



Digital Europe Programme (DIGITAL)

Call for proposals

Data space for security and law enforcement
DIGITAL-2022-DATA-SEC-LAW-03

Version 2.0
23 February 2023



HISTORY OF CHANGES			
Version	Publication Date	Change	Page
1.0	16.11.2022	▪ Initial version (new MFF).	
2.0	23.02.2023	▪ Includes the link to the results of the 'Study to support the technical, legal and financial conceptualisation of a European Security Data Space for Innovation'	9
		▪	
		▪	



EUROPEAN COMMISSION
Directorate-General for Communications Networks, Content and Technology

CNECT.G– Data
CNECT.G.1 – Data Policy and Innovation

CALL FOR PROPOSALS

TABLE OF CONTENTS

0. INTRODUCTION	5
1. BACKGROUND	6
2. OBJECTIVES — SCOPE — OUTCOMES AND DELIVERABLES — KPIS TO MEASURE OUTCOMES AND DELIVERABLES — TARGETED STAKEHOLDERS — TYPE OF ACTION — SPECIFIC TOPIC CONDITIONS	7
DIGITAL-2022-DATA-SEC-LAW-03-ENFORCE- Data space for security and law enforcement	7
Objectives	7
Scope	8
Outcomes and deliverables	8
KPIs to measure outcomes and deliverables	10
Targeted stakeholders	10
Type of action	10
Specific topic conditions	10
3. AVAILABLE BUDGET	11
4. TIMETABLE AND DEADLINES	11
5. ADMISSIBILITY AND DOCUMENTS	11
6. ELIGIBILITY	12
Eligible participants (eligible countries)	12
Consortium composition	14
Eligible activities	14
Geographic location (target countries)	14
Ethics	14
Security	15
7. FINANCIAL AND OPERATIONAL CAPACITY AND EXCLUSION	16
Financial capacity	16
Operational capacity	16
Exclusion	17

8. EVALUATION AND AWARD PROCEDURE	18
9. AWARD CRITERIA	19
10. LEGAL AND FINANCIAL SET-UP OF THE GRANT AGREEMENTS	20
Starting date and project duration	20
Milestones and deliverables	20
Form of grant, funding rate and maximum grant amount	20
Budget categories and cost eligibility rules	21
Reporting and payment arrangements	22
Prefinancing guarantees	23
Certificates	23
Liability regime for recoveries	23
Provisions concerning the project implementation	24
Other specificities	24
Non-compliance and breach of contract	25
11. HOW TO SUBMIT AN APPLICATION	25
12. HELP	26
13. IMPORTANT	27
ANNEX 1	30
ANNEX 2	33

0. Introduction

This is a call for proposals for EU **action grants** in the field of Cloud, Data and Artificial Intelligence 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 Commission, Directorate-General for Communication, Networks, Content and Technology (DG CONNECT)**.

The call covers the following **topic**:

- **DIGITAL-2022-DATA-SEC-LAW-03-ENFORCE** - Data space for security and law enforcement

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

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

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

- the [Call Document](#) outlines the:
 - background, objectives, scope, 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)
 - legal and financial set-up of the Grant Agreements (section 10)
 - how to submit an application (section 11).
- the [Online Manual](#) outlines the:

¹ Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe programme (OJ L166, 11.05.2021).

² Commission Implementing Decision C/2021/7914 of 10.11.2021 concerning the adoption of the work programme for 2021 - 2022 and the financing decision for the implementation of the Digital Europe Programme.

- 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*).

1. Background

The Specific Objective 2 of the Digital Europe Programme aims to reinforce the EU's core Artificial Intelligence (AI) capacities as a crucial driver for the digital transformation of the public and private sectors. The EU data strategy³ outlined the importance of building a thriving ecosystem of private actors to generate economic and societal value from data, while preserving high privacy, security, safety and ethical standards. It announced that the Commission will invest in a High Impact Project that will fund infrastructures, data-sharing tools, architectures and governance mechanisms for thriving data-sharing and Artificial Intelligence ecosystems.

To reach these objectives, three main interlinked work strands are foreseen in the first two years of implementation of the Digital Europe Programme:

- The deployment of **cloud-to-edge infrastructure and services** compliant with EU rules, notably on security, data protection and privacy and environmental aspects. Open-source by default, they will ensure fluid data flows. Completing the picture, the deployment of the Testing and Experimentation Facility for edge-AI will support the green transition with support to advanced low-power computing technologies. Such facility should be a role model in showing effective ways to comply with existing legislation, and taking into account relevant codes of conduct and guidelines.
- The deployment of a Data for EU strand with a focus on building **common data spaces**, based on the above federated cloud-to-edge infrastructure and services that are accessible to businesses and the public sector across the EU. The objective is the creation of data infrastructure with tailored governance mechanisms that will enable secure and cross-border access to key datasets in the targeted thematic areas. Focus will be on data spaces for Green deal, smart communities, mobility, manufacturing, agriculture, cultural heritage, health, media, skills, language technologies, financial sector, public administrations and tourism. Data spaces will be supported by a Data Space Support Centre in order to guarantee coordination between the various initiatives and guarantee that data could be accessed across different sectors. The centre will ensure the best use of the cloud-to-edge infrastructure and services to serve the needs of these data spaces.
- The deployment of **AI reference testing and experimentation facilities** with a focus on four prioritized application sectors (i.e. health, smart communities, manufacturing, and agriculture)⁴. These facilities will provide common, highly specialised resources to be shared at European level. In addition, the **AI-on-demand platform** will be consolidated as a catalogue of

³ Communication from the Commission, A European strategy for data; COM/2020/66 final

⁴ The Commission has worked intensively with Member States to refine to prioritise the four selected sectors (see also the [Coordinated Plan on Artificial Intelligence 2021 Review](#))

AI-based resources and marketplace, for trustworthy AI tools made in Europe for both private and public sector use.

The present call covers supports the deployment of the data ecosystem (second work strand).

All topics in this call are subject to the provisions of Article 12(6) of the Digital Europe Programme Regulation. All eligible entities should include in their proposal evidence on how they will address the underlying security issues, including, wherever relevant, measures to avoid falling under foreign jurisdiction obligations, and how they will deal with confidentiality of the information and include evidence of their security expertise. All selected entities implementing such actions shall have the obligation to prevent access by non-eligible third countries or by non-eligible third country entities to classified and non-classified sensitive information.

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

DIGITAL-2022-DATA-SEC-LAW-03-ENFORCE- Data space for security and law enforcement

Objectives

The objective is to deploy a common European Security data space for innovation allowing research, development, testing, training and validation of algorithms for AI-based systems for security (law enforcement) based on various types of datasets, including operational pseudonymized and anonymized datasets, following the data minimisation principle (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 – GDPR and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 - LED). Particular attention must be given to reducing potential bias in algorithms to be used by law enforcement.

Technological sovereignty of Member States and the EU in the field of fighting crime and terrorism in the digital age is a fundamental public interest as well as a matter of national security, and can be strengthened by creating high quality and trusted datasets that would enable Member States' Law Enforcement Agencies (LEAs) to develop and validate their own digital tools.

A dedicated common Data space for Security and law enforcement will satisfy both principles set in the "A European strategy for data"⁵: (1) that actions under data spaces for public administrations will also focus on data use for improving law enforcement in the EU in line with EU law, and (2) that data for the public good can serve to ensure more efficient fight against crime.

Namely, this data space would serve the interests of all stakeholders in charge of public or internal security, and in particular, the Member States' law enforcement authorities, authorities in charge of border security as well as the relevant European Agencies, such as Europol, the European Border and Coast Guard Agency, and eu-LISA (in accordance with the legal bases that apply to them). In such a way, the EU open strategic autonomy in the field of AI applications for law enforcement will be enhanced.

⁵ COM(2020) 66 final

The objective of the Data space for Security and law enforcement is solely to facilitate innovation, it should not cover data sharing for investigative purposes.

Scope

This action will lay the economic, organisational and technical foundations of a federated data infrastructure. Specifically, it is expected that at the end of the project a system and a model of the data governance will be available, thus the project will include the following tasks:

- to develop a reference architecture, to define data standards and to determine criteria for certifications and product quality while addressing ethical concerns and complying with data protection requirements. Standardisation of data should be proposed and the framework may be defined based upon the UMF (uniform message format) project defining data models in a number of areas, such as data on persons, firearms and vehicles;
- to generate, collect, annotate and make interoperable data suitable to test, train and validate algorithms, which should be available for the training, validation and testing of tools using AI technologies, and, when possible, proportional and where provided for by law, shareable for security research purposes. There should be a monitoring process to ensure the quality of the data and the validation of the results. It would focus in particular the technical standard and the content, i.e. that the data is not biased against ethnicity, gender, nationality or other social categories.
- The projects will have to deploy trust mechanisms (security and privacy by design), data services which ensure the identity of the source and receiver of data and which ensure the access and usage rights towards the data. Projects are encouraged to perform the study and analysis of alternatives for data collection with maximum efficiency in order to provide interoperability within the domain. Through this concept of a federated data infrastructure, we enable European security stakeholders to develop their potential in a dynamic security ecosystem. Projects under this action should pay specific attention to fundamental rights challenges notably by proposing adequate bias mitigation and non-discrimination mechanisms as well as by providing enhanced data quality. They should also demonstrate strict compliance with the EU legal framework on data processing for police purposes as set out in Directive 2016/680 of the European Parliament and the Council of 27 April 2016 and the GDPR. The projects will ensure appropriate coordination with relevant projects funded under the research Framework Programmes and, when applicable, EU Space programmes operating security services (Copernicus, Galileo).

The projects selected for the deployment of this data space will have to make provisions for gradually becoming fully compliant with the European Data Spaces Technical Framework. They will also have to coordinate and collaborate with other projects participating in the deployment of the data space and the Data Spaces Support Centre in order to build on common standards.

Outcomes and deliverables

The creation of a common data platform, including the national components and a communication infrastructure, with trusted datasets to train, test and validate algorithms aims to create sufficient quantity of data to research, innovate and develop AI technologies, with the objective to gather and analyse automatically big number of various types of information (pictures, reports, video etc.). The Data space for Security and law enforcement will create a data ecosystem specific for the needs of the security and immigration stakeholders, including national authorities, EU agencies in charge of European security and justice representatives. Private sector

representatives may benefit from a dedicated section of the Data space for Security and law enforcement containing anonymous datasets provided that they are carrying out security research under the European Framework Programmes for Research.

A common Data space for Security and law enforcement will substantially foster development of AI technologies, which will constitute a very important contribution to combat crime, enhance border security and facilitate legal migration.

It will also improve the European open strategic autonomy by allowing the national and European law enforcement authorities to develop and validate their own digital tools so to (i) eliminate the threat of malicious interference of third countries/parties; (ii) allow for setting quality standards at EU level and (iii) increase the technological capabilities of Member States LEAs. On this basis, foreign controlled entities participating in the action should only perform specific, clearly defined tasks and should not be involved in the design of the technical architecture or the security components of the product.

The following elements shall be delivered by the selected project:

- Reference architecture for a federated data space, integrating national components (allowing their interconnection with future central components, once these are developed) with the objective of allowing to train, test and validate algorithms.
- Components enabling interoperability between the national data infrastructure and the future central data infrastructure, once the latter is developed (e.g. APIs connecting to national data infrastructure where feasible). Alternatively, in cases where national data infrastructure for internal security does not exist, components facilitating the development of national data infrastructure, and its interoperability at EU level can be developed.
- Micro-services enabling the application of the principle of federated access to data sources and privacy-preserving linkage techniques (e.g. including secure multi-party computation approaches).
- A set of anonymised/pseudonymised, high-quality data sets that can be used for the development (training), testing and evaluation of algorithms of relevance for applications in the domain of internal security and border management, and a set of tools allowing for automated anonymization/pseudonymisation, as well as annotation of data sets relevant for the use cases in the area of internal security and border management. This point shall be addressed in complementarity with other work strands on the European Security Data Space for Innovation, including the calls under the Internal Security Fund Thematic Facility 2021-2022, in order to avoid overlaps and to seek for complementarities.
- Develop a set of best practices, for example focusing on interoperability, data governance, data quality management, as well as identify common standards (including domain-specific semantic standards and interoperability protocols).

Proposers should take into consideration the results of the 'Study to support the technical, legal and financial conceptualisation of a European Security Data Space for Innovation. The results of the study are now available here:

<https://home-affairs.ec.europa.eu/document/download/4ad85efa-cccf-41ac-a3c7-84d33b5102d7>

KPIs to measure outcomes and deliverables

- Number of national components developed across the EU Member States, according to minimal alignment and standards allowing interchangeability and possible combination of training data, through a private cloud.
- Number of national data infrastructures connected.
- Number of micro-services within the platform developed (which should provide proper SaaS, IaaS and PaaS).
- User satisfaction on usefulness and efficiency of the different elements of the cloud (including, for instance, data platform, application programming interfaces (API's), raw data, specific databased and classic data warehouse, separated innovation, testing and training environment, analytics functionalities, etc.).
- Number of best practises to be shared.
- Number of data sets that can be used for training, testing and evaluation of algorithms, which can be made available to other authorities operating in the area of internal security and border management in the EU and associated countries.

Targeted stakeholders

Law enforcement authorities from at least 2 Member States. The participation of additional law enforcement authorities from additional EU Member States is encouraged. In addition, private entities, or public and publicly-funded organisations, including research institutes from eligible countries are encouraged to participate.

Type of action

Simple Grants — 50% funding rate

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

Specific topic conditions

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

3. Available budget

The available call budget is **EUR 8 000 000**. This budget might be increased by maximum 20%.

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

Topic	Topic budget
DIGITAL-2022-DATA-SEC-LAW-03-ENFORCE	EUR 8.000.000,00

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

4. Timetable and deadlines

Timetable and deadlines (indicative)	
Call opening:	15 December 2022
<u>Deadline for submission:</u>	<u>16 March 2023 – 17:00:00 CET</u> <u>(Brussels local time)</u>
Evaluation:	May-June 2023
Information on evaluation results:	July 2023
GA signature:	December 2023

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 [Search Funding & Tenders](#) section). Paper submissions are NOT possible.

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

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


- Application Form Part A — contains administrative information about the participants (future coordinator, beneficiaries and affiliated entities) and the summarised budget for the project (*to be filled in directly online*)
- Application Form Part B — contains the technical description of the project (*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/calculator: not applicable
 - CVs of core project team: not applicable
 - activity reports of last year: not applicable
 - list of previous projects (key projects for the last 4 years): not applicable
 - **ownership control declaration: 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 are limited to maximum **70 pages** (Part B). Evaluators will not consider any additional pages.

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

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

6. Eligibility

Eligible participants (eligible countries)

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

- be legal entities (public or private bodies)
- be established in one of the eligible countries, i.e.:
 - EU Member States (including overseas countries and territories (OCTs))
 - non-EU countries:
 - listed EEA countries
 - countries associated to the Digital Europe Programme (list of [countries^{\(en\)}](#)) or countries which are in ongoing negotiations for an

association agreement and where the agreement enters into force before grant signature.⁶ All applicants from an associated countries have to present a guarantee approved by the country, to comply with the conditions set out in the work programme Annex 3.

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

Please be aware that **this call is subject to restrictions due to security**, therefore entities must not be directly or indirectly controlled from a country that is not an eligible country. **All entities⁷ have to fill in and submit a declaration on ownership and control.**

Moreover:

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

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 persons⁸.

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'⁹. ⚠ 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).

⁶ Proposals including entities from countries which are in ongoing negotiations for an association agreement that does not enter into force before the signature of the grant might be declared ineligible. In those cases the consortium will be asked to replace the participant concerned (or redistribute the tasks between the other participants). If this is not possible and the consortium cannot propose any other acceptable solution, the proposal will have to be rejected.

⁷ Except for entities that are validated as public bodies by the Central Validation Service.

⁸ See Article 197(2)(c) EU Financial Regulation [2018/1046](#).

⁹ For the definitions, see Articles 187(2) and 197(2)(c) EU Financial Regulation [2018/1046](#).

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 [EU restrictive measures](#) under Article 29 of the Treaty on the European Union (TEU) and Article 215 of the Treaty on the Functioning of the EU (TFEU)¹⁰ and entities covered by Commission Guidelines No [2013/C 205/05](#)¹¹*). Such entities are not eligible to participate in any capacity, including as beneficiaries, affiliated entities, associated partners, subcontractors or recipients of financial support to third parties (if any).

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

Consortium composition

Proposals must be submitted by:

- minimum 2 law enforcement authorities (beneficiaries; not affiliated entities) from at least 2 different EU Member States

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*).

Financial support to third parties is not allowed

Geographic location (target countries)

Due to restrictions due to security:

- the proposals must relate to activities taking place in the eligible countries (*see above*)

Ethics

Projects must comply with:

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

¹⁰ Please note that the EU Official Journal contains the official list and, in case of conflict, its content prevails over that of the [EU Sanctions Map](#).

¹¹ 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).

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](#)¹² and its implementing rules and/or national rules) provide for instance that:

- projects involving information classified TRES SECRET UE/EU TOP SECRET (or equivalent) can NOT be funded
- classified information must be marked in accordance with the applicable security instructions in the SAL
- information with classification levels CONFIDENTIEL UE/EU CONFIDENTIAL or above (and RESTREINT UE/ EU RESTRICTED, if required by national rules) may be:
 - created or accessed only on premises with facility security 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.

¹² 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).

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

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

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

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

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

- further information
 - an enhanced financial responsibility regime, i.e. joint and several responsibility for all beneficiaries or joint and several liability of affiliated entities (*see below, section 10*)
 - prefinancing paid in instalments
 - (one or more) prefinancing guarantees (*see below, section 10*)
- or
- propose no prefinancing
 - request that you are replaced or, if needed, reject the entire proposal.

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

Operational capacity

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

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

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

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

- general profiles (qualifications and experiences) of the staff responsible for managing and implementing the project
- description of the consortium participants
- list of previous projects (key projects for the last 4 years) for topics made applicable in section 5

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 participate¹³:

- bankruptcy, winding up, affairs administered by the courts, arrangement with creditors, suspended business activities or other similar procedures (including procedures for persons with unlimited liability for the applicant's debts)
- in breach of social security or tax obligations (including if done by persons with unlimited liability for the applicant's debts)
- guilty of grave professional misconduct¹⁴ (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

¹³ See Articles 136 and 141 of EU Financial Regulation [2018/1046](#).

¹⁴ 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.

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 that¹⁵:

- 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:

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.*

¹⁵ See Article 141 EU Financial Regulation [2018/1046](#).

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 [Funding & Tenders Portal Terms and Conditions](#)). Please also be aware that for complaints submitted electronically, there may be character limitations.

9. Award criteria

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

- **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 — but never earlier than the proposal submission date.

Project duration:

- 36 months

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

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 8 000 000** per project

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 cost¹⁶: Yes

¹⁶ Commission [Decision](#) of 20 October 2020 authorising the use of unit costs for the personnel costs of the owners of small and medium-sized enterprises and beneficiaries that are natural persons not receiving a salary for the work carried out by themselves under an action or work programme (C(2020)7715).

- travel and subsistence unit costs¹⁷: No (only actual costs)
- equipment costs:
 - depreciation + full cost for listed equipment
- other cost categories:
 - costs for financial support to third parties: not
 - 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
- EU Synergies call: No
 - restrictions due to security:
 - country restrictions for subcontracting costs: Yes, subcontracted work must be performed in the eligible countries
 - eligible cost country restrictions: Yes, only costs for activities carried out in eligible countries are eligible.

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).

¹⁷ Commission [Decision](#) of 12 January 2021 authorising the use of unit costs for travel, accommodation and subsistence costs under an action or work programme under the 2021-2027 multi-annual financial framework (C(2021)35).

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

All payments will be made to the coordinator.

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

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

Prefinancing guarantees

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

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

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

Prefinancing guarantees are 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: Yes
- exploitation 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: No
- special IPR obligations linked to restrictions due to security:
 - exploitation in eligible countries: Yes
 - first exploitation obligation in eligible countries: No
 - limitations to transfers and licensing: Yes

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

- communication and dissemination plan: Yes
- dissemination of results: Yes
- additional dissemination obligations: No
- 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
- special obligations linked to restrictions due to security:
 - implementation in case of restrictions due to security or EU strategic autonomy: Yes

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 [AGA — Annotated Grant Agreement](#).

11. How to submit an application

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

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

a) create a user account and register your organisation

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

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

b) submit the proposal

Access the Electronic Submission System via the Topic page in the [Search Funding & Tenders](#) 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 [Online Manual](#). The Online Manual also contains the links to FAQs and detailed instructions regarding the Portal Electronic Exchange System.

12. Help

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

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

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

Contact

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

Non-IT related questions should be sent to "[Write to us](#)"

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 (n/a for FPAs) — 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 (n/a for FPAs) — 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 (n/a for FPAs) — 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 [EU Financial Regulation](#), information about EU grants awarded is published each year on the [Europa website](#).

This includes:

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

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

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

Annex 1

Digital Europe types of action

The Digital Europe Programme 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 cash-flow 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 cash-flow 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 pre-financing and reporting obligations.

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

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

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

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

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 Grants

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)¹⁸.

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 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 reasons¹⁹.

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 [Guidance on participation in DEP, HE, EDF and CEF-DIG restricted calls](#).

¹⁸ See Article 12(5) and (6) of the Digital Europe Regulation 2021/694

¹⁹ See Article 18(4) of the Digital Europe Regulation 2021/694.