



Digital Europe Programme (DIGITAL)

Call for proposals

Digital transformation (DIGITAL-2021-TRUST-01)

Version 1.0 17 November 2021

HISTORY OF CHANGES						
Version	Publication Date	Change	Page			
1.0	17.11.2021	Initial version (new MFF).				
		•				
		•				
		•				



EUROPEAN HEALTH AND DIGITAL EXECUTIVE AGENCY (HaDEA)

HaDEA.B - Digital, Industry and Space HaDEA.B.2.01 – Digital Europe

CALL FOR PROPOSALS

TABLE OF CONTENTS

0.	Introduction	5
1.	Background	б
2.	Objectives — Scope — Outcomes and deliverables — KPIs to measure outcomes and deliverables — Targeted stakeholders — Type of action — specific topic conditions	8
	DIGITAL-2021-TRUST-01-EDMO — European Digital Media Observatory (EDMO) - national and multinational hubs	8
	Objectives	8
	Scope	8
	Outcomes and deliverables	9
	Targeted stakeholders	10
	Type of action	11
	Specific topic conditions	12
	DIGITAL-2021-TRUST-01-SAFERINTERNET — Safer Internet Centres (SICs)	12
	Objectives	12
	Scope	12
	Outcomes and deliverables	15
	KPIs to measure outcomes and deliverables	16
	Targeted stakeholders	16
	Type of action	16
	Specific topic conditions	17
	DIGITAL-2021-TRUST-01-ECODEX — e-Justice Communication via Online Data Exchange (e-CODEX)	17
	Objectives	17
	Scope	17
	Outcomes and deliverables	20
	KPIs to measure outcomes and deliverables	20
	Targeted stakeholders	21
	Type of action	21
	Specific topic conditions	21
	DIGITAL-2021-TRUST-01-DIGIPASS — Digital Product Passport: sustainable and circular systems	21
	Objectives	21
	Scope	22
	Outcomes and deliverables	23
	KPIs to measure outcomes and deliverables	23

Targeted stakeholders	23
Type of action	24
Specific topic conditions	24
3. Available budget	24
4. Timetable and deadlines	25
5. Admissibility and documents	25
6. Eligibility	26
Eligible participants (eligible countries)	26
Specific cases	26
Consortium composition	27
Eligible activities	28
Ethics	28
Security	28
7. Financial and operational capacity and exclusion	29
Financial capacity	29
Operational capacity	30
Exclusion	30
8. Evaluation and award procedure	31
9. Award criteria	32
10. Legal and financial set-up of the Grant Agreements	33
Starting date and project duration	34
Milestones and deliverables	34
Form of grant, funding rate and maximum grant amount	34
Budget categories and cost eligibility rules	35
Reporting and payment arrangements	36
Prefinancing guarantees	37
Certificates	37
Liability regime for recoveries	37
Provisions concerning the project implementation	37
Other specificities	38
Non-compliance and breach of contract	38
11. How to submit an application	38
12. Help	39
13. Important	41
Annex 1	44
Annex 2	47

0. Introduction

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

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

- Regulation 2018/1046 (EU Financial Regulation)
- The basic act (Digital Europe Regulation 2021/694¹).

The call is launched in accordance with the [2021-2022] Work Programme² and will be managed by the **European Health and Digital Executive Agency (HaDEA)** ('Agency').

The call covers the following **topics**:

- DIGITAL-2021-TRUST-01-EDMO European Digital Media Observatory (EDMO) - national and multinational hubs
- DIGITAL-2021-TRUST-01-SAFERINTERNET Safer Internet Centres (SICs)
- DIGITAL-2021-TRUST-01-ECODEX e-Justice Communication via Online Data Exchange (e-CODEX)
- DIGITAL-2021-TRUST-01-DIGIPASS Digital Product Passport: sustainable and circular systems

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** on the Funding & Tenders Portal Topic page carefully, and in particular this Call Document, the Model Grant Agreement, the <u>EU Funding & Tenders Portal Online Manual</u> and the <u>EU Grants AGA — Annotated Grant Agreement</u>.

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

- the <u>Call Document</u> outlines the:
 - background, objectives, scope, activities that can be funded and the expected results (sections 1 and 2)
 - timetable and available budget (sections 3 and 4)
 - admissibility and eligibility conditions (including mandatory documents; sections 5 and 6)
 - criteria for financial and operational capacity and exclusion (section 7)
 - evaluation and award procedure (section 8)
 - award criteria (section 9)

Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme (OJ L 166, 11.05.2021).

Commission Implementing Decision C/2021/7914 of 10.11.2021 concerning the adoption of the multiannual work programme for 2021 - 2022 and the financing decision for the implementation of the Digital Europe Programme.

- 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 topic website to consult the list of projects funded previously:

DIGITAL-2021-TRUST-01-EDMO — European Digital Media Observatory (EDMO) - national and multinational hubs: https://edmo.eu/2021/05/26/national-edmo-hubs-announced/

1. Background

The Digital Europe Programme will reinforce EU critical digital capacities by focusing on the key areas of artificial intelligence (AI), cybersecurity, advanced computing, data infrastructure, governance and processing, the deployment of these technologies and their best use for critical sectors like energy, climate change and environment, manufacturing, agriculture and health.

The Digital Europe Programme is strategic in supporting the digital transformation of the EU industrial ecosystems. It targets upskilling to provide a workforce for these advanced digital technologies. It also supports private sector, small and medium-sized enterprises (SMEs), and public administration in their digital transformation with a reinforced network of European Digital Innovation Hubs (EDIH). The Digital Europe Programme will accelerate the economic recovery and drive the digital transformation of Europe.

During 2021-2022, one of the priorities of the Digital Europe Programme is 'accelerating best use of technologies'. Under 'accelerating best use of technologies', the roll-out and best use of digital capacities will focus on priority areas such as the support to the Green Deal, to SMEs and public authorities in their digital transformation and will also provide resources to those activities started in previous programmes, for which the continuations of funding is essential not to disrupt the services provided.

This call will cover the European Digital Media Observatory (EDMO) national and multinational hubs, Safer Internet, e-Justice Communication via online data exchange (e-CODEX) and Digital Product Passport as call topics that fall under the 'Accelerating Best Use of Technologies priority.

1. **EDMO-national and multinational hubs** – The Internet has profoundly changed how citizens access information. On the one hand, it has the potential to boost participation and inclusiveness in democratic processes. On the other

hand, it can facilitate the dissemination of disinformation. The April 2018 Commission Communication "Tackling online disinformation - A European has developed a strategy to limit the impact of online disinformation while respecting freedom of expression and other fundamental rights and democratic values.

As part of this strategy, the European Digital Media Observatory (EDMO) was launched on 1 June 2020. In the current phase, EDMO has deployed the Core Service Platform made of a technical infrastructure designed to facilitate knowledge exchanges and collaborative processes among fact-checkers, academic researchers and other relevant stakeholders, whose activities will be steered and coordinated by an independent governance body. Moreover, on 26 May the Commission announced the eight national and multinational hubs of EDMO selected through a competitive call for proposals. The selected hubs cover Ireland, Belgium, Czech Republic, Denmark, Finland, France, Italy, Luxemburg, the Netherlands, Poland, Slovakia, Spain, Sweden, as well as Norway, in the EEA. All the hubs are now operational. This call is to create additional hubs and cover the EU Member States and EEA countries which were not yet covered by the selected hubs.

- 2. Safer Internet Centres (SICs) has the objective to support national Safer Internet Centres in providing online safety information, educational resources, public awareness tools and counselling and reporting services, through dedicated helplines and hotlines for children, parents, and teachers and other professionals working with children. This call contributes to building trust in the digital transformation by supporting the sustainability of the Better Internet for Kids (BIK) strategy⁴ which is expected to be updated in 2022.
- 3. e-Justice Communication via Online Data Exchange (e-CODEX) is a key technological enabler for modernising, through digitalisation, communication in the context of cross-border judicial proceedings. e-CODEX consists of a package of software components that enables the interoperable connectivity between national systems. In this way, it allows its users (judicial and other competent authorities, legal practitioners and citizens) to electronically send and receive documents, legal forms, evidence or other information in a swift and secure manner. e-CODEX has been developed and maintained with EU financing by a consortium of Member States. The Commission adopted on 2 December 2020 a "Proposal for a Regulation on a computerised system for communication in cross-border civil and criminal proceedings (e-CODEX system)", the e-CODEX Regulation⁵. The Proposal aims to entrust the further development and maintenance of e-CODEX to the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) as of 2023.
- 4. Digital Product Passport sustainable and circular systems: has the objective to support sustainable production, to enable the transition to circular economy, to provide new business opportunities to economic actors, to support consumers in making sustainable choices and to allow authorities to verify compliance with legal obligations.

Communication from the Commission "Tackling online disinformation: a European Approach" COM(2018) 236 final

European Strategy for a Better Internet for Kids COM (2012) 196 final

Regulation on a computerised system for communication in cross-border civil and criminal proceedings (e-CODEX system), and amending Regulation (EU) 2018/1726 COM/2020/712 final

The Participation is open to all eligible entities as established by Article. 18 of the Digital Europe programme, in particular public sector as well as private sector organisations, including SMEs, NGOs and international organisations.

2. Objectives — Scope — Outcomes and deliverables — KPIs to measure outcomes and deliverables — Targeted stakeholders — Type of action — specific topic conditions

DIGITAL-2021-TRUST-01-EDMO — European Digital Media Observatory (EDMO) - national and multinational hubs

Objectives

As indicated in the Guidance to strengthen the Code of Practice on Disinformation⁶, EDMO and its national hubs are crucial to address the problem of disinformation effectively. EDMO does not only provide support in the area of research and fact-checking, but it also plays an important role regarding the monitoring framework, including assisting the Commission in the assessment of the Code's implementation and being part of the Permanent task-force.

This call aims to create new independent national or multinational hubs in order to expand the regional coverage of EDMO and its hubs. The ultimate objective of the call is to support the establishment of EDMO hubs in the **Member States not yet covered by the existing hubs**⁷. In this regard, one Member State should be covered by only one hub (including existing hubs and hubs yet to be established). At the same time, one hub can cover more than one Member State⁸.

A national/multinational hub is a network of organisations active in one or several Member State(s), that will provide specific knowledge of local information environments so as to strengthen the detection and analysis of disinformation campaigns, improve public awareness, and design effective responses relevant for national and regional audiences. The activities of the hubs should be independent from any public authority⁹.

These national/multinational hubs will focus their activities on emerging digital media vulnerabilities and disinformation campaigns, which are of special relevance within the territory and/or linguistic area in which they will operate. Multinational hubs will cover more than one Member State preferably with similar media ecosystems within an EU region. The hubs should as well strengthen the networks of independent fact-checkers at national and regional level.

Scope

 Increase the number of independent national or multinational EDMO hubs and cover Member States not yet covered by existing EDMO hubs while avoiding geographical overlaps between hubs – one Member State should be covered only by one hub.

⁶ European Commission Guidance on Strengthening the Code of Practice on Disinformation, 26 May 2021 (COM(2021) 262 final).

Member States covered by the existing EDMO hubs: Ireland, Belgium, Czech Republic, Denmark, Finland, France, Italy, Luxemburg, the Netherlands, Poland, Slovakia, Spain, Sweden, as well as Norway in the EEA.

⁸ It is highly recommended that potential applicants use the 'partner search' functionality in the funding and tenders portal, to check whether there are potential applicants from the same Member State and to explore the possibility for close collaboration at the application stage.

⁹ In the context of this call universities and public media organisations are not considered as public authorities unless they are under the direct influence of the national governments.

- Pull together and foster the growth of a national/multinational multidisciplinary community composed of academic researchers, independent fact-checkers based in the covered regions, media practitioners and other relevant stakeholders in order to create a network capable of quickly detecting and analysing disinformation campaigns, as well as producing content to support mainstream and local media and public authorities in exposing harmful disinformation campaigns. To this end applicants must prove their ability to reach out to at least 3 experts and/or organisations not involved in the proposal with **expertise in relevant areas of investigation and research** (e.g. health, climate change, immigration, security, economics, European policies, or other relevant areas prone to disinformation)¹⁰.
- Cooperate with EDMO and contribute to its repositories of fact-checks, media literacy materials and scientific articles, including surveys on disinformation trends, situational analyses and assessments of online platforms' policies to address disinformation-related harms. Hubs should aim to support the growth of local fact-checking and media literacy activities.
- Detect, analyse and disclose harmful disinformation campaigns at regional, national, multinational and EU level and analyse their impact on society and democracy. Hubs will analyse relevant actors, vectors, tools, methods, dissemination dynamics and prioritised targets of disinformation campaigns by applying a common methodology, established in coordination with EDMO, to monitor the evolution of disinformation-related harms on relevant audiences. Each hub should indicate in its proposal the type of collaborations intended with independent media outlets operating within its territory or linguistic area.
- Regularly assess the impact of relevant disinformation campaigns on society and democratic processes, as well as the effectiveness of the policies set out by online platforms to counter disinformation. In addition, the hubs will actively participate in the EDMO joint research activities selected by the EDMO Governance Body and promptly react to EDMO requests linked to emerging disinformation issues.
- Support tailor-made media literacy campaigns for the covered territory or linguistic area. Hubs will leverage on the exchange of good practices and materials stored on the EDMO platform and contribute to the EDMO repositories with their own material.
- Cooperate with institutions responsible for the monitoring of online platforms' policies and digital media ecosystem at national level. In particular, they will support the competent entities which oversee and participate in the monitoring of the implementation of the Code of Practice on Disinformation by its signatories.

Outcomes and deliverables

The following outcomes are expected to be elaborated in the proposal with an aim to include them in the Grant Agreement preparation and implementation of actions:

- Create the national/multinational hub, including a website and a communication campaign at national/multinational level;
- Integrate the hub into the EDMO in cooperation with EDMO's Governance Body; and link its platform to the <u>EDMO platform</u>;
- Ensure the production of a continuous flow of fact-checks which will be stored at the EDMO's repository;

Relevant information should be provided in the Application Form B Section 2.3

- Deliver at least 10 analytical reports on specific disinformation campaigns and/or studies linked to relevant disinformation phenomena;
- Deliver at least 5 media literacy campaigns or events at national/multi-national level to increase citizens' awareness and societal resilience;
- Deliver the annual reports on the support provided to monitor the policies put in place by online platforms to limit the impact of disinformation;
- Deliver the annual reports on the activities, including the information on: i) the cooperation with other national/multinational hubs through EDMO; ii) additional funds received by the hubs; and iii) the process put in place to preserve the independence of the hub.

Targeted stakeholders

Targeted stakeholders are fact-checking organisations, public and private research organisations, media organisations, and other stakeholders which conduct relevant activities for tackling the phenomenon of disinformation.

The following conditions are considered as important for the successful implementation of the hub activities described above:

a. The entity **coordinating** the consortium ("coordinator") should preferably be an independent public or private research organisation (see definition below¹¹

If the coordinator is not an independent public or private research organisation the proposal must: 12:

- Demonstrate independence of the coordinator from public authorities;
- Provide information about the coordinating organisation funding sources and demonstrate its independence from external sources of funding;
- Proof of coordinator's experience and activities related to research and/or investigations on the disinformation phenomenon.
- b. Public or private research organisations included in the application must demonstrate their relevant academic independent research experience in the fields such as communication, social and political sciences, law, economics, network science, data and computer sciences or other relevant areas¹³.
- c. Organisations that are not public or private research organisations must elaborate on their experience and activities related to research and/or investigations on the disinformation phenomenon 14 .
- d. At least one of the consortium applicants must be an **independent fact-checking organisation** or a fact-checking unit from an independent media

The coordinator should be a research organisation as per its statute and should provide in the Application Form B Section 2.3 a list with at least 10 scientific publications accepted in top conferences and/or journals covering fields such as media and disinformation, communication science, political science, network science, data and computer science or other relevant areas.

Relevant information should be provided in the Application Form B Section 2.3

The applicant must provide in the Application Form B Section 2.3 i)information that it is a research organisation as per its statute; ii) a list with at least 10 scientific publications accepted in top conferences and/or journals covering fields such as media and disinformation, communication science, political science, network science, data and computer science or other relevant areas.

The applicant should provide relevant information regarding the activities in the Application Form B Section 2.3

organisation with proven fact-checking activities in the last 12 months¹⁵. The consortium must have fact-checking services covering all geographical area covered by the hub (i.e. in every Member State covered by the hub).

Definitions of required types of applicants

For the purposes of this call, a research organisation is intended as "an entity, such as university or research institute, irrespective of its legal status (organised under public or private law) or way of financing, whose primary goal is to conduct fundamental research, industrial research or experimental development and to disseminate their results by way of teaching, publication or technology transfer; all profits are reinvested in these activities, the dissemination of their results or teaching; undertakings that can exert influence upon such an entity, in the quality of, for example, shareholders or members, shall enjoy no preferential access to the research capacities of such an entity or to the research results generated by it."

For the purposes of this call, a fact-checking organisation is intended as an organisation that:

- Regularly publishes nonpartisan reports on the accuracy of widely circulated claims of interest to society and of statements by major institutions, public figures and/or other. This includes the verification of multimedia content that reached a wide public. Provide through online links: i) Proof of legal or organisational statute; ii) fact checks published in the previous three months.
- Fact-checks claims using the same standard for every fact check; adheres to the highest quality standard in journalism, content verification and/or research; does not concentrate fact-checking efforts on any one side; follows the same process for every fact check and lets the evidence dictate conclusions; does not advocate or take policy positions on the issues it factchecks.
- Is transparent about its funding sources and states clearly where it's funding comes from. If it accepts funding from other organisations, it ensures that funders have no influence over the conclusions it reaches in its reports.
- It details the professional background of all key staff in the organisation and explains the organisational structure and legal status. It clearly indicates a way for readers to communicate with the organisation.
- Publishes its corrections policy and follows it scrupulously. It corrects clearly and transparently in line with the corrections policy, seeking so far as possible to ensure that readers see the corrected version.

Type of action

SME Support Actions — 50% and 75% (for SMEs) funding rate

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

The applicant must provide in the Application Form B Section 2.3: i) information that it is a fact-checker as per its statute and it fulfils the description given in the next subsection; ii) demonstrate that there is a publicly available statement or policy regarding advocacy/political positions from the organisation and its staff, iii) demonstrate that it has published at least 10 (ten) fact-checks in the previous twelve months; iv) information regarding the source(s) of its funding and demonstrate independence from external funders.

Specific topic conditions

- For this topic, multi-beneficiary applications are mandatory and specific conditions for the consortium composition apply (see section 6).
- For this topic, following reimbursement option for equipment costs applies: full costs only.
- 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-2021-TRUST-01-SAFERINTERNET — Safer Internet Centres (SICs)

Objectives

The objective of the topic is to support national Safer Internet Centres (SICs) (i.e hubs gathering NGOs, government bodies/agencies, private sector organisations) in providing online safety information, educational resources, public awareness tools and counselling and reporting services (through dedicated helplines and hotlines) for children¹⁶, parents, and teachers and other professionals working with children. The activities performed by the SICs will help children to tackle online risks and to become media literate, resilient digital citizens, and will allow citizens to anonymously report online child sexual abuse material (CSAM).

Scope

The funding will ensure the financial sustainability of the European network of SICs, by enabling the awarded national Safer Internet Centre to provide at least:

Activity 1

A centre for **raising awareness** about online opportunities and risks among children, parents, teachers and other professionals working with children (e.g. educators, child care workers, health personnel) about online opportunities and risks. The focus will be, also in the light of Covid-19 crisis experience¹⁷, to identify and address emerging risks (e.g. self-generated sexualised content, live streaming of violent and age-inappropriate content, datafication of childhood) and challenges such as mental and physical health issues related to the use of technologies (self-harm, addiction, perception of self-identity and self-image) as well as to foster digital literacy, empowerment and youth participation.

¹⁶ A child is a person under 18 years of age <u>Eurostat</u>, 2020.

Europol, Exploiting Isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic and JRC, How children (10-18) experienced online risks during the Covid-19 lockdown - Spring 2020

More specifically the awareness centre will:

- a. Devise informative and innovative awareness campaigns and resources to give children the digital skills and tools they need to take advantage of the digital transformation. Promote awareness of parents and children on online high quality and age appropriate content and experiences and make the associated resources available through their services. The resources proposed should represent a balanced mix of different public friendly and accessible online and offline resources such as, but not limited to: teaching resources, apps, booklets and leaflets, videos, games, blogs, vlogs, posters, etc. The resources should address children's rights, and a range of ages and topics. Moreover positive online experiences should be promoted, for example through stimulating uptake of games and other engaging media to support awareness raising, and encouraging children to define their needs for better protection and empowerment in the digital transformation..
- b. Engage directly with children from different demographic groups, including the organisation of regular youth participation activities, allowing them to express their views and pool their knowledge and experience of using online technologies. Particular attention should be paid to maximising opportunities and minimising risks for children in situations of vulnerability (e.g. children with disabilities, children with a minority racial or ethnic background, child victims).
- c. Evaluate the impact of the awareness campaigns on the target groups and provide qualitative and quantitative feedback at European level on a regular basis as defined by the EU Better Internet for Kids (BIK) platform;
- d. Establish and maintain partnerships and promote dialogue and exchange of information with key players (government agencies, private sector, user organisations and education stakeholders) at national level.

Activity 2

A **helpline** to give advice and support to children, parents and other adults concerned on issues related to children's use of digital technologies and services. More specifically the helpline will:

- a. Offer one-to-one conversations via telephone, email and online chat services, with trained helpers to give advice and support to children and parents on online related issues; solutions to offer a '24 hours a day / 7 days a week' support should be explored, including using artificial intelligence together with human moderation when appropriate;
- Develop/launch an ambitious national communication strategy including key performance indicators, both in terms of reach and impact to raise the visibility of the helpline services;
- c. Draw up or update the operating guidelines in compliance with national law, including data protection rules;
- d. Provide qualitative and quantitative feedback at European level on a regular basis on the main online risks and new trends as defined by the EU Better Internet for Kids (BIK) platform¹⁸.

13

¹⁸ https://www.betterinternetforkids.eu

Activity 3

A **hotline** for tackling CSAM (i.e. receiving, analysing, and processing reports of such material). Closer cooperation with law enforcement and the private sector should be further explored. The specific tasks include the following:

- Establish or continue to operate a hotline to receive information from the public relating to potential CSAM (reports), and if deemed appropriate racism and xenophobia;
- b. Draw up or update the hotline manual of procedures in cooperation with law enforcement authorities and in accordance with best practice guidelines;
- c. Cooperate with the INHOPE network of hotlines and make full use of and connect to the technical infrastructure ICCAM;
- d. Undertake a preliminary assessment of the legality of the content reported and trace its origin, and forward the report to the body for action (Internet Service Provider, law enforcement agency or corresponding hotline) including systematic notice to the host provider of content assessed as CSAM and monitoring of the take-down; forward suspicions of illegal content to certain stakeholders (Internet Service Provider, law enforcement agency or corresponding hotline) for further assessment;
- e. Ensure compatibility with data formats of the technical infrastructure ICCAM and provide statistics required for measuring the impact and effectiveness of the network of hotlines (e.g. time to removal of the illegal content);
- f. Develop/update and launch an ambitious national communication strategy including key performance indicators, both in terms of reach and impact to raise the visibility of the hotline services;
- g. Develop/update and implement a proactive monitoring and follow-up procedure for the takedown of CSAM where legally possible, including the collection of statistical data (e.g. time of receipt of report, notice, takedown; number of reports transmitted to law enforcement, requests for takedown to hosting services, feedback to users);
- Extend the notice and takedown procedure to child sexual exploitation material (CSEM) not qualified as illegal at national level (e.g. posing, nudity) where legally possible, in order to protect personal data of children;
- i. Extend the notice and takedown procedure of CSAM to countries without a national hotline, where legally possible;
- j. Propose a design enabling a high level of automation in the report handling process, so reducing manual tasks. The automation strategy shall take into account the national legal environment, which sets the limits for the hotline's operations.

SICs must be composed of an awareness centre and a helpline, and preferably a hotline. If a hotline is not part of the proposal, this absence has to be justified. SICs that have been awarded a grant under this call are expected to join the Insafe network of awareness centres and helplines, and the INHOPE network of hotlines.

The three strands of the SIC will be expected to cooperate by setting up or to continue to run a single Advisory Board with relevant national stakeholders (e.g. from public authorities; academia; private sector; civil society; representatives of parents, teachers, and children), and to actively contribute to the implementation of a

European approach by sharing information, good practices, and resources with the EU Better Internet for Kids (BIK) platform, and by taking part in EU-level events.

Funding will be limited to one Safer Internet Centre per eligible country

Outcomes and deliverables

The investment will deliver a pan-European network of SICs that will allow children to become more resilient digital users through awareness-raising activities in informal and formal education (e.g. youth participation activities, workshops, classroom visits, competitions). Parents, teachers and other professionals working with children will gain a better understanding of the risks and opportunities of children accessing digital content and services, through information sessions, train the trainers programmes, and online and offline material. Local, national, and European actors will gain timely information on emerging risks through the helpline service. Public authorities including law enforcement agencies will have access to resources and services, and exchanges with hotline analysts to develop better preventive measures and to remove CSAM in an effective manner. The private sector will benefit from increased market opportunities for high quality online content and will cooperate with the SICs through joint initiatives and awareness campaigns such as the Safer Internet Day.

For each of the three strands of activities the proposals selected for funding will be required to demonstrate that they have achieved the following results by the end of the Action:

Activity 1: An awareness centre

- a. A dissemination and communication plan for the awareness activities including key performance indicators, both in terms of reach and impact for each of the proposed activities and resources targeting children, parents and teachers and other professionals working with children.
- b. On a regular basis, provide qualitative and quantitative feedback at European level as defined by the EU Better Internet for Kids platform.
- c. An evaluation of the impact of the awareness campaigns on the target groups and report on the key performance indicators.
- d. A report on the partnerships established/maintained and on the exchange of information with key players (e.g. government agencies, private sector, user organisations, education stakeholders) at national level.

Activity 2: Helpline

- a. A national communication and dissemination strategy including key performance indicators, both in terms of reach and impact to raise the visibility of the helpline services.
- b. A helpline operating guidelines in compliance with national law, including data protection rules.
- c. On a regular basis provide qualitative and quantitative feedback at European level as defined by the EU Better Internet for Kids (BIK) platform.
- d. An evaluation of the impact of the national communication and dissemination strategy and report on the key performance indicators of the helpline.

Activity 3: Hotline

- a. A national communication and dissemination strategy including key performance indicators, both in terms of reach and impact to raise the visibility of the hotline services.
- b. An evaluation of the impact of the national communication and dissemination strategy and report on the key performance indicators of the hotline.
- c. A hotline manual of procedures in cooperation with law enforcement authorities and in accordance with best practice guidelines.
- d. Regular and timely processing of reports received. Where legally possible, the hotline must make a preliminary assessment of the legality of the content reported, trace its origin, and forward the report to the appropriate body for action (Internet Service Provider, the law enforcement agency or corresponding hotline). This should include, where legally possible, systematic notice to the host provider of content assessed as CSAM, monitoring of the take-down, and/or forwarding suspected illegal content to certain stakeholders (Internet Service Provider, the law enforcement agency or corresponding hotline) for further assessment.
- e. Compatibility with data formats of the technical infrastructure ICCAM and the production of statistics required for measuring the impact and effectiveness of the network of hotlines (e.g. time to removal of the illegal content).
- f. A proactive monitoring and follow-up procedure for the takedown of CSAM, where legally possible, including the collection of statistical data (e.g. time of receipt of report, notice and takedown).
- g. An extension of the notice and takedown procedure of CSAM to countries without a national hotline, where legally possible.
- h. An extension of the notice and takedown procedure to CSEM, where legally possible, including the collection of statistical data (e.g. time of receipt of report, notice, takedown).
- i. A report on the design and implementation of automated report handling.

KPIs to measure outcomes and deliverables

- Number of new or updated online resources made available by the Safer Internet Centres (e.g. trainings, videos, events, etc.). The minimum target is 1,100 resources uploaded combined by all EU co-funded Safer Internet Centres per year.
- Number of requests handled by the co-funded helpline services. The minimum target is 63,000 requests every year combined by all EU co-funded helplines.
- Number of reports received by the co-funded hotlines. The minimum target is 200,000 reports every year combined by all EU co-funded hotlines.

Targeted stakeholders

Existing or new Safer Internet Centres in the eligible countries.

Type of action

Simple Grants - 50% co-funding rate

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

Specific topic conditions

- For this topic, following reimbursement option for equipment costs applies: full costs only
- 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-2021-TRUST-01-ECODEX — e-Justice Communication via Online Data Exchange (e-CODEX)

Objectives

The aim of this call for proposals is to provide a continued robust, albeit temporary, sustainability framework for the continued management, development and maintenance of the e-CODEX system, previously developed and maintained as a Core Service Platform (CSP) under the Connecting Europe Facility (CEF) in the field of Trans-European Telecommunication Networks. At the end of the project, the e-CODEX system will be handed over to the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA).

In the description of the activities described below, the term "core projects" shall be understood to cover the following e-CODEX use cases at the minimum:

- European Payment Order
- European Small Claims Procedure
- The e-Evidence Digital Exchange System (including Mutual Legal Assistance in Criminal Matters)
- In the context of the decentralised IT system pursuant to the recast Service of documents and Taking of Evidence Regulations in civil and commercial matters
- The iSupport system

Scope

The applicants must cover, at the minimum, the full set of tasks and activities outlined hereunder. The action should follow seamlessly from the presently ongoing Me-CODEX II project. It should be noted that those tasks that follow from the draft e-CODEX Regulation, currently being negotiated in Council and the European Parliament, may be adjusted to reflect the provisions of the final Regulation as adopted.

Governance and management aspects

- Governance and operational management of the e-CODEX system;
- Project, risk and quality management;
- Transparent administration and communication about the progress of the project, monitoring of the uptake of e-CODEX and identification of stakeholder needs;
- Management of the components of the e-CODEX system and of the supporting software products;
- Provision of an updated project plan (every six months), available to the Commission¹⁹, HaDEA and all e-CODEX stakeholders, with detailed delivery milestones for tasks and sub-tasks. This is required in order to ensure the visibility of task planning and the reliability of the delivery deadlines to the user community.
- Further developing e-CODEX to support areas where its potential use has already been identified. These activities must not exceed 10% of the overall project budget.

Software development aspects

- Provision of maintenance, further technical evolution, defect resolution and regular updates (with a swift response to security issues) of the e-CODEX system's software components;
- Adjustments to the e-CODEX components to:
 - Ensure alignment with amendments in legal procedures for which e-CODEX is already used or could be used (e.g. in the context of Regulation (EU) 2020/1784²⁰ and Regulation (EU) 2020/1783²¹)
 - Align with other legal changes with impact on the use of the e-CODEX system (e.g. pertaining to electronic signatures);
 - Maintain semantic interoperability;
 - Maintain alignment with changes in the CEF eDelivery and eSignature Building Blocks and/or evolutions concerning other software components;
 - Upgrade the e-CODEX system to align with evolving standards and address user requirements. Exploration of technical solutions to limit the operational overhead caused by the growing number of participants in the network, such as dynamic discovery;
 - Ensure compliance with Regulation (EU) 2016/679 (the General Data Protection Regulation)²²;
 - Implement the principles of security by design and data protection by design and by default.
- Production and provision of new or improved clear and comprehensive technical documentation for the e-CODEX system technical artefacts;
- Updates and distribution to the authorised e-CODEX access points of all documentation relating to the components of the e-CODEX system and its supporting software products, the business process models, the templates defining the electronic format of documents and of the underlying pre-defined collection of data models;

¹⁹ DG Justice and Consumers of the European Commission.

²⁰ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020R1784

^{21 &}lt;a href="https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020R1783">https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020R1783

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. L 119/1, 4.5.2016.

- Maintenance of the EU e-Justice Core Vocabulary, on which the business process models and templates are based;
- Making all e-CODEX products available in public repositories and ensuring that what is published is constantly up to date. This should not only cover the produced technical artefacts, but also the necessary source material for their maintenance and re-generation (e.g. source code, input for generation of XML schemas, etc.);
- Provision and maintenance of environment-independent versions of the e-CODEX products. In particular, of the Central Testing Platform and the Configuration Management Tool to be used for the maintenance, update and distribution of a configuration file containing an exhaustive list of authorised e-CODEX access points, including the cross-border procedures and forms each of these access points is authorised to use;
- Preparation and distribution to the authorised e-CODEX access points of new business process models and templates defining the electronic format of documents.

Communication, support and customer outreach activities

- Stakeholder engagement using electronic means of communication, and where relevant and possible via physical meetings;
- Online presence and communication activities.
- Elaboration of an engagement strategy with the e-CODEX system user community in order to assess the quality, usability and sustainability of the products and creation of a follow-up action plan;
- Outreach to further Member States for deploying the e-CODEX generic service in the context of one or more areas where it is in use;
- Support all current pilot e-CODEX use cases²³, to help align to the version of e-CODEX that will be handed over to eu-LISA. This concerns operational activities in view of the handover to eu-LISA;
- Rollout and operational support for new and existing participants in the core projects;
- Advice and support of new areas of e-CODEX, both at a technological and business level. Support to projects leveraging e-CODEX other than its core projects (conference calls, remote assistance);
- Support and coordination of testing activities, including connectivity testing, involving the authorised e-CODEX access points;
- Coordination with parallel projects dealing with other e-CODEX aspects;
- Collection of user feedback in a systematic way and preparation of future adaptations of the Core Service Platform.
- Communication and customer outreach activities must not exceed 10% of the overall project budget

Handover activities

- By 1 October 2022 at the latest, the grant beneficiaries must submit the following information and material, in a format and with a level of detail appropriate to serve as implementing acts under a future EU Regulation governing the e-CODEX system:
 - the minimum technical specifications and standards, including on security (see below) and methods for integrity and authenticity verification;

²³ https://www.hcch.net/en/instruments/conventions/specialised-sections/child-support/isupport1

- draft service level requirements for the activities to be carried out by eu-LISA, as well as other necessary technical specifications for those activities:
- a proposal for the specific arrangements of the handover/takeover process (see below).
- The grant beneficiaries must submit a detailed security plan for e-CODEX by 31 December 2022, at the latest. In addition, they must develop security rules and guidance on security issues regarding the e-CODEX access points, which are managed by authorised national authorities.
- By 31 December 2022, at the latest, the grant beneficiaries should submit a common handover document to eu-LISA, specifying the detailed arrangements for the transfer of the e-CODEX system, including the description on how the criteria for a successful handover process and completion, established by the Commission, are going to be fulfilled. It will also contain the related documentation.
- The grant beneficiaries must plan for a handover and transfer of the intellectual property and usage rights associated with all e-CODEX material i.e. software binaries, source code, project documentation, XML schemas, etc. to either the European Commission or eu-LISA following the Grant Agreement's conclusion. Directorate-General Justice and Consumers of the Commission will inform the beneficiary(ies) on the exact modalities in this regard during the project's execution. In view of the Commission proposal on e-CODEX (COM 2020/712)²⁴, the transfer of intellectual property rights must take place by 31 December 2022. The applicants must take this date into account in their proposal²⁵.
- The handover process should be completed by 1 July 2023. During the implementation period, the grant beneficiaries will continue to manage the e-CODEX system and will retain full responsibility for it. They will ensure that only corrective maintenance activities are performed in the system and that no new release of the e-CODEX system is delivered. The Commission²⁶ will monitor the handover/takeover process.

Outcomes and deliverables

The outcome of the action grant must guarantee robust management, development and maintenance of the e-CODEX system, as well as its timely handover to eu-LISA.

The project partners must further ensure that the tools chosen to produce the project's artefacts should not lead to vendor lock-in and thus impede the future take-up, further development and maintenance of those artefacts. If such tools are used, clear arrangements have to be made to provide a perpetual free of charge licence for their use by the receiving organisation.

All software components produced or updated in the execution of work must be published on the <u>Joinup platform</u> under a <u>EUPL v1.2 licence</u>. In case applicants are unable to comply with this condition, due to third party licencing restrictions, they should provide substantiated justifications.

KPIs to measure outcomes and deliverables

All project milestones have been met;

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020PC0712

Without prejudice to the final legal act, which may revise this date.

²⁶ DG Justice and Consumers of the European Commission.

- All planned deliverables have been produced, delivered and accepted;
- e-CODEX is successfully²⁷ handed over to eu-LISA by 1 July 2023.

Targeted stakeholders

EU Member State public authorities and other international organisations, Joint Undertakings²⁸, public and private undertakings, bodies or entities established in the EU Member States or EEA countries.

Please also refer to Section 6 - Consortium Composition.

Type of action

Coordination and Support Actions — 100% funding rate

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

Specific topic conditions

- For this topic, multi-beneficiary applications are mandatory and specific conditions for the consortium composition apply (see section 6)
- For this topic, following reimbursement option for equipment costs applies: full costs only
- For this topic, access rights to ensure continuity and interoperability obligations apply (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-2021-TRUST-01-DIGIPASS — Digital Product Passport: sustainable and circular systems

Objectives

The Sustainable Products Initiative foreseen in the new Circular Economy Action Plan (CEAP)²⁹ should establish a Digital Product Passport (DPP) that gathers and makes accessible data on a product and its value chain. The objective of the DPP is:

 To support sustainable products and production, to enable the transition to circular economy, boosting material and energy efficiency, extending product lifetimes and optimizing product use;

²⁷ Defined as based on the agreement of the beneficiary(ies), the Commission and eu-LISA.

²⁸ For the purposes of this call, a Joint Undertaking means a joint undertaking established by the EU for the efficient execution of EU research, technological development and demonstration programmes, as referred to in Article 187 of the <u>Treaty on the Functioning of the European Union</u>.

²⁹ Circular Economy Action Plan (CEAP), COM(2020) 98 final

- To provide new business opportunities to economic actors through circular value retention and extraction (for example repair, servicing, remanufacturing, recycling, extended producer responsibility and product-as-a-service activities) based on improved access to data;
- To support consumers in making sustainable choices; and
- To allow authorities to verify compliance with legal obligations.

The objective of this Coordination and Support Action is to prepare the ground for a gradual piloting as of 2023 of a digital product passport (DPP) in minimum 3 key value chains: electronics and ICT (at least consumer electronics), batteries as defined in and included in the scope in the proposal for a Regulation on batteries³⁰, and, at least another one of the key value chains identified in CEAP such as textiles (garments and apparel), packaging (particularly plastic), furniture, construction and buildings.

Scope

The overall aim is to support the goals of the Green Deal and in particular Circular Economy Action Plan's Sustainable Product Initiative, the EU Digital strategy's Circular Electronics Initiative and the EU Data strategy by improving product sustainability, boosting material and energy efficiency, enabling new business models and circular value extraction based on data sharing.

A specific contribution is expected on identifying the data held or generated by operators along these value chains for which an access by other relevant stakeholders would have a major beneficial impact on circularity and sustainability. This should be done through consultation with the private and public stakeholders at all stages of those value chains, in order to establish which data could be included in the DPP. In order to keep the DPP manageable, it is not expected to include comprehensive data, but rather the most essential for unlocking circular value and improving product sustainability.

The work should also establish protocols for secure and tailored access for relevant stakeholders, and contribute to the development of standardized and open digital solutions for identification, tracking, mapping and sharing of product information along its life-cycle, ensuring interoperability across borders and a well-functioning EU Internal Market. This work needs to build on and complement existing open global standards with the aim to provide for a consistent operational framework.

Particular emphasis should be given to balanced and inclusive engagement of all relevant stakeholders throughout the value chain and to optimal use of adequate and up-to-date digital technologies.

This CSA will support the establishment of an interoperable data space, building on and linking to manufacturing dataspaces (see topic 2.2.1.4 in the DEP 2021-2022 Work Programme) and other available and relevant data sources. The awarded consortium will work in partnership with the Data Spaces Support Centre (see 2.2.2.1 in the DEP 2021-2022 Work Programme) in order to ensure alignment with the Smart Middleware Platform developed under topic 2.1.1, and actions in the context of section 2.2.1 of this Work Programme, and in particular:

Proposal for a Regulation of the European Parliament and of the Council concerning batteries and waste batteries, repealing Directive 2006/66/EC and amending Regulation (EU) No 2019/1020 COM(2020) 798 final and Annex 13

- the data space reference architecture, building blocks and common toolboxes to be used;
- the common standards, including semantic standards and interoperability protocols, both domain-specific and crosscutting;
- The data governance models, business models and strategies for running data spaces.

Outcomes and deliverables

Delivery of at least 3 digital product passport prototypes, one in each of the 3 key value chains mentioned above, including agreements on:

- Agreed key data for circularity and their classification according to potential importance in delivering benefits for circularity and sustainability, along with recommendations for dealing with potential disagreements over access;
- Data and system architectures, including an analysis of any risks;
- Open European or global standards and relevant classifications and nomenclatures, based on a commonly applicable framework concept.

For each of the key value chains considered, the deliverables should include a roadmap with milestones for piloting of the developed DPP prototypes as of 2023, as well as a gradual deployment of DPP as of 2026, based on analysis of existing and upcoming legislation, existing European and global standards, past and ongoing activities and initiatives related to DPP in these sectors. The business model to ensure the deployment and continuity of use has to be also addressed.

While different product groups will have different information requirements, the necessary conditions to enable cross-sectoral interoperability and use should be identified and proposed. The results are also expected to support the EU Single Market providing consistent information about products, across the value chain and borders, to business, customers and authorities.

The work should also-contribute to future DPP in other key value chains by harnessing lessons learnt in effective concertation of stakeholders, provision of a roadmaps for open and standardised approaches for viable use of digital product passports based on digital innovations that are beneficial in terms of environmental sustainability and circular business opportunities.

KPIs to measure outcomes and deliverables

Agreements and protocols between the stakeholders for each key value chain considered on:

- Specific data provision requirements for each class of stakeholder.
- The architecture and solutions for product identification and data access.
- Horizontal rules for data provision, classifications and access.
- The roadmap and milestones for their key value chain deployment.

Targeted stakeholders

Targeted stakeholders are parties that represent or have demonstrated ability to gather economic actors/standardization bodies along each entire key value chain, including suppliers (of components, intermediary goods and materials), materials

processors, Original Equipment Manufacturers (OEMs), distributors, wholesalers and retailers, public and private consumers, recyclers and producer responsibility organisations. Particular attention should be paid to ensuring representation of SMEs, disruptive and circular businesses.

Relevant stakeholders include also European and international bodies and standardization organisations that will work on ensuring cross-sector interoperability of sectoral digital product passports.

The Consortium should display the relevant convening power to identify, address and involve the targeted stakeholders along the considered value chains (also including other experts from academia and NGOs) to work on common methodologies for DPP and the product related DPP prototypes. The consortium should show a good understanding of circular economy and sustainable design, and minimum experience in the subject matter of digital data exchanges, in steering complex multi-stakeholder projects and providing a robust project design as a basis to delivering within the short projects duration.

Type of action

Coordination and Support Actions — 100% funding rate

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

Specific topic conditions

- For this topic, following reimbursement option for equipment costs applies: depreciation only
- For this topic, access rights to ensure continuity and interoperability obligations apply (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*

3. Available budget

The available call budget is **EUR 37 000 000**. This budget might be increased by maximum 20%. Specific budget information per topic can be found in the table below.

Торіс	Topic budget	
1 — DIGITAL-2021-TRUST-01-EDMO	EUR 11 000 000	
2 — DIGITAL-2021-TRUST-01-SAFERINTERNET	EUR 21 000 000	
3 — DIGITAL-2021-TRUST-01-ECODEX	EUR 3 000 000	
4 — DIGITAL-2021-TRUST-01-DIGIPASS	EUR 2 000 000	

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

4. Timetable and deadlines

imetable and deadlines (indicative)			
Call opening:	17 November 2021		
Deadline for submission:	22 February 2022 – 17:00:00 CET (Brussels)		
Evaluation:	14 March to 29 April 2022		
Information on evaluation results:	End of May 2022		
GA signature:	September 2022		

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 <u>Search Funding & Tenders</u> section). Paper submissions are NOT possible.

Proposals (including annexes and supporting documents) must be submitted using the forms provided *inside* the Submission System ($\stackrel{1}{\bigtriangleup}$ 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 (to be downloaded from the Portal Submission System, completed and then assembled and re-uploaded)
- mandatory annexes and supporting documents (to be uploaded):
 - detailed budget table: not applicable
 - CVs of core project team: not applicable
 - activity reports of last year: not applicable
 - list of previous projects: not applicable
 - security issues table: applicable
 - ethics issues table: applicable
 - ownership control declaration: not 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 the 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**.

Proposals for <u>Simple Grants</u> and <u>SME Support Actions</u> are limited to maximum **70 pages** (Part B). Proposals for <u>Coordination and Support Actions</u> are limited to maximum **50 pages** (Part B). Evaluators will not consider any additional pages.

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

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

6. Eligibility

Eligible participants (eligible countries)

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

- be legal entities (public or private bodies)
- be established in one of the eligible countries, i.e.:
 - EU Member States (including overseas countries and territories (OCTs)
 - non-EU countries
 - listed EEA countries and countries associated to the Digital Europe Programme (associated countries) or countries which are in ongoing negotiations for an association agreement and where the agreement enters into force before grant signature) or countries which are in ongoing negotiations for an association agreement and where the agreement enters into force before grant signature

Beneficiaries and affiliated entities must register in the <u>Participant Register</u> — 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).

Specific cases

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

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

Entities without legal personality — Entities which do not have legal personality under their national law may exceptionally participate, provided that their representatives have the capacity to undertake legal obligations on their behalf, and offer guarantees for the protection of the EU financial interests equivalent to that offered by legal persons31.

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'32. 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 (see above) may participate in the call and can sign grants if the negotiations are concluded before grant signature (with retroactive effect, if provided in the agreement).

EU restrictive measures — Special rules apply for certain entities (e.g. entities subject to <u>EU restrictive measures</u> under Article 29 of the Treaty on the European Union (TEU) and Article 215 of the Treaty on the Functioning of the EU (TFEU)33 and entities covered by Commission Guidelines No <u>2013/C 205/05</u>34). 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).

For more information, see <u>Rules for Legal Entity Validation</u>, <u>LEAR Appointment and Financial Capacity Assessment</u>.

Consortium composition

Proposals must be submitted by:

for topics **DIGITAL-2021-TRUST-01-EDMO**:

- Minimum 2 applicants (beneficiaries; not affiliated entities).
- The coordinator of the consortium is established in a Member State to be covered by the hub.
- The consortium includes at least one independent fact-checking organisation or a fact-checking unit from an independent media organisation. The consortium must have fact-checking services covering all geographical area to be covered by the hub (i.e. in every Member State to be covered by the hub).

for topics **DIGITAL-2021-TRUST-01-ECODEX**:

- Minimum 2 applicants (beneficiaries; not affiliated entities) from different

³¹ See Article 197(2)(c) EU Financial Regulation 2018/1046.

For the definitions, see Articles 187(2) and 197(2)(c) EU Financial Regulation 2018/1046.

³³ Please note that the EU Official Journal contains the official list and, in case of conflict, its content prevails over that of the <u>EU Sanctions Map</u>.

Commission guidelines No 2013/C 205/05 on the eligibility of Israeli entities and their activities in the territories occupied by Israel since June 1967 for grants, prizes and financial instruments funded by the EU from 2014 onwards (OJEU C 205 of 19.07.2013, pp. 9-11).

eligible countries.

 Proposals **must** be submitted by at least two EU Member State public authorities which have been previously responsible for the maintenance of the e-CODEX system.

Refer to section - Targeted Stakeholders.

Eligible activities

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).

Ethics

Projects must comply with:

- highest ethical standards and
- applicable EU, international and national law (including the <u>General Data Protection Regulation 2016/679</u>)

Proposals under this call for proposals 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 $2015/444^{35}$ 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

³⁵ See Commission Decision 2015/544/EU, Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53.

- 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 clearing (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 clearing may have to be provided before grant signature. The granting authority will assess the need for clearing 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 clearing.

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

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

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 these projects.

The financial capacity check will be carried out on the basis of the documents you will be requested to upload in the <u>Participant Register</u> 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 <u>Rules for Legal Entity Validation</u>, <u>LEAR Appointment and Financial Capacity Assessment</u>.

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 operational 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 participate³⁶:

 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)

See Articles 136 and 141 of EU Financial Regulation 2018/1046.

- 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 misconduct³⁷ (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 Regulation No 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).

Applicants will also be refused if it turns out that³⁸:

- 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** (composed or 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:

Professional misconduct includes: violation of ethical standards of the profession, wrongful conduct with impact on professional credibility, false declarations/misrepresentation of information, participation in a cartel or other agreement distorting competition, violation of IPR, attempting to influence decision-making processes or obtain confidential information from public authorities to gain advantage.

³⁸ See Article 141 EU Financial Regulation 2018/1046.

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.

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. 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 are considered to have been accessed and that deadlines will be counted from opening/access (see also <u>Funding & Tenders Portal Terms and Conditions</u>). 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:

- 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*

- 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

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 call budget. 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. Retroactive application can be granted exceptionally for duly justified reasons.

Indicative Project duration:

- 30 months for topic DIGITAL-2021-TRUST-01-EDMO
- 24 months for topics: DIGITAL-2021-TRUST-01-SAFERINTERNET and DIGITAL-2021-TRUST-01-ECODEX
- 18 months for topic DIGITAL-2021-TRUST-01-DIGIPASS

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

The following deliverables will be mandatory for DIGITAL-2021-TRUST-01-ECODEX are:

- Supporting material required for the preparation of the implementing act (minimum technical specifications and standards, draft service level requirements, handover/takeover proposal) – by 1 October 2022
- Detailed security plan for e-CODEX by 31 December 2022
- Bill of Materials (BOM)
- Project Plan
- Risk assessment list
- Software, documentation and supporting material

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 (maximum grant amount):

EUR 1 500 000 per project for topic DIGITAL-2021-TRUST-01-EDMO

- EUR 1 500 000 per project for topic DIGITAL-2021-TRUST-01-SAFERINTERNET
- EUR 3 000 000 per project for topic DIGITAL-2021-TRUST-01-ECODEX
- EUR 2 000 000 per project for topic DIGITAL-2021-TRUST-01-DIGIPASS

The grant awarded may be lower than the amount requested.

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.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): Yes
 - SME owner/natural person unit cost³⁹: Yes

³⁹ Commission <u>Decision</u> 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

- travel and subsistence unit costs⁴⁰: No (only actual costs)
- equipment costs:
 - depreciation for topic DIGITAL-2021-TRUST-01-DIGIPASS
 - full cost for topics DIGITAL-2021-TRUST-01-SAFERINTERNET, DIGITAL-2021-TRUST-01-EDMO, DIGITAL-2021-TRUST-01-ECODEX
- other cost categories:
 - costs for financial support to third parties: not allowed.
 - internally invoiced goods and services (costs unit cost according to usual cost accounting practices): 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 VAT is eligible (but please note that since 2013 VAT paid by beneficiaries that are public bodies acting as public authority is NOT eligible)
- other:
 - in-kind contributions for free are allowed, but cost-neutral, i.e. they cannot be declared as cost
 - kick-off meeting: costs for kick-off meeting organised by the granting authority are eligible (travel costs for maximum 2 persons, return ticket to Brussels and accommodation for one night) only if the meeting takes place after the project starting date set out in the Grant Agreement; the starting date can be changed through an amendment, if needed
 - project websites: communication costs for presenting the project on the participants' websites or social media accounts are eligible; costs for separate project websites are not eligible

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 **50%** 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.

receiving a salary for the work carried out by themselves under an action or work programme (C(2020)7715).

Commission <u>Decision</u> 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).

Please be aware that payments will be automatically lowered if 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 note that you are responsible for keeping records on all the work done and the costs declared.

Prefinancing quarantees

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 formally NOT linked to individual consortium members, which means that you are free to organise how to provide the guarantee amount (by one or several beneficiaries, for the overall amount or several guarantees for partial amounts, by the beneficiary concerned or by another beneficiary, etc). It is however important that the requested amount is covered and that the guarantee(s) are sent to us 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.

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: Yesexploitation of results: Yes

- rights of use on results: Yes

access to results for policy purposes: Yes

- access rights for the granting authority to results in case of a public emergency: Yes
- access rights to ensure continuity and interoperability obligations: Yes for topic DIGITAL-2021-TRUST-01-ECODEX

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 communication activities: Yes

special logo: No

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

Other specificities

n/a

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 <u>AGA — Annotated Grant Agreement</u>.

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 <u>create</u> an <u>EU Login user account</u>.

Once you have an EULogin account, you can <u>register your organisation</u> 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 <u>Search Funding & Tenders</u> 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 might 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 <u>Online Manual</u>. 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
- <u>FAQs on the Topic page</u> (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 ${\underline {\tt IT}}$ ${\underline {\tt Helpdesk}}.$

Non-IT related questions should be sent to the following email address: <u>HADEA-DEP-DIGITAL-CALLS@ec.europa.eu</u>

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).
- **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).
- **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 double funding** There is a strict prohibition of double 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 declared to two different EU actions.
- **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).
- **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 Model 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 a 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 one of them (or it 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 <u>EU Financial Regulation</u>, information about EU grants awarded is published each year on the <u>Europa website</u>.

This includes:

- o beneficiary names
- o beneficiary addresses
- o the purpose for which the grant was awarded
- o 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 will use the following actions to implement grants:

Simple Grants

Description: The Simple Grants 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: 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: 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: Type of action for which 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 cashflow to finance the procurements) – payment of the balance

PAC Grants for Procurement

Description: 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 cashflow to finance the procurements) – payment of the balance

Grants for Financial Support

Description: Type of action with 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 prefinancing 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 cashflow to finance sub-grants) – payment of the balance

Framework Partnerships (FPAs) and Specific Grants (SGAs)

FPAs

Description: An FPA establishes 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 coordinator of the FPA has to be the coordinator of each SGA signed under the FPA and will always take to role of single contact point for the granting authority. All the other partners of the FPA can participate in any SGA. 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

Lump Sum Grant

Description: Lump Sum Grants 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). The granting authority defines a methodology for calculating the amount of the lump sum. There is an overall amount, i.e. the lump sum will cover the beneficiaries' direct and indirect eligible costs. 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: 50%

Payment model: Prefinancing – second (third) prefinancing (as there is no cost reporting) – 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 associated country, or established in the EU territory but *controlled* by a third country or third country legal entities (including associated countries)⁴¹.

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 EU MS or EU legal entities will be able to participate with no exceptions.
- In SO1 and SO2, entities controlled by third countries or third country legal entities may be able to participate if they comply with certain conditions set up in the Work Programme. To that end, additional rules will be imposed on those legal entities, which need to be followed if they want to participate.

The activation of this article will be 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.

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 reasons⁴².

The application of this article 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 the Guidance on ownership control restrictions in EU grants.

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

⁴² See Article 18(4) of the Digital Europe Regulation 2021/694.