



DIGITAL Europe Programme – Cybersecurity

Francesco Barbato
Wide Hogenhout

DG CNECT H1 – Cybersecurity Technologies and Capacity Building

[#DigitalEuropeProgramme](https://twitter.com/DigitalEuropeProgramme)



EU Cybersecurity Competence Centre and Network



European Competence Centre

- Funds manager for cybersecurity in Digital Europe and Horizon Europe 2021-2027
- Facilitate the Network and Community to drive the cybersecurity technology agenda
- Support joint investment by the EU, Member States and industry



Network of National Coordination Centres

- Member States contact point
- Objective: national capacity building and link with existing initiatives
- National Coordination Centres may receive and pass financial support



Community

- A large, open, and diverse group of cybersecurity stakeholders (research, private and public sectors, both civilian and defence)





Network of National Coordination Centres

One NCC per Member State

May receive/pass EU funding

Promotes participation in cross-border projects and in cybersecurity action

National capacity building and link with existing initiatives

Coordinates the national, regional and local levels

Promotes cybersecurity educational programmes

Advocates involvement of relevant entities



Competence Community



A large, open, and diverse group of cybersecurity stakeholders



Exchanges with the ECCC/NCCs on developments in cybersecurity



Provides input to the activities of the ECCC/NCCs



DIGITAL Europe Programme

Deployment of technology to businesses and citizens.

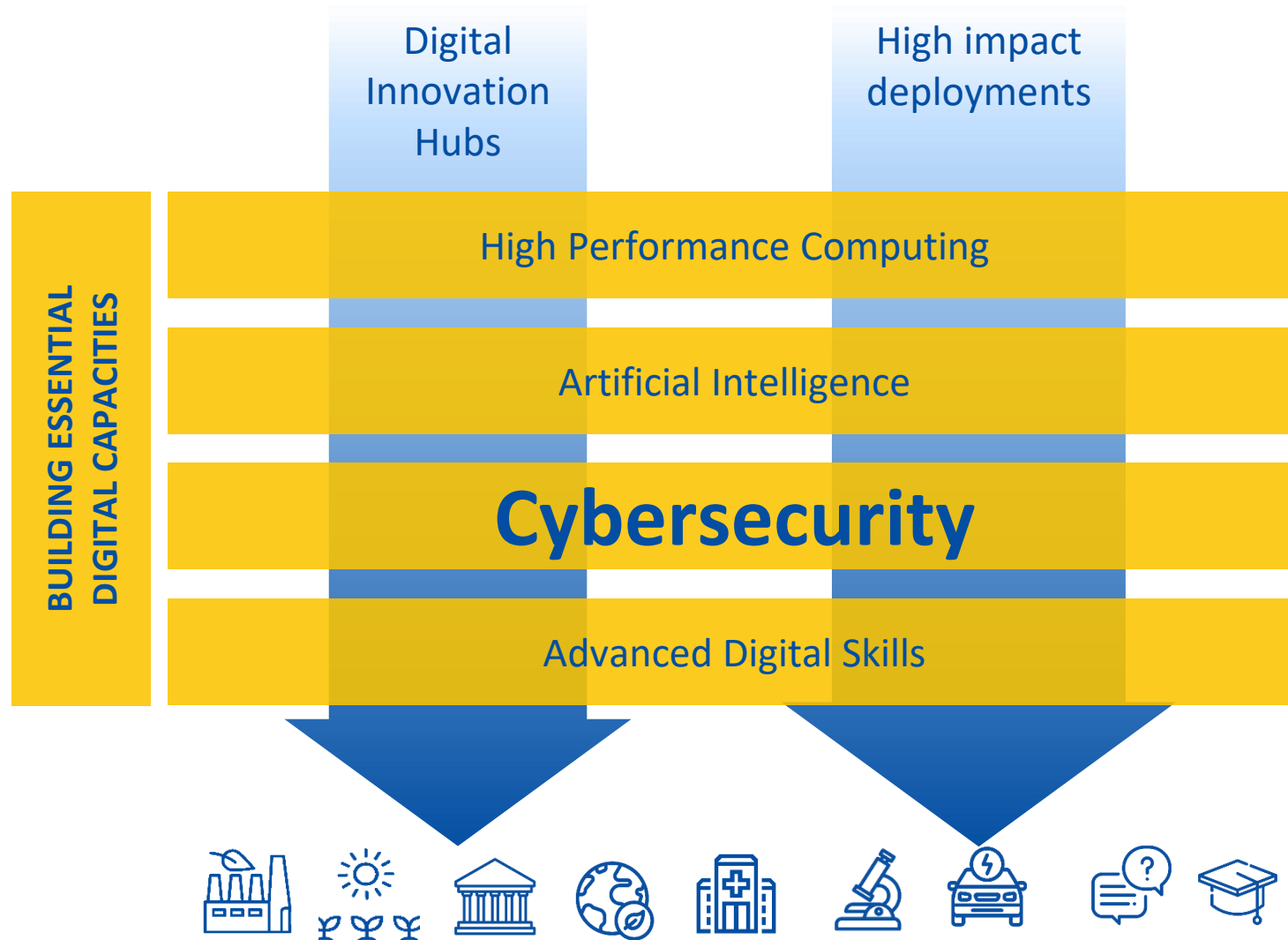
Speed up economic recovery and digital transformation of European economy and society.

Complementary to other EU programmes, e.g., Horizon Europe

Strategic financing for five crucial areas



Digital Europe Programme - Structure





Digital Europe Programme – Open Calls

Submission
deadline
6/07/2023

DIGITAL-ECCC-2022-CYBER-B-03-CYBER-RESILIENCE
DIGITAL-ECCC-2022-CYBER-B-03-SOC
DIGITAL-ECCC-2022-CYBER-B-03-UPTAKE-CYBERSOLUTIONS

Submission
deadline
26/09/2023

DIGITAL-ECCC-2023-DEPLOY-CYBER-04-SUPPORT-ASSIST
DIGITAL-ECCC-2023-DEPLOY-CYBER-04-CIVIL-DEFENCE
DIGITAL-ECCC-2023-DEPLOY-CYBER-04-STANDARDISATION
DIGITAL-ECCC-2023-DEPLOY-CYBER-04-EULEGISLATION



Digital Europe Programme

**DIGITAL-ECCC-2023-DEPLOY-
CYBER-04**



Digital Europe: 2023 topics and deadlines

Topic	Budge	Opening	Deadline
DIGITAL-ECCC-2023-DEPLOY-CYBER-04-SUPPORT-ASSIST <i>Preparedness Support and Mutual Assistance</i>	€ 35M	25/05/23	26/09/23
DIGITAL-ECCC-2023-DEPLOY-CYBER-04-CIVIL-DEFENCE <i>Coordination Between the Cybersecurity Civilian and Defence Spheres</i>	€ 3M		
DIGITAL-ECCC-2023-DEPLOY-CYBER-04-STANDARDISATION <i>Standardisation in the Area of Cybersecurity</i>	€ 3M		
DIGITAL-ECCC-2023-DEPLOY-CYBER-04-EULEGISLATION <i>Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies</i>	€ 30M		



Preparedness Support and Mutual Assistance (I)

Objectives

- Increase the level of protection and resilience to cyber threats, by assisting Member States in their efforts to improve the preparedness for cyber threats and incidents by providing them with knowledge and expertise.

Scope

- Support for testing of essential entities operating critical infrastructure for potential vulnerabilities
- Support for threat assessment and risk assessment.
- Risk monitoring service

*Proposals must implement a mechanism for **financial support to third parties**. Proposals that do not foresee this will be ineligible.*



Preparedness Support and Mutual Assistance (II)

Outcomes and deliverables

- Preparedness support services
- Threat assessment and risk assessment services
- Risk monitoring services
- Mutual assistance among Member States

KPIs to measure outcomes and deliverables

- Number of penetration tests provided
- Number of essential entities supported
- Number of threat assessments / risk scenario analyses carried out
- Number of risk monitoring services provided
- Number of potential number of users covered per test/exercise
- Number and nature of vulnerabilities discovered
- Number of cross-border actions/exercises



Preparedness Support and Mutual Assistance (III)

Targeted stakeholders

This topic targets in particular:

- National cybersecurity authorities,
- National cybersecurity competence centres,
- National Coordination Centres (as defined in Regulation (EU) 2021/887),
- Private entities and any other relevant stakeholders with the capacity to aggregate demand from end beneficiaries,

to launch tenders for procurement in the cybersecurity market space and to run downstream calls for allocating Financial Support to Third Parties.

Grants for Financial Support — 100% funding rate, EUR 35M, duration up to 48 months, indicative budget: EUR 3-7M per project

Multi-country consortia composition is not mandatory for this topic but will positively contribute to the impact of the action.



Standardisation in the Area of Cybersecurity (I)

Objective

- Support further standardisation in the area of cybersecurity, notably in view of the implementation of the proposed Regulation on the Cyber Resilience Act (CRA) , in particular with a view to improving the awareness and engage stakeholders in such standardisation work.

Scope

- Ensure wide stakeholder participation in standardisation activities in the area of cybersecurity, and in particular in relation to development of harmonized standards facilitating the implementation of the Cyber Resilience Act. This can be in the form of meetings, workshops and collaborative activities, involving the private as well as the public sector.



Standardisation in the Area of Cybersecurity (II)

Outcomes and deliverables

- Organization of events, workshops, stakeholder consultations, and production of white papers, all fostering the development of harmonised standards and conformity with requirements stemming from above mentioned legislative framework.
- Support for participation of relevant European experts in European and international cybersecurity standardisation fora.

KPIs to measure outcomes and deliverables

- Number of standardisation work items directly relevant for the development of harmonised standards for CRA presented in white papers, reporting on substantive discussions, options considered, conclusions taken and their relevance to the policy objectives.
- Number of experts participating in cybersecurity standardisation activities that are directly relevant for the development of harmonised standards for CRA.
- Number of standardisation activities in the area of cybersecurity that are directly relevant for the development of harmonised standards for CRA.
- Number of SMEs and start-ups participating in cybersecurity standardisation activities that are directly relevant for the development of harmonised standards for CRA.
- Number of cybersecurity standardisation workshops/trainings/events organised, as well as the number of attendees per each of them.
- Number of active collaborations implemented with other relevant initiatives or European players.
- Number of open access guidance material produced aiming to support the implementation of standards developed for the CRA and to support conformity with the requirements of the CRA
- Number of open access educational/audio-visual material produced aiming to support the implementation of standards developed for the CRA and to support conformity with the requirements of the CRA.



Standardisation in the Area of Cybersecurity (III)

Targeted stakeholders

This topic targets:

- Cybersecurity standardisation stakeholders (notably European standardisation bodies and conformity assessment bodies)
- Industrial players, including SMEs and start-ups
- and relevant actors that play a role in the European standardisation process and in the implementation of the Cyber Resilience Act and Cybersecurity Act.

Coordination and Support Actions — 100% funding rate, EUR 3M, 36mos, Indicative budget: up to EUR 3M per project

Multi-country consortia composition is not mandatory for this topic but will positively contribute to the impact of the action.



Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (I)

Objectives

- Proposals should contribute to achieving at least one of these objectives:
 - Development of trust and confidence between Member States.
 - Effective operational cooperation of organisations entrusted with EU or Member State's national level cybersecurity, in particular cooperation of CSIRTs (including in relation to the CSIRT Network) or cooperation of Operators of Essential Services including public authorities.
 - Better security and notification processes and means for Operators of Essential Services and for digital service providers in the EU.
 - Better reporting of cyber-attacks to law enforcement authorities in line with the Directive on attacks against information systems.
 - Improved security of network and information systems in the EU.
 - More alignment of Member States' implementations of NIS2 (Directive (EU) 2022/2555).
 - Support cybersecurity certification in line with the Cybersecurity Act.



Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (II)

Scope

The action will focus on the support of at least one of the following priorities:

- Implementation, validation, piloting and deployment of technologies, tools and IT-based solutions, processes and methods for monitoring and handling cybersecurity incidents.
- Collaboration, communication, awareness-raising activities, knowledge exchange and training, including through the use of cybersecurity ranges, of public and private organisations working on the implementation of NIS2 (Directive (EU) 2022/2555).
- Twinning schemes involving originator and adopter organisations from at least 2 different Member States to facilitate the deployment and uptake of technologies, tools, processes and methods for effective cross-border collaboration preventing, detecting and countering Cybersecurity incidents.
- Robustness and resilience building measures in the cybersecurity area that strengthen suppliers' ability to work systematically with cybersecurity relevant information or supplying actionable data to CSIRTs.
- Ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle.
- Ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers.
- Enhance the transparency of security properties of products with digital elements.
- Enable businesses across all sectors and consumers to use products with digital elements securely.
- Support to Cybersecurity certification, including support to national cyber authorities and other relevant stakeholders, such as SMEs.



Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (III)

Outcomes and deliverables

- Incident management solutions reducing the overall costs of cybersecurity for individual Member States and for the EU as a whole.
- Better compliance with NIS2 (Directive (EU) 2022/2555) and higher levels of situational awareness and crisis response in Member States.
- Organization of events, workshops, stakeholder consultations and white papers.
- Enhanced cooperation, preparedness and cybersecurity resilience in the EU.
- Support actions in the area of certification.

KPIs to measure outcomes and deliverables

- Number of technologies and IT-based solutions, processes and methods for handling cybersecurity incidents implemented, validated, piloted or deployed.
- Number of activities organised for collaboration, communication, awareness-raising or knowledge exchange and training (on the implementation of the NIS2 Directive).
- Number of twinning schemes implemented between at least two Member States for effective cross-border collaboration preventing, detecting and countering cybersecurity incidents.
- Number of tools and IT-based solutions, processes and methods for monitoring and handling exploited vulnerabilities in products with digital elements in the scope of the CRA.
- Number of products or services available that simplify and/or automate CRA compliance.
- Number of SMEs using open access or low-cost tools to support the implementation of the CRA for public authorities and economic operators.
- Number of tools to support market surveillance authorities and notifying authorities appointed under the CRA in the implementation of their respective mandates.
- Number of communication, awareness-raising events, knowledge exchange and training activities about the rules of the CRA.
- Number of activities organised to promote sharing of technical specifications, best practices and use-cases amongst actors that have obligations under the CRA.
- Uptake of CRA compliant products across sectors.



Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (IV)

Targeted stakeholders

This topic targets:

- Industrial stakeholders, including SMEs and start-ups in the scope of the upcoming CRA, concerned by the NIS2 Directive or that may benefit from the European cybersecurity certification schemes;
- Member State competent authorities, which play a central role in the implementation of the NIS2 Directive;
- Computer Security Incident Response Teams (CSIRTs), including sectorial CSIRTs;
- Security Operation Centres (SOC),
- Operators of Essential Services (OES);
- Digital service providers (DSP);
- Information Sharing and Analysis Centres- ISACs;
- Actors that play a role in the implementation of the Cyber Resilience Act (including certification bodies), and any other actors within the scope of the legislations mentioned above.

Simple Grants — 50% funding rate, EUR 30M, 36mos, Indicative budget: EUR 1-5M per project

Multi-country consortia composition is not mandatory for this topic but will positively contribute to the impact of the action.



Coordination Between the Cybersecurity Civilian and Defence Spheres (I)

Objective

- Enhance exchange and coordination between the cybersecurity civilian and defence spheres. This should in particular foster synergies between cybersecurity actions in Horizon Europe, Digital Europe and defence related actions carried out by the Union through its bodies and programmes, such as the European Defence Agency and the European Defence Fund.

Scope

- Organise activities that bring foster exchange with regards to cybersecurity technologies that have relevance in both civilian and defence context: meetings, workshops and collaborative activities between stakeholders of the civil and defence communities, addressing all stakeholders (academic, SMEs, industry, public authorities, etc.).



Coordination Between the Cybersecurity Civilian and Defence Spheres (II)

Outcomes and deliverables

- Concrete activities such as discussions, meetings, white papers, workshops, which strengthen the links between the cybersecurity civilian and defence spheres.
- Synergies between these communities, such as common activities to exchange know-how and information.

KPIs to measure outcomes and deliverables

- Number of cybersecurity workshops/trainings/events organised, as well as the number of participants per each of them; Number of stakeholders from both communities involved in organised activities
- Number of common activities involving both communities
- Number of Industrial stakeholders, including large enterprises, SMEs and start-ups participating in cybersecurity activities that are directly relevant for the defence and civilian sector.
- Number of active collaborations implemented with other relevant initiatives or European players.
- White papers produced aiming to support the implementation of better cooperation between the two communities.



Coordination Between the Cybersecurity Civilian and Defence Spheres (III)

Targeted stakeholders

Stakeholders in either Cybersecurity Civilian and Defence Sphere, aiming at fostering links across communities.

Such as:

- Industrial players
- Defence Ministries and Agencies
- SMEs and start-ups
- and relevant actors that play a role in the European Cybersecurity Civilian and Defence Spheres.

Coordination and Support Actions — 100% funding rate, EUR 3M, duration up to 24 months, indicative budget: up to EUR 3M per project

Multi-country consortia composition is not mandatory for this topic but will positively contribute to the impact of the action.



Call document - Support to proposers

- Details on **admissibility and eligibility**
- Information for applicants on **financial and operational capacity**
- Exclusion criteria
- **Evaluation procedure**
- Guarantees, obligatory milestones and deliverables, certificates and any many other description on legal conditions to participate in grants
- Financial support to third party schemes and conditions
- All the **mandatory annexes** needed for the call (e.g. ethic issues, security issues)
- **Type of action** description
- Other important legal and operational provisions
- **Help for applicants** and how to reach out to the commission



Award criteria: 1. Relevance




- Alignment with the **objectives and activities**
- Contribution to **long-term policy and strategic objectives**
- Reinforcement of the Union's **digital technology supply chain***

** applicable only for topics **Standardisation in the Area of Cybersecurity** and **Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies***



Award criteria: 2. Implementation

- 
- **Maturity** of the proposed action
 - Soundness and efficiency of the **implementation plan**
 - Capacity of the **applicants or consortium** to carry out the proposed work



Award criteria: 3. Impact



- Achievement of the **expected outcomes and deliverables**, as well as communication and dissemination
- Competitiveness strengthen and **contribution to society**



Lessons learnt from previous DEP Calls

- Pay more attention to the Work Programme and call document text;
- Multiple layers of checks needed (many clerical errors in proposals);
- Contact your NCCs/NPCs for help and clarifications

- Common mistakes from proposers:
 - Inadequate level of understanding of the Call requirements
 - Tangible KPIs and metrics were missing from proposals
 - The work-plan (deliverables, milestones, critical risks) was insufficiently elaborated.




Budget categories and cost eligibility

- A. Personnel costs
 - A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons and 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. Financial Support to Third Parties (if applicable to the Topic)



Funding & tender portal



Funding & tender opportunities

Single Electronic Data Interchange Area (SEDIA)

español ES
[Register](#) | [Login](#)

SEARCH FUNDING & TENDERS
HOW TO PARTICIPATE
PROJECTS & RESULTS
WORK AS AN EXPERT
SUPPORT

Digital Europe Programme (DIGITAL)

clear filter

Digital Europe Programme

Digital Europe Programme is the first EU programme that aims to accelerate the recovery and drive the digital transformation of Europe.

Worth €7.6 billion (in current prices), the Programme is a part of the next long-term EU budget, (the Multiannual Financial Framework), and it covers 2021 to 2027. It will provide funding for projects in five crucial areas: supercomputing, artificial intelligence, cybersecurity, advanced digital skills, and ensuring the wide use of digital technologies across the economy and society.

The Programme is fine-tuned to fill the gap between the research of digital technologies and their deployment, and to bring the results of research to the market - for the benefit of Europe's citizens and businesses, and in particular SMEs. Investments under the Digital Europe programme supports the Union's twin objectives of a green transition and digital transformation and strengthens the Union's resilience and strategic autonomy.

- Find calls for proposals
- Projects & Results
- Priorities
- What's new?

Find calls for proposals in Digital Europe Programme


View (47)

🚫 **Calls for Tenders** are not available when you have selected a programme. [See all calls for tenders published by EC](#)

Projects & Results

See the work done in past and ongoing projects. View the statistics on proposals, success rates, funded projects and participants.

[Check dashboard](#)



Funding & tender opportunities

Single Electronic Data Interchange Area (SEDIA)

español ES
[Register](#) | [Login](#)

SEARCH FUNDING & TENDERS
HOW TO PARTICIPATE
PROJECTS & RESULTS
WORK AS AN EXPERT
SUPPORT

Find calls for proposals and tenders

Search

EU Programmes

Asylum, Migration and Integration Fund (AMIF)	Border Management and Visa Instrument (BMVI)	Customs Control Instrument (CCEI)	Connecting Europe Facility (CEF)	Citizens, Equality, Rights and Values Programme (CERV)	Creative Europe (CREA)
Outropa Programme (CUST)	Digital Europe Programme (DIGITAL)	Europe Direct (ED)	European Defence Fund (EDF)	European Parliament (EP)	EU Anti-fraud Programme (ELAF)
European Solidarity Corps (ESC)	Erasmus+ Programme (ERASMUS)	EU4Health Programme (EU4H)	European Social Fund + (ESF)	European Maritime, Fisheries and Aquaculture Fund (EMFAF)	Eurostars Research and Training Programme (EURATOM)
Fiscalis Programme (FISCI)	Innovation Fund (INNOV-FUND)	Internal Security Fund (ISF)	Horizon Europe (HORIZON)	Single Market Programme (SMP)	Social Prerogative and Specific Competences Lines (SOCPCL)
EU External Action (RELEX)	Interregional Innovation Investments (I3)	Justice Programme (JUST)	Protection of the Euro against Counterfeiting Programme (PERICLES)	Pilot Projects and Preparatory Actions (PPA)	Programme for the Environment and Climate Action (LIFE)
Promotion of Agricultural Products (AGRI-P)	Research Fund for Coal & Steel (RFCS)	Union Civil Protection Mechanism (UCPM)	Information Measures for the EU Cohesion policy (IMREC)		

[show all](#)

News

25 Feb, 2022
Research Fund for Coal and Steel (RFCS) - Call for experts!
The Research Fund for Coal and Steel is looking for expert evaluators. A call for experts for RFCS has been published on the RFCS website. **IMPORTANT!** interested...

23 Feb, 2022
Important Communication to Implementing Partners on Logframe encoding in OPSYS - 22/02/2022
Dear Implementing Partners, Communicating on and learning from results is an important dimension of our external action. The European Commission's results campa...

11 Feb, 2022
Have you heard about the Horizon Impact Award?
HBP beneficiaries - have you considered applying for the Horizon Impact Award? It's the European Commission's initiative to celebrate outstanding research prog...

[All news >](#)

How to participate in 5 steps

- 1 Find an opportunity
- 2 Find partner(s)
- 3 Create an account
- 4 Register your organisation
- 5 Submit your proposal or offer

[Learn more](#)

What are calls for proposals?

With calls for proposals the Commission selects, on a competitive basis, organisations or natural persons to implement projects co-financed by EU because these projects contribute to EU policy aims.

In a nutshell:

- Advance payments allowed
- Reimbursement for real costs
- Deliverable is a report or completion of project

[See all calls for proposals >](#)

What are calls for tenders?

With calls for tenders the Commission aims to purchase goods, services or works in exchange for payment of an agreed price.

In a nutshell:

- Payment to agreed conditions and price
- Delivery of goods, services or works in compliance with predefined requirements
- Execution according to contractual conditions.

[Read more](#) [See all calls for tenders >](#)

© 2018 European Commission | [About](#) | [Free text search](#) | [IT Helpdesk](#) | [Cookies](#) | [Legal Notice](#) | [APIs](#)

<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital>

29



Useful links

Digital Europe Programme website

<https://digital-strategy.ec.europa.eu/en/activities/digital-programme>

Digital Europe Programme Regulation

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0694&qid=1621344635377>

Funding & tender opportunities portal

<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital>



Horizon Europe

HORIZON-CL3-2023-CS-01



HORIZON-CL3-2023-CS-01	<i>Budget</i>	<i>Opening</i>	<i>Closing</i>
<i>Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)</i>	28 M EUR	29/06/2023	23/11/2023
<i>Privacy-preserving and identity technologies</i>	15.7 M EUR		
<i>Security of robust AI systems</i>	15 M EUR		



Funding & tender portal

Funding & tender opportunities

Single Electronic Data Interchange Area (SEDIA)

español ES
[Register](#) | [Login](#)

SEARCH FUNDING & TENDERS
HOW TO PARTICIPATE
PROJECTS & RESULTS
WORK AS AN EXPERT
SUPPORT

Digital Europe Programme (DIGITAL)

clear filter

Digital Europe Programme

Digital Europe Programme is the first EU programme that aims to accelerate the recovery and drive the digital transformation of Europe.

Worth €7.6 billion (in current prices), the Programme is a part of the next long-term EU budget, (the Multiannual Financial Framework), and it covers 2021 to 2027. It will provide funding for projects in five crucial areas: supercomputing, artificial intelligence, cybersecurity, advanced digital skills, and ensuring the wide use of digital technologies across the economy and society.

The Programme is fine-tuned to fill the gap between the research of digital technologies and their deployment, and to bring the results of research to the market - for the benefit of Europe's citizens and businesses, and in particular SMEs. Investments under the Digital Europe programme supports the Union's twin objectives of a green transition and digital transformation and strengthens the Union's resilience and strategic autonomy.

- Find calls for proposals
- Projects & Results
- Priorities
- What's new?

Find calls for proposals in Digital Europe Programme

View (47)

▲ **Calls for Tenders** are not available when you have selected a programme. See all calls for tenders published by EC

Projects & Results

See the work done in past and ongoing projects. View the statistics on proposals, success rates, funded projects and participants.

[Check dashboard](#)

<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital>

Funding & tender opportunities

Single Electronic Data Interchange Area (SEDIA)

español ES
[Register](#) | [Login](#)

SEARCH FUNDING & TENDERS
HOW TO PARTICIPATE
PROJECTS & RESULTS
WORK AS AN EXPERT
SUPPORT

Find calls for proposals and tenders

clear filter

EU Programmes

Asylum, Migration and Integration Fund (AMIF)	Border Management and Visa Instrument (BMVI)	Customs Control Instrument (CCI)	Connecting Europe Facility (CEF)	Citizens, Equality, Rights and Values Programme (CERV)	Creative Europe (CREATIVE)
Customs Programme (CUP)	Digital Europe Programme (DIGITAL)	Europe Direct (ED)	European Defence Fund (EDF)	European Parliament (EP)	EU Anti-Fraud Programme (EUFRA)
European Solidarity Corps (ESC)	Erasmus+ Programme (ERASMUS)	EU4Health Programme (EU4H)	European Social Fund + (ESF)	European Maritime and Fisheries Fund (EMFF)	Erasmus Research and Training Programme (ERATRAC)
Fiscals Programme (FPIC)	Innovation Fund (INNOV-FUND)	Internal Security Fund (ISF)	Horizon Europe (HORIZON)	Single Market Programme (SMP)	Social Perspectives and Specific Competitiveness Lines (SOCP)
EU External Action (EUA)	Interregional Innovation Investments (I3)	Justice Programme (JUST)	Promotion of the Euro against Counterfeiting Programme (PROMOTEC)	Flag Projects and Proprietary Actions Programme (FPAP)	Programme for the Environment and Climate Action (PECA)
Promotion of Agricultural Products (PAP)	Research Fund for Coal and Steel (RFCS)	Union Civil Protection Mechanism (UCPM)	Information Measures for the EU Green Deal (IM-GD)		

News

23 Feb. 2022
Research Fund for Coal and Steel (RFCS) - Call for experts!

The research fund for Coal and Steel is looking for expert evaluators. A call for experts for RFCS has been published on the RFCS website. [More info](#)

23 Feb. 2022
Important Communication to Implementing Partners on Logframe encoding in QPDS - 22/02/2022

Dear Implementing Partners, Communicating on and learning from results is an important dimension of our external action. The European Commission's results centre...

11 Feb. 2022
Have you heard about the Horizon Impact Award?

HIP beneficiaries - have you considered applying for the Horizon Impact Award? It's the European Commission's initiative to celebrate outstanding research projects...

[All news](#)

How to participate in 5 steps

- 1 Find an opportunity
- 2 Find partner(s)
- 3 Create an account
- 4 Register your organisation
- 5 Submit your proposal or offer

Learn how to find and apply for suitable EU funding and tender opportunities.

[Learn more](#)

What are calls for proposals?

With calls for proposals the Commission selects, on a competitive basis, organisations or natural persons to implement projects co-financed by EU because these projects contribute to EU policy aims.

In a nutshell

- Advance payments allowed
- Reimbursement for real costs
- Defensible in a court or arbitration of project

[See all calls for proposals](#)

What are calls for tenders?

With calls for tenders the Commission aims to purchase goods, services or works in exchange for payment of an agreed price.

In a nutshell

- Payment to agreed conditions and price
- Delivery of goods, services or works in compliance with specified requirements
- Execution according to contractual conditions.

[See all calls for tenders](#)

© 2018 European Commission | [About](#) | [Free text search](#) | [IT Helpdesk](#) | [Cookies](#) | [Legal Notice](#) | [APIs](#)



Thank you



CNECT-H1-DIGITAL@ec.europa.eu

#DigitalEuropeProgramme