universities, and community events (for instance by launching a pan-European programme where young individuals will be trained as ambassadors to promote cybersecurity.)
- Strengthen collaboration between institutions for higher education, e.g. by jointly organising events, by teaching students and working together on cutting-edge research. Support activities in primary and secondary levels of education to increase cybersecurity awareness and hygiene, through educating the teachers and educators.
- Build stronger partnerships with established SMEs, tech companies, and government agencies to develop and distribute software tools and services that assist in early threat detection, actor identification, and threat evolution monitoring. These collaborations can ensure that cybersecurity professionals have access to the latest tools and technologies for effective threat management.
- In collaboration with other entities, as needed, organise periodic cybersecurity boot camps, challenges, awareness campaigns and training courses across Europe, specifically for SMEs or students (e.g. focusing on equipping participants with hands-on skills to manage prevalent cyber threats through training sessions, workshops, and simulation activities tailored to their

industry). Organise periodic awareness raising campaigns, at national and regional level, to increase cybersecurity awareness and hygiene aimed at different demographics. Organise national and regional cyber exercises to enhance the security and resilience of critical sectors as well as SMEs.

- Foster a community of cybersecurity professionals who can share their experiences, challenges, and solutions.
- Support and encourage the uptake of cybersecurity educational policy goals in national (cybersecurity) strategies.
- Promote safer digital behaviours and more youth considering cybersecurity careers.

The action could also aim to:

- Support the adoption of market-ready innovative cybersecurity solutions, including solutions developed in the framework of EU-supported research and innovation projects.
- Provide and deploy up to date tools and services to organisations (in particular SMEs) to prepare, protect (e.g. network security, advanced two-factor or passwordless authentication) and respond to cybersecurity threats.

This topic targets exclusively National Coordination Centres which have been recognised by the Commission as having the capacity to manage funds to achieve the mission and objectives laid down in the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. These actions aim at the operation of National Coordination Centres, which occupy a central role in the cybersecurity landscape as foreseen in Regulation (EU) 2021/887. Due to the synergetic role they play with regard to the activities at national, regional and local levels, such as addressing cybersecurity in national policies on research, development and innovation in the area of those policies stated in the national cybersecurity strategies, they must be able to handle sensitive information, and be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt undue foreign influence and control.

As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions are subject to Article 12(5) of the DEP Regulation (2021/694).

Expected Outcome

Depending on the decision of each NCC, one or more of the following should be covered:

- Network of national initiatives to accelerate the cybersecurity industry and facilitate Access-to-Market.
- European frameworks for establishing cybersecurity incubators and accelerators.
- Cybersecurity Community Observatory to inform subsequent policy interventions by the ECCC and NCCs.
- Matchmaking events to create connections and build trust; platforms and events for Access-to-Finance and Access-to-Market including in the area of dual-use technologies
- Strengthened Cybersecurity Community to support the European Cybersecurity Industrial, Technology and Research Competence Centre; Maintained technical registration possibilities for candidates for the Cybersecurity Competence Community; Technical assistance for potential applicants for ECCC calls.
- Uptake of cybersecurity solutions.
- Strengthened cybersecurity capacities of stakeholders.
- Synergetic activities that strengthen the role of NCC.

- Centralise the many initiatives focusing on raising awareness and work together with other NCCs to support a cross European approach covering education, studies, training courses and awareness campaigns⁵ ; Share and provide best practices related to the awareness topic.
- Support the transfer of best practices related to cybersecurity teaching for primary and secondary school and other activities for children and youngsters (including camps, materials, games, etc.).
- Support for teachers and professors to have access to best practices available in the EU and facilitate dialogue.
- Support the development of cross-over educational solutions for SMEs, for example by gamification.
- Cyber campaign material focused on young professionals and students of all ages and gender to pursue and advance in cybersecurity careers, where the NCCs can build on in view of regional differences.
- Cyber campaign material focused on parents and teachers of future students of all ages and gender to raise the number of cybersecurity students.
- Platform supporting a network of young cybersecurity ambassadors spreading awareness and fostering a culture of cybersecurity among Europe's youth.
- Common services to be provided within national cyber campuses.
- Hybrid events for the cybersecurity competence community to increase awareness of cybersecurity threats, threat actor modus operandi and potential impact, potentially in collaboration with existing initiatives and platforms.
- Deliverables supporting the implementation of the Cyber skills Academy.
- Support for activities dedicated to the EU Cybersecurity Challenges.

In addition, activities could cover setting up a platform integrating all other existing platforms, hosted and maintained at the European level under the .eu domain, so as to:

- Establish and maintain a marketplace for cybersecurity products and services.
- Allow the retrieval of information on entities adhering to the NCC communities.

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.

- Number of users and user communities getting access to EU cybersecurity facilities;
- Number of entities supported in strengthening preparedness for and response to major cybersecurity incidents;
- Number of registered candidates for the Cybersecurity Competence Community;
- Number of Matchmaking events organised and promotion of available funding opportunities;
- Number of events organised for the cybersecurity competence community to increase awareness of cybersecurity threats, threat actor modus operandi and potential impact, potentially in collaboration with existing initiatives and platforms;

⁵ The activities should consider other ongoing projects, activities, campaigns as well as the mandate of ENISA and other EU or national bodies. These actions should ensure synergies at EU level and should not duplicate efforts at EU or national levels.

- Number of interactions (requests of clarifications, questions or call/topic related questions, etc.) with the local Cybersecurity Competence Community for assistance to apply for funding opportunities;
- Number of entities benefitting from cascade financing;
- Number of actions to promote the expertise and achievements of the members of the cybersecurity community;
- Number of collaboration actions with other NCCs and with the ECCC.

Targeted stakeholders

This call targets National Coordination Centres which have been recognized by the Commission as having the capacity to manage funds to achieve the mission and objectives laid down in the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres and other private and other private and public entities in consortium with NCCs, including academia and research entities.

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 only (see *section 10*)
- For this topic, financial support to third parties is allowed (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-2025-DEPLOY-CYBER-08-CyberHEALTH — Dedicated action to reinforce hospitals and healthcare providers

Objectives

This action aims to strengthen the cybersecurity of hospitals and healthcare providers. The goal is to ensure that hospitals and healthcare providers, which are crucial operators in the health sector, can effectively detect, monitor, and respond to cyber threats, particularly ransomware, which pose significant risks, thereby enhancing the resilience of the European healthcare system.

The action will contribute to the EU action plan on cybersecurity in hospitals and healthcare, adopted by the Commission⁶ in January 2025.

Scope

This action addresses the growing need for continuous cybersecurity monitoring, threat intelligence, and incident response in hospitals and healthcare providers, which often lack dedicated cybersecurity resources to adequately protect themselves from cyber threats.

The action will support pilot projects, which will bring together stakeholders such as regional and/or national clusters associations⁷ of hospitals and healthcare providers (such as national healthcare systems, hospitals or associations of hospitals, healthcare providers and/or professional associations of healthcare practitioners), as well as cybersecurity service providers.

The pilot projects will define the state of preparedness of clusters of hospitals and healthcare providers in the European Union, to be able to assess their needs. Based on this analysis, they will prepare an overview of the state-of-the-art cybersecurity solutions and resources needed (technologies, services, tools, human resources, training needs, etc.) for hospitals and healthcare providers to meet the scope of the action. These may include, for example: Security Operation Centres offering real-time monitoring, threat detection, and rapid incident response, and advanced cybersecurity tools, such as Security Information and Event Management (SIEM) platforms, threat intelligence, and automated response capabilities, among others.

The pilots will develop technical plans, tailored to the needs of representative hospitals and healthcare providers (e.g. small or large hospitals, private healthcare providers, etc.) which will also need to include best implementation recommendations and cost estimates for effective deployment.

The pilot projects will conduct a demo implementation of these technical plans to demonstrate their effectiveness in operations at the stakeholders' sites, showcasing different use cases for different user groups at small, medium and large hospitals and healthcare providers, at least in two different Member States.

The pilot projects will serve as demonstration projects and will also provide cybersecurity education and training to the staff of their partner hospitals and healthcare providers, enhancing awareness and ensuring best practices in safeguarding sensitive healthcare information.

Finally, in cooperation with each other, the pilot projects will undertake wide dissemination activities of best practices across the EU, with the specific goal of helping replicate and scale up the pilots' activities as widely as possible.

The pilot projects will support healthcare institutions complying with the NIS 2 Directive.

Expected Outcome

- Mapping of common cybersecurity needs of hospitals and healthcare providers.
- Guidelines for healthcare providers to assess their current state of cybersecurity protection and relevant needs.

⁶ https://commission.europa.eu/cybersecurity-healthcare_en.

⁷ 'Cluster associations' refers to any legally established group of hospitals and healthcare providers, such as regions and professional associations established in one or more Member States.

- Technical cybersecurity plans to enhance preparedness and cyber resilience: improved detection and response capabilities for healthcare institutions minimising the impact of cyberattacks, particularly for ransomware. This also includes dedicated training courses to staff.
- Pilot cybersecurity demo installations at partner hospitals and healthcare provider sites to ensure hospitals and healthcare providers can maintain operational continuity in the face of cybersecurity incidents. This should be monitored through specific KPIs.
- Wide dissemination campaigns to help scale up preparedness of hospitals and healthcare providers in Europe.

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.

- Number of cybersecurity and/or tools deployed;
- Number of users and user communities getting access to the tools deployed;
- Number of entities supported in strengthening preparedness for and response to major cybersecurity incidents;
- Number of tools, methods, organisational and management practices dedicated to detection and response capabilities for minimising the impact of cyberattacks, adopted in healthcare and health institutions, and in particular small and medium-size entities;
- Number of cybersecurity dedicated training courses to healthcare institutions staff.
- Number of pilot cybersecurity demo installations at partner hospitals and healthcare provider sites.
- Number of people reached by dissemination campaigns;

Targeted stakeholders

This topic targets in particular stakeholders such as regional and/or national clusters associations of hospitals and healthcare providers (such as national healthcare systems, hospitals or associations of hospitals, healthcare providers and/or professional associations of healthcare practitioners), as well as cybersecurity service providers.

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*)
- For this topic, multi-beneficiary applications are mandatory and specific conditions for the consortium composition apply (see *section 6*)

- 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 55 000 000**.

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

Topic	Topic budget
DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PUBLICPQC	EUR 15.000.000
DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC	EUR 10.000.000
DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH	EUR 30.000.000

The availability of the call budget still depends on the final adoption of the 2025-2027 Work Programme amendment.

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:	12/06/2025
<u>Deadline for submission:</u>	<u>07 October 2025 – 17:00:00 CET</u> <u>(Brussels)</u>
Evaluation:	November - December 2025
Information on evaluation results:	January - February 2026
GA signature:	June - July 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: 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**

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

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 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 note however that all topics of this call are subject to restrictions due to security reasons, therefore entities must not be directly or indirectly controlled from a country that is not an eligible country. **All entities⁸ 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*)
- the Grant Agreement may provide for IPR restrictions (*see section 10*).

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

⁸ Except for entities that are validated as public bodies by the Central Validation Service.

for the protection of the EU financial interests equivalent to that offered by legal persons⁹.

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'¹⁰. ⚠ 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)¹¹. 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 2020/2092¹². 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 for 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

Proposals must be submitted by:

for topics DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PUBLICPQC and DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC:

- n/a

for topic DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH:

- minimum 2 independent applicants (beneficiaries; not affiliated entities) from at least 2 eligible countries;

⁹ See Article 200(2)(c) EU Financial Regulation [2024/2509](#).

¹⁰ For the definitions, see Articles 190(2) and 200(2)(c) EU Financial Regulation [2024/2509](#).

¹¹ 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](#).

¹² 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 allowed in topics DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC for grants under the following conditions:

- the calls must be open, published widely and conform to EU standards concerning transparency, equal treatment, conflict of interest and confidentiality
- the calls must be published on the Funding & Tenders Portal, and on the participants' websites
- the calls must remain open for at least two months
- if call deadlines are changed this must immediately be published on the Portal and all registered applicants must be informed of the change
- the outcome of the call must be published on the participants' websites, including a description of the selected projects, award dates, project durations, and final recipient legal names and countries
- the calls must have a clear European dimension.

For topics DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PUBLICPQC and DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH, 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](#)¹³ 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*).

¹³ 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).

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.

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 participate¹⁴:

- 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 misconduct¹⁵ (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)

¹⁴ See Articles 138 and 143 of EU Financial Regulation [2024/2509](#).

¹⁵ '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 resisted¹⁶ 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 that¹⁷:

- 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).

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.

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.

¹⁶ '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.

¹⁷ See Article 143 EU Financial Regulation [2024/2509](#).

 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 topics DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PublicPQC the indicative duration of the action is indicatively 36 months, other durations, that are properly justified, are not excluded.
- for topics DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC the indicative duration of the action is indicatively 36 or 48 months, other durations, that are properly justified, are not excluded.
- for topics DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH the indicative duration of the action is indicatively 18 or 24 months, other durations, that are properly justified, are not excluded.

Extensions are possible, if duly justified and through an amendment.

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;
- additional deliverables (yearly) on achievement of relevant KPIs and project outputs.

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 topics DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PublicPQC: indicatively between 3 and 4 million EUR per project but other amounts, if duly justified, are not excluded.
- for topics DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC: indicatively between 2 and 3 million EUR per project but other amounts, if duly justified, are not excluded.
- for topics DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH: indicatively between 3 and 5 million EUR per project but other amounts, if duly justified, 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 (for topic DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC)
 - 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)¹⁸: Yes
 - SME owner/natural person unit cost¹⁹: Yes
- travel and subsistence unit costs²⁰: No (only actual costs)
- travel costs: eligible only in EU and EEA countries
- equipment costs:
 - depreciation (for topic DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC)
 - depreciation + full cost for listed equipment (for topics DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PublicPQC and DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH)
- other cost categories:
 - costs for financial support to third parties allowed for grants:
 - for topic DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC: maximum amount per third party EUR 100 000; amounts of more than 60 000 EUR per third party are necessary because the nature of the actions under this call is such that their objectives would otherwise be impossible or overly difficult to achieve;
 - internally invoiced goods and services (unit cost according to usual cost accounting practices)²¹: Yes
- indirect cost flat-rate: 7% of the eligible direct costs (categories A-D, except volunteers costs and exempted specific cost categories, if any).
- 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:

¹⁸ [Decision](#) of 29 June 2021 authorising the use of unit costs based on usual cost accounting practices for actions under the Digital Europe Programme.

¹⁹ 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).

²⁰ 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).

²¹ [Decision](#) of 29 June 2021 authorising the use of unit costs based on usual cost accounting practices for actions under the Digital Europe Programme.

- 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 Bucharest 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: 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 multi-beneficiary consortium.

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 EULogin 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) at 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 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)²².

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, participants²³ 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 DEP, HE, EDF and CEF-DIG restricted calls](#)).

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:

²² See Article 12(5) and (6) of the Digital Europe Regulation [2021/694](#).

²³ 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 reasons²⁴.

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 DEP, HE, EDF and CEF-DIG restricted calls](#).

²⁴ See Article 18(4) of the Digital Europe Regulation [2021/694](#).