Connecting Europe Facility (CEF)

Call for proposals

CEF 2 Digital - Backbone networks for pan-European cloud federation (CEF-DIG-2021-CLOUD)

Version 2.0

14 March 2022

HISTORY OF CHANGES			
Version	**Publication Date**	**Change**	**Page**
1.0	12.01.2022	▪ Initial version (new MFF).	
2.0	14.03.2022	▪ Extension of call deadline to 20 April 2022 - 17:00:00 CEST	18
		▪	
		▪	

HEALTH AND DIGITAL EXECUTIVE AGENCY (HaDEA)

HaDEA B - Digital, Industry and Space
HaDEA B1 - Connecting Europe Facility - Digital

CALL FOR PROPOSALS

TABLE OF CONTENTS

0. Introduction 4
1. Background 5
2. Objectives — Scope (including digital security requirements) — Expected impact 7
2.1 CEF-DIG-2021-CLOUD-FED-WORKS — Interconnection of backbone networks for Cloud federations 7
Objectives 7
Scope 7
Digital security requirements 9
Expected impact 11
2.2 CEF-DIG-2021-CLOUD-OTHER-STUDIES — Interconnection of backbone networks for cloud federations with other Cloud, HPC and edge infrastructures 11
Objectives 11
Scope 11
Digital security requirements 12
Expected impact 12
2.3 CEF-DIG-2021-CLOUD-DNS-WORKS - Equipping backbone networks with high-performance and secure DNS resolution infrastructures - Works 12
Objectives 13
Scope 13
Digital security requirements 15
Expected impact 17
3. Available budget 17
4. Timetable and deadlines 18
5. Admissibility and documents 18
6. Eligibility 19
Eligible participants (eligible countries) 19
Consortium composition 20
Eligible activities 21
Geographic location (target countries) 21
Duration 21

Project budget....21
7. Financial and operational capacity and exclusion....21
Financial capacity....21
Operational capacity....22
Exclusion....22
8. Evaluation and award procedure....23
9. Award criteria....24
10. Legal and financial set-up of the Grant Agreements....25
Starting date and project duration....25
Milestones and deliverables....26
Form of grant, funding rate and maximum grant amount....26
Budget categories and cost eligibility rules....26
Reporting and payment arrangements....28
Prefinancing guarantees....28
Certificates....29
Liability regime for recoveries....29
Provisions concerning the project implementation....29
Other specificities....30
Non-compliance and breach of contract....30
11. How to submit an application....30
12. Help....31
13. Important....32

0. Introduction

This is a call for proposals for EU **action grants** in the field of "Cloud" under the Digital strand of the **Connecting Europe Facility (CEF)**.

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

- Regulation 2018/1046 (EU Financial Regulation)
- the basic act (CEF Regulation 2021/1153[1]).

The call is launched in accordance with the 2021-2025 Work Programme[2] and will be managed by the European Health & Digital Executive Agency (HaDEA) (hereafter 'the Agency').

The call covers the following **topics**:

- **CEF-DIG-2021-CLOUD-FED-WORKS — Interconnection of backbone networks for Cloud federations - Works**

[1] Regulation (EU) 2021/1153 of the European Parliament and of the Council of 7 July 2021 establishing the Connecting Europe Facility (OJ L 249, 14.7.2021, p. 38–81).

[2] Commission Implementing Decision C(2021) 9463 final of 16 December 2021 concerning the adoption of the work programme for 2021-2023 and the financing decision for the implementation of the Connecting Europe Facility (CEF).

- **CEF-DIG-2021-CLOUD-OTHER-STUDIES — Interconnection of Cloud federations with other Cloud, HPC and edge infrastructures - Studies**

- **CEF-DIG-2021-CLOUD-DNS-WORKS — Equipping backbone networks with high-performance and secure DNS resolution infrastructures - Works**

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.

NOTE: The term 'project' used in the call documentation is synonymous to the term 'action' used in the CEF Regulation 2021/1153.

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 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:
  - 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 the successful applicants will have to sign in order to obtain the grant *(including cost eligibility, payment schedule, accessory obligations, etc.)*.

1. Background

End users' tight budgetary constraints, the growing awareness of cloud impact on climate change, the relatively low cloud uptake among both the public and private sectors (18%)[3], and the need to enable the free flow of data across the EU are all fuelling the demand for federated cloud and edge infrastructures. Such infrastructures need to be interconnected in a highly secure, highly energy-efficient, and fully interoperable manner, respecting data protection and offering very low latency. This demand is driven by a technological shift in which cloud has become the technology underpinning the uptake of emerging technologies such as Artificial Intelligence (AI), Blockchain, Internet of Things (IoT) and High-Performance Computing (HPC).

Yet, the market for cloud services and infrastructure is highly concentrated among a limited number of companies. While some local alternatives exist at national level, none of the pan-European providers is European-owned. Similarly, DNS[4] resolution, a critical backbone function to access resources on the internet, is increasingly concentrated in the hands of a few non-European operators, creating overall internet resilience weaknesses, and potentially insecure in terms of guaranteeing privacy safeguards according to EU rules and protection from local cybersecurity threats (e.g. malware and phishing in local EU languages).

This situation is especially problematic for public administrations or public and private entities entrusted with the operation of services of general interest (SGIs[5]) or of Services of General Economic Interest (SGEIs[6]) as well as critical infrastructures, who are in need for particularly robust and secure backbone networks and interconnection services such as DNS resolution. Their respective infrastructures are not properly interconnected and alternative (sub)contractors which could provide such services are either too small or not in line with their high demands in terms of data management [7].

Answering this challenge, in its Data Strategy of February 2020[8], the European Commission committed to invest in a High Impact Project on European data spaces, and federated cloud-to-edge infrastructures and services.

Together with the Digital Europe programme, InvestEU and the Recovery and Resilience Fund (RRF), the CEF Digital programme, and specifically this call, will be the catalyst to deploy cross-border and national cloud-to-edge infrastructure interconnections at both the physical (i.e. very high capacity networks) and functional levels (i.e. DNS resolution, management systems and software-defined infrastructures) among socio-economic drivers (SED) across the EU to the benefit of

---

3 Only 1 company in 4 and 1 in 5 SME are using cloud computing in the EU according to the 2019 Digital Economy and Society Index (DESI)

4 The Domain Name System is the system allowing connecting a domain name to a resource on the internet, like a website or an application server.

5 Commission Notice on the notion of State aid as referred to in Article 107(1) of the Treaty on the Functioning of the European Union, OJ C 262, 19.7.2016, p. 1–50

6 See the Communication from the Commission on the application of the European Union State aid rules to compensation granted for the provision of services of general economic interest Official Journal C8, 11.01.2012, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012XC0111(02), and the Commission Decision of 20 December on the application of Article 106(2) of the Treaty on the Functioning of the European Union to State aid in the form of public service compensation granted to certain undertakings entrusted with the operation of services of general economic interest Official Journal L7, 11.01.2012, p. 3-10, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32012D0021

7 https://digital-strategy.ec.europa.eu/en/news/study-economic-detriment-smes-unfair-and-unbalanced-cloud-computing-contracts

8 COM(2020) 66 final https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

EU citizens and businesses. Within the context of this call, socio-economic drivers are public administrations or public or private entities entrusted with the operation of SGIs or of SGEIs.

The associated architectural requirements to enable security, safety, energy and resource efficiency, data protection and interoperability of those interconnections is also an inherent part of this call.

2. Objectives — Scope (including digital security requirements) — Expected impact

2.1 CEF-DIG-2021-CLOUD-FED-WORKS — Interconnection of backbone networks for Cloud federations

Objectives

CEF Digital aims to stimulate the commercial offering of cloud services throughout the EU. The cloud capacity will be strengthened and users will have access to multiple computing resources as a result of the projects supported by CEF.

This topic will support the deployment of Gigabit links for the interconnection between Socio-economic drivers that are public administrations or public or private entities entrusted with the operation of SGIs or of SGEIs and backbone networks for cloud federations. Market forces are not providing sufficient answers to the challenge of adequate interconnection with cloud providers. The deployments will take place where existing infrastructure cannot satisfy proper seamless functioning of resources from different providers, and also where there is a lack of the necessary redundancy to guarantee the reliability and resilience of cloud connectivity that can ensure adequate, safe and secure connectivity for the Gigabit society.

Scope

This topic will support the deployment of new and significant upgrade of cloud interconnections, for which the market alone will not invest, because such an investment would not be commercially viable, i.e. where no relevant direct link of the same characteristics exists or is planned in the near future.

In addition, for links within Member States, to be eligible for funding under this call, projects must (i) address a market failure which cannot be solved by regulatory measures, (ii) avoid crowding out private investments or unduly distorting competition.

The topic will support the investment costs (studies, works and equipment) related to the development and deployment of cross-border and national cloud infrastructure interconnections at both the physical (i.e. very high capacity networks) and functional levels (i.e. management systems, and software-defined infrastructures) for public administrations or public and private entities entrusted with the operation of SGIs or of SGEIs[9] across the EU.

The applicants may apply for grants for works, including studies:

[9] Services of general economic interest (SGEI) are economic activities that public authorities identify as being of particular importance to citizens and that would not be supplied (or would be supplied under different conditions) if there were no public intervention. The concept may apply to different situations and terms, depending on the Member States, but SGEIs can typically range from activities such as postal services, energy supply, or public transport, to social services, such as care for the elderly and disabled or hospitals being part of national health service, to public education organised within the national educational system funded and supervised by the State. See footnote 6.

- For works, the total project costs required to construct, long-term lease and deliver the described networking solution for the foreseen system lifetime, from end to end, including the on-premises portion.
- Any costs for operating the infrastructure during the lifetime and extra components after the arrival on premises such as cloud resources not necessary to support the links, hosting facilities and other services, after the end of the project, will be excluded under the call.
- For studies, all preparatory work required prior to signing a contract with a supplier is covered under this call. Studies specifically include topographic definition of the links for required permits and rights of way.

The end users will be public administrations or public and private entities entrusted with the operation of SGIs or SGEIs.

All proposals must define the post-project ownership of the infrastructure and describe the mechanism to be used to provide services, including business models. In particular, any arrangements for providing services on a non-discriminatory basis to different clouds, as well as the operational relationship(s) between the different participants in the value chain for providing services should be elaborated in the proposal. They should also provide the necessary security commitments to ensure the continuity of the level of security required during the implementation phase and explain how operators of essential services related to connectivity involved in the cross-border interconnection of national cloud infrastructures address the cybersecurity risks mentioned below.

In this context, proposals under this topic should address these federated cloud-to-edge infrastructures 'as a product' and will need to:

1. Cope with the latest digital and sustainability challenges, in particular:
   - enabling the industrial and low power processing of large amounts of data including in HPCs and at the edge;
   - fostering a swift and sustainable uptake of emerging technologies such as AI applications;
   - supporting the operationalisation of data spaces and specific use cases for socio-economic drivers;
2. Respond dynamically to needs of beneficiaries by providing data processing and storage capacities across the EU including at the edge at high speed, with low latency and in an energy and resource efficient manner;
3. Leverage high-performance end-to-end backbone connectivity;
4. Meet EU data protection, security, portability and environmental requirements; and anticipate forthcoming rules pursuant to the legislative work programme of the European Commission, notably the Data Governance Act[10], Digital Services Act[11], Digital Market Act[12] and the Data Act[13].

In their proposals, applicants will need to demonstrate that they adhere to the data protection, security, portability and energy and resource efficiency requirements applicable to data-processing/storage services and activities developed under the

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[11] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN

[12] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

[13] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act

relevant European codes of conduct, initiatives and legislation[14]. Participants should also demonstrate that they have put in place all reasonable technical, legal and organisational measures in order to prevent transfer or access – including unsolicited transfers or access - to personal or non-personal data (including processed data and meta-data) held in the Union that would be unlawful under Union law or applicable national law.

This topic is complementary to the actions foreseen under the Digital Europe Programme (DEP)[15], which focuses on the deployment at large-scale of the next generation of European cloud to edge services, the associated EU marketplace, and modular middleware platforms for interoperability between different data services.

Where applicable, proposals can as well be combined with the RRF in line with State aid rules as relevant, where CEF Digital is used to e.g. interconnect stakeholders across borders and RRF is used to complement with intra-national cloud infrastructure investments.

Proposals should also explain how operators of essential services related to connectivity involved in the cross-border interconnection of national cloud infrastructures address the cybersecurity risks.

Specific measures addressing green policy objectives, in particular in terms of reducing the carbon footprint, will be taken into account during the evaluation of proposals.

No State aid approval is required, if no state resources are used to co-finance the project. Applicants can find information on when State aid applies and whether it needs to be notified for cloud and edge investment in the State aid Cloud Capabilities Guiding Document[16].

Proposals funded under this topic may include synergetic (ancillary) elements relating to another sector of the CEF programme, i.e. energy and transport, if these synergetic elements allow to significantly improve the socio-economic, climate or environmental benefits of the action. CEF co-funding may be provided as long as the cost of these synergetic elements does not exceed 20% of the total eligible costs of the action.

Digital security requirements

In view of the particular sensitivity of cloud infrastructures from a security perspective and the importance to reduce exposure to risks to the maximum possible extent, proposals under this topic are subject to strict exclusion of non-EU controlled entities, under the Article 11.4 of the CEF Regulation 2021/1153[17].

The assessment of the foreign (non-EU) control will be addressed during the eligibility phase of the evaluation of proposals. Participants will be requested to submit an ownership control questionnaire for this purpose to determine their control status.

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0694

[16] https://ec.europa.eu/competition/state_aid/what_is_new/template_RFF_cloud_capabilities.pdf

[17] Art. 11 (4) of the CEF Regulation 2021/1153: "*The work programmes may provide that legal entities established in third countries associated to the CEF in accordance with Article 5, and legal entities established in the Union but directly or indirectly controlled by third countries or nationals of third countries or by entities established in third countries, are not eligible to participate in all or some of the actions under the specific objectives set out in Article 3(2), point (c), for duly justified security reasons. In such cases, calls for proposals and calls for tenders shall be restricted to entities established, or deemed to be established, in Member States and directly or indirectly controlled by Member States or by nationals of Member States.*"

They will also be requested to submit supporting documents in order for the Commission to determine that the entities are not controlled by a third country.

All proposals submitted to this topic, to be eligible, must include security declarations by the participating entities, which demonstrate that the network technologies and equipment (including software and services) funded by the project will comply with security requirements as specified in this call conditions, in accordance with the applicable EU law, national law, and EU guidance on cybersecurity[18]; and indicate that no security sensitive equipment or services deployed or used within the proposal will be procured from third country suppliers[19,20]. The content of these declarations will be assessed during the evaluation phase.

Proposals for this topic, must address, in the digital security section in the application form, the following risk scenarios and mitigating measures as described in the 5G networks EU Toolbox of risk mitigating measures[21]:

- involvement of high risk suppliers (as defined in the EU coordinated risk assessment on cybersecurity of 5G networks); restrictions applied against such suppliers for critical and sensitive key assets and measures to avoid dependency on such high risk suppliers;
- measures to promote supply chain resilience and strategic autonomy (in line with the 5G networks EU Toolbox of risk mitigating measures);
- security requirements for your network operators *(e.g.* strict access controls, rules on secure operation and monitoring, limitations on outsourcing of specific functions, etc.);
- measures adopted to prevent unsolicited transfer to, or access by, third parties of the data (personal or non-personal) stored or transported in the context of the project.

Based on the security declarations in the proposals, as well as the evaluation carried out by independent experts, the Commission or Agency, where appropriate, may carry out a follow-up assessment of the fulfilment of the security conditions in the declaration, including as regards beneficiaries' suppliers and sub-contractors. Funding for actions, which do not comply with the conditions related to security, may be suspended, terminated, or reduced at any time in accordance with the Financial Regulation.

---

[18] Such as: the Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks, C/2019/2335; the Report on EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks of 9 October, 2019; the Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G of 3 December, 2019; the Cybersecurity of 5G networks - EU Toolbox of Risk Mitigating Measures of 29 January, 2020; and COM(2020)50 of 29 January 2020 on Secure 5G deployment in the EU – implementing the toolbox.

[19] According to the EU coordinated risk assessment, the risk profiles of individual suppliers can be assessed based on several factors. These factors include the likelihood of interference from a third country. This is one of the key factors specified in paragraph 2.37 of the EU coordinated assessment.

[20] In particular, telecom operators may rely on third party entities to perform certain tasks, such as the maintenance and upgrade of the networks and software, as well as other outsourced managed services, in addition to the supply of network equipment. This may constitute a source of security risk. Thus, a thorough security assessment may also be required of the risk profile of the suppliers tasked with these services, in particular when these tasks are not performed in the EU.

[21] Principles underlined in the 5G toolbox and the related measures apply mutatis-mutandis to backbone infrastructures.

For further background on security requirements, please see sections 8.2, 8.3 and 8.4 as well as sections 2 (paragraph "Strengthen cybersecurity and resilience") and section 3.2.3 of the CEF Digital Work Programme.

Expected impact

The call aims to result in the following key benefits:

a) providing the key data processing infrastructures to support the digital transformation and modernisation of the public sector in Europe;

b) increased competitiveness and resilience of the EU computing industry in line with EU rules on data protection, security, portability and sustainability;

c) technological autonomy in essential digital computing infrastructures to process EU data, in particular through European common dataspaces; the infrastructure will also be an essential enabler for the roll-out of emerging technologies, including AI, IoT, HPC;

d) energy efficiency and sustainable large scale deployment of interconnected cloud-to-edge infrastructures across the EU territory.

Additionally, the expected benefits relate to addressing market failures by allowing cloud providers to act federated simulating the capacity of a cloud hyperscaler. Thus, they will contribute to bringing Digital autonomy to the EU and ensure widespread access to the Gigabit Society for all EU citizens and businesses.

The key performance indicators for the topic are:

- the sum of the bandwidth-distance product[22] of each deployed link (in Gb/s*Km) created between cloud providers;
- the number of data centres of socio-economic drivers, including public-sector, which will be interconnected physically (fibre) or virtually (new software or middleware deployment).

2.2 CEF-DIG-2021-CLOUD-OTHER-STUDIES — Interconnection of backbone networks for cloud federations with other Cloud, HPC and edge infrastructures

Objectives

Federated cloud infrastructures will gradually need to be interconnected with other cloud, HPC and edge infrastructures. The objective of this topic is to fund feasibility studies for these interconnections to anticipate the technical, legal and economic requirements to progressively establish a fully secured and highly energy-efficient European computing continuum.

The studies funded under this topic should cover future investment needs and required technology for the interconnection of cloud, HPC and edge infrastructures. The priority is the identification of shortages that prevent the EU from holding digital independence while participating from the existing technological status quo.

Scope

The applicants may apply for grants for studies, including the following activities:

[22] https://www.rp-photonics.com/bandwidth_distance_product.html

- Analysis of investment needs related to the development and deployment of cross-border and national cloud infrastructure interconnections at both the physical (i.e. very high capacity networks) and functional levels (i.e. management systems, software-defined infrastructures) for public sector end-users and private actors operating data infrastructures for services of general public interest across the EU.

- Analysis of economic sovereignty of deployed alternatives. This covers the analysis of total cost of ownership and of the relevant items that result in the extraction of the funding from the required value-chains.

- Analysis of technological needs relevant for the interconnection of the aforementioned networks and resources.

The end users will be public administrations or public and private entities entrusted with the operation of SGIs or SGEIs.

Digital security requirements

In view of the particular sensitivity of cloud infrastructures from a security perspective and the importance to reduce exposure to risks to the maximum possible extent, proposals under this topic are subject to strict exclusion of non-EU controlled entities, under the Article 11.4 of the CEF Regulation[23].

The assessment of the foreign (non-EU) control will be addressed during the eligibility phase of the evaluation of proposals. Participants will be requested to submit an ownership control questionnaire for this purpose to determine their control status. They will also be requested to submit supporting documents in order for the Commission to determine that the entities are not controlled by a third country.

Expected impact

The call aims to result in the following key benefits:

a) Investment roadmap for achieving a robust cloud federation network in the EU with increased competitiveness and resilience of the EU computing industry in line with EU rules on data protection, security, portability and sustainability.

b) Roadmap for developing key building blocks to achieve technological autonomy in essential digital computing infrastructures to process EU data, in particular through European common dataspaces. The technological roadmap should also include the needs for the roll-out of emerging technologies, including AI, 'internet of things' (IoT), HPC in the aforementioned interconnections.

c) Requirements definition for energy efficiency and sustainable large scale deployment of interconnected cloud-to-edge infrastructures across the EU territory.

[23] Art. 11 (4) of the CEF Regulation2021/1153: "*The work programmes may provide that legal entities established in third countries associated to the CEF in accordance with Article 5, and legal entities established in the Union but directly or indirectly controlled by third countries or nationals of third countries or by entities established in third countries, are not eligible to participate in all or some of the actions under the specific objectives set out in Article 3(2), point (c), for duly justified security reasons. In such cases, calls for proposals and calls for tenders shall be restricted to entities established, or deemed to be established, in Member States and directly or indirectly controlled by Member States or by nationals of Member States.*"

2.3 CEF-DIG-2021-CLOUD-DNS-WORKS - Equipping backbone networks with high-performance and secure DNS resolution infrastructures - Works

Objectives

This topic will support the deployment of a recursive European DNS resolver service infrastructure (hereafter DNS4EU) serving socio-economic drivers, public, corporate and residential internet end-users in the EU, and offering very high reliability and protection against global cybersecurity threats and those specific to the EU (e.g. phishing in EU languages). This is a key policy action announced in the 2020 "Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade"[24]. Such a critical service infrastructure is currently not available at European level with the level of performance, resilience, security and privacy envisaged, and the market will not invest in it alone given the lack of a business case (DNS resolution is normally provided for free). As stated the EU's Cybersecurity Strategy, citizens and organisations in the EU increasingly rely on a few public DNS resolvers operated by non-EU entities. The deployment of DNS4EU aims to address such consolidation of DNS resolution in the hands of few companies, which renders the resolution process itself vulnerable in case of significant events affecting one major provider. Moreover the lack of significant EU investment in the field hampers the development of infrastructures that favour the detection and filtering of local cyber-threats that nonetheless could have significant socio-economic impacts. In addition, the processing of DNS data can have an impact on privacy and data protection rights.

DNS4EU shall offer a high level of resilience, global and EU-specific cybersecurity protection, data protection and privacy according to EU rules, ensure that DNS resolution data are processed in Europe and personal data are not monetised. It shall adhere to the latest internet security and privacy standards. It shall be widely discoverable and easy to configure by end-users on their equipment and software.

The service infrastructure shall offer additional optional services such as free parental control, as well as paid premium services for enhanced performance or security for corporate users.

Scope

The proposal for this topic shall meet the following requirements at the level of users and services:

1. *Customer base*: Support the deployment of a recursive European DNS resolver service infrastructure serving EU-based internet users in need of privacy-respecting and secure DNS resolution to access resources on the internet. These users encompass socio-economic drivers, actors operating data and cloud infrastructures across the EU, public and private corporate users, and residential internet end-users in the EU. The proposal shall aim at a high adoption rate by addressing multiple customer bases (e.g. residential, education, governments, and vertical sectors).

2. *Availability and service level*: Provide wide geographic coverage in the EU, and ensure high reliability and uptime, as well as low latency of DNS resolution through among others a large distributed footprint (Points of Presence) and redundancy.

3. *Accessibility:* Ensure broad accessibility from user equipment, such as home routers and user devices, as well as from user software, such as major operating

[24] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

systems and browsers. DNS4EU shall be easy to configure by non-experts thanks to clear user guides and other support material available, including in audio-visual format, via a dedicated website under a clearly branded URL. The website shall contain all the relevant technical, legal and transparency-related information (e.g. protection of privacy, technical use of data) of the service.

4. *Discoverability*: The service shall be widely discoverable by major browsers, operating systems or user equipment. To this end it will be important to engage with industry groups (e.g. web browsers, ISPs), with the DNS standardisation community (e.g. DNS over HTTPS (DoH)) and other stakeholders.

5. *Premium and wholesale services*: Provide opt-in paid premium services for enhanced security (e.g. ad hoc filtering, monitoring, 24x7 support), tailored to specific sectorial needs (e.g. cloud, finance, health, transport), as well as wholesale resolution services for other digital service providers, including ISPs and cloud service providers.

6. *Residential services*: Offer to residential internet end-users strictly opt-in and fully transparent parental control filtering services. Other possible URL filtering services could also be offered in a strictly opt-in and fully transparent way. Such optional filtering shall be fully in line with national and EU rules (see below).

The proposal for the service infrastructure shall comply with the following security and privacy requirements and standards:

7. *Security*: State-of-the-art protection against cybersecurity threats by blocking malware, phishing and other threats based on reliable and up to date global threat feeds and own threat feeds developed on the basis of own threat detection and analysis as well as information exchange with trusted partners (e.g. CERTs), addressing in particular local threats (e.g. based on EU-languages). The corresponding threat detection and analysis infrastructure should be an integral part of the DNS4EU service infrastructure and provide a very high level of protection in the EU.

8. *Data processing*: Data processing shall be established through transparent and published policy and rules, in full compliance with EU rules (see below). DNS resolution data and meta-data shall be processed in the EU. There shall be no monetisation of personal data. Potential use of aggregated data (e.g. for cybersecurity analysis) shall be specified and made transparent.

9. *Internet Standards*: The service infrastructure shall conform to the latest security and privacy-enhancing standards (e.g. HTTPS, DNSSEC), including DNS encryption (e.g. DNS over TLS (DoT) and DoH) and be fully IPv6 compliant.

10. *Best practices:* Notwithstanding other requirements of this call or applicable law, the service infrastructure should be designed in line with industry best practices and guidelines for the provision of secure and privacy-preserving DNS resolution

The proposal for the service infrastructure shall comply with EU regulation and applicable national regulations of its Member States, in particular:

11. *Data protection and privacy:* Compliant with GDPR[25] and national rules, where applicable.

[25] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

12. *Lawful filtering:* Filtering of URLs leading to illegal content based on legal requirements applicable in the EU or in national jurisdictions (e.g. based on court orders), in full compliance with EU rules.

The proposal for the service infrastructure shall ensure a forward looking approach regarding technological innovation:

13. *Technology/Innovation:* The selected consortium will be expected to test and deploy innovative technologies, including the latest DNS security and privacy-enhancing technologies and technologies for the development and improvement of cybersecurity threat feeds, in collaboration with third-party innovators.

Priority will be given to proposals addressing the following aspects:

14. *Governance/Federated structure:* A federated and expandable service infrastructure with a diverse membership is preferred in order to maximise the footprint and customer base of DNS4EU across the EU, reduce costs through shared resources and ensure the long-term sustainability of DNS4EU.

The applicants may apply for grants for works, including studies. The grants are for:

- project costs (e.g. studies, works and equipment) related to the development, construction and deployment of cross-border and national DNS resolution infrastructure at physical and functional levels for the foreseen system lifetime;
- other equipment, goods, works and services necessary to support the infrastructure services.

Costs for operating the infrastructure during its lifetime will be excluded under the call.

Proposals funded under this topic may include synergetic (ancillary) elements relating to another sector of the CEF programme, i.e. energy and transport, if these synergetic elements allow to significantly improve the socio-economic, climate or environmental benefits of the action. CEF co-funding may be provided as long as the cost of these synergetic elements does not exceed 20% of the total eligible costs of the action.

Digital security requirements

In view of the particular sensitivity of DNS infrastructures from a security perspective and the importance to reduce exposure to risks to the maximum possible extent, proposals under this topic are subject to strict exclusion of non-EU controlled entities, under the Article 11.4 of the CEF Regulation[26].

The assessment of the foreign (non-EU) control will be addressed during the eligibility phase of the evaluation of proposals. Participants will be requested to submit an ownership control questionnaire for this purpose to determine their control status.

[26] Art. 11 (4) of the CEF Regulation 2021/1153: "*The work programmes may provide that legal entities established in third countries associated to the CEF in accordance with Article 5, and legal entities established in the Union but directly or indirectly controlled by third countries or nationals of third countries or by entities established in third countries, are not eligible to participate in all or some of the actions under the specific objectives set out in Article 3(2), point (c), for duly justified security reasons. In such cases, calls for proposals and calls for tenders shall be restricted to entities established, or deemed to be established, in Member States and directly or indirectly controlled by Member States or by nationals of Member States.*"

They will also be requested to submit supporting documents in order for the Commission to determine that the entities are not controlled by a third country.

All proposals submitted to this topic, to be eligible, must include security declarations by the participating entities, which demonstrate that the network technologies and equipment (including software and services) funded by the project will comply with security requirements as specified in this call conditions, in accordance with the applicable EU law, national law, and EU guidance on cybersecurity[27]; and indicate that no security sensitive equipment or services deployed or used within the proposal will be procured from third country suppliers[28][29]. The content of these declarations will be assessed during the evaluation phase.

Proposals for this topic, must address, in the digital security section in the application form, the following risk scenarios and mitigating measures as described in the 5G networks EU Toolbox of risk mitigating measures:

- involvement of high risk suppliers (as defined in the EU coordinated risk assessment on cybersecurity of 5G networks); restrictions applied against such suppliers for critical and sensitive key assets and measures to avoid dependency on such high risk suppliers;
- measures to promote supply chain resilience and strategic autonomy (in line with the 5G networks EU Toolbox of risk mitigating measures);
- security requirements for your network operators *(e.g. strict access controls, rules on secure operation and monitoring, limitations on outsourcing of specific functions, etc.);*
- measures adopted to prevent unsolicited transfer to, or access by, third parties of the data (personal or non-personal) stored or transported in the context of the project.

Proposals should also define the post-project ownership of the infrastructure and provide the necessary security commitments to ensure the continuity of the level of security required during the implementation phase, as well as the operational relationship(s) between the different participants in the value chain. They should explain how operators of essential services related to connectivity involved in the cross-border interconnection of national cloud infrastructures address the cybersecurity risks.

Based on the security declarations in the proposal, as well as the evaluation carried out by independent experts, the Commission or Agency, where appropriate, may carry out a follow-up assessment of the fulfilment of the security conditions in the declaration, including as regards beneficiaries' suppliers and sub-contractors. Funding

[27] Such as: the Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks, C/2019/2335; the Report on EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks of 9 October, 2019; the Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G of 3 December, 2019; the Cybersecurity of 5G networks - EU Toolbox of Risk Mitigating Measures of 29 January, 2020; and COM(2020)50 of 29 January 2020 on Secure 5G deployment in the EU – implementing the toolbox.

[28] According to the EU coordinated risk assessment, the risk profiles of individual suppliers can be assessed based on several factors. These factors include the likelihood of interference from a third country. This is one of the key factors specified in paragraph 2.37 of the EU coordinated assessment.

[29] In particular, telecom operators may rely on third party entities to perform certain tasks, such as the maintenance and upgrade of the networks and software, as well as other outsourced managed services, in addition to the supply of network equipment. This may constitute a source of security risk. Thus, a thorough security assessment may also be required of the risk profile of the suppliers tasked with these services, in particular when these tasks are not performed in the EU.

for actions, which do not comply with the conditions related to security, may be suspended, terminated, or reduced at any time in accordance with the Financial Regulation.

For further background on security requirements, please see sections 8.2, 8.3 and 8.4 as well as sections 2 (paragraph "Strengthen cybersecurity and resilience") and section 3.2.3 of the CEF Digital Work Programme.

Expected impact

The deployment and wide use of DNS4EU will have the following key benefits:

a) Offer a high-end alternative to existing dominant non-EU public resolvers, leading to a more resilient, more secure and diversified DNS resolution offering for EU internet users.

b) Autonomy of DNS resolving, diminishing the dependency on major public resolvers established outside the EU, and reducing vulnerability to outages of these resolvers.

c) Complete safeguards for EU internet users that their data and privacy are protected and handled according to EU rules.

d) Increased protection against malicious activities based on both global and local (EU) threat feeds and intelligence.

e) Testing and deploying innovative technologies to enhance internet access security and privacy.

For more information about the call, *see https://hadea.ec.europa.eu/calls-proposals_en*.

3. Available budget

The available call budget is **EUR 80 000 000**. This budget might be increased by maximum 20% of the budget of the multiannual plan.

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

Topic	Topic budget
CEF-DIG-2021-CLOUD-FED-WORKS	**EUR 65 000 000**
CEF-DIG-2021-CLOUD-OTHER-STUDIES	**EUR 1 000 000**
CEF-DIG-2021-CLOUD-DNS-WORKS	**EUR 14 000 000**

For the topic CEF-DIG-2021-CLOUD-OTHER-STUDIES the available funding per topic will be attributed to one action.

For the topic CEF-DIG-2021-CLOUD-DNS-WORKS the available funding per topic will be attributed to one action.

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

4. Timetable and deadlines

Timetable and deadlines (indicative)	
Call opening:	12 January 2022
Deadline for submission:	20 April 2022 – 17:00:00 CEST (Brussels)
Evaluation:	May-July 2022
Information on evaluation results:	August 2022
GA signature:	November/December 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 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)*
- Part C (to be filled in directly online, *for works topic only*) containing additional project data
- **mandatory annexes and supporting documents** *(to be uploaded)*:
  - detailed budget table per WP *(template available in the Submission System)*
  - activity reports of last year (unless exempted from operational capacity check; *see section 7*)
  - list of previous projects (key projects for the last 4 years) *(template available in Part B)*
  - timetable/Gantt chart *(template available in the Submission System)*
  - letters of support (MS agreement) *(template available in the Submission System)*

- ownership control questionnaire *(template available in the Submission System)*
- security declaration (*for works proposals, to be uploaded in the Submission System in "Other annexes"*)
- other annexes.

Please note that the amounts entered into the summarised budget table (filled in directly online) must correspond to the amounts calculated in the detailed budget table. In case of discrepancies, the amounts in the online summarised budget table will prevail.

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 **120 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)).

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

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

Please note however that this call is subject to restrictions due to security reasons. This means that only the EU Member States are eligible countries and entities must not be directly or indirectly controlled from a country that is not an eligible country.

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 eligible. The rules on eligible countries do not apply to them.

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 persons[30].

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

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)[31] and entities covered by Commission Guidelines No 2013/C 205/05[32])*. 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:

for the topic CEF-DIG-2021-CLOUD-OTHER-STUDIES:

- n/a

for the topics CEF-DIG-2021-CLOUD-FED-WORKS and CEF-DIG-2021-CLOUD-DNS-WORKS:

- minimum 3 applicants (beneficiaries; not affiliated entities) from 3 different eligible countries.

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

[31] 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.

[32] 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 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)

Proposals must relate to activities taking place in the eligible countries *(see above)*.

Duration

Projects for topics CEF-DIG-2021-CLOUD-FED-WORKS and CEF-DIG-2021-CLOUD-DNS-WORKS should normally range up to 36 months, for CEF-DIG-2021-CLOUD-OTHER-STUDIES up to 12 months (extensions are possible, if duly justified and through an amendment).

Project budget

Project budgets (maximum grant amount) are expected to be around:

CEF-DIG-2021-CLOUD-OTHER-STUDIES: EUR 1 000 000

CEF-DIG-2021-CLOUD-DNS-WORKS: EUR 14 000 000

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 'Quality' 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 this 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:

- description of the consortium participants
- applicants' activity reports of last year
- list of previous projects (key projects for the last 4 years).

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

Public bodies, Member State organisations, and international organisations are exempted from the operational capacity check.

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 participate[33]:

- 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)

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

- guilty of grave professional misconduct[34] (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, decisionmaking- 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, decisionmaking- 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, decisionmaking- 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 that[35]:

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

8. Evaluation and award procedure

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

An **evaluation committee** (assisted by independent outside experts) will assess all applications. Proposals will first be checked for formal requirements (admissibility, and eligibility, *see sections 5 and 6*). Proposals found admissible and eligible will be evaluated (for each topic) against the operational capacity and award criteria (3 phases: individual evaluation, consensus phase and panel review) and then ranked according to their scores *(see sections 7 and 9)*.

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

1) Score obtained under the 'Priority and urgency' criterion

[34] 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.

[35] See Article 141 EU Financial Regulation 2018/1046.

2) Score obtained under the 'Relevance and maturity' criterion

3) Score obtained under the 'Catalytic effect' criterion

4) Score obtained under the 'Impact' criterion

5) Score obtained under the 'Quality' criterion.

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. Proposals that are below the budget threshold (i.e. passed, but not ranked high enough to receive funding) will be awarded a Seal of Excellence.

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 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:

- **Priority and urgency:** evaluating correspondence of the proposal with the sectoral policy objectives and priorities, measuring its EU added-value and, where applicable, assessing the possible synergies with other sectors or CEF Digital topics and ensuring a geographical balance of the CEF digital support in the respective area. (5 points)

- **Maturity:** assessing the maturity of the action in the project development. The criterion will measure, among others, i) the readiness/ability of the project to start by the proposed start date and to complete by the proposed end date, ii) the status and planning of the contracting procedures and the necessary permits, and iii) information on the availability of the financial resources needed to complement the CEF investment (5 points)

- **Quality:** evaluating the soundness of the implementation plan proposed, both from the technical and financial point of view, the architecture and design approach, the organisational structures put in place (or foreseen) for the implementation, the risk analysis, the control procedures and quality management and the communication strategy. Moreover, when applicable, it will also assess the information related to the operations/maintenance strategy proposed for the completed project (5 points)

- **Impact:** assessing, when applicable, the economic, social, competition and environmental impact, including the climate impact, and other relevant externalities. This criterion may be substantiated by a Cost Benefit Analysis

(CBA), in which case the evaluation will look at the soundness, comprehensiveness, and transparency of the analysis as well as proposed means to monitor its impact. The criterion will also assess the safety, security, cybersecurity of telecommunication networks, interoperability and accessibility aspects of the proposal, innovation and digitalisation, as well as its cross-border dimension, and contribution to network integration and territorial accessibility, including particular for Outermost Regions and islands. Moreover, the criterion will assess, where applicable, potential complementarities with other public funding programmes. (5 points)

- **Catalytic effect:** evaluating i) the financial gap (for instance the need to overcome financial obstacles generated by insufficient commercial viability, high upfront costs or the lack of market finance), ii) the capacity to mobilise different investments sources, iii) the capacity to trigger important overall investments with limited EU support and, where appropriate, iv) the extent to which externalities justify the CEF financial support. It shall also be used to assess the catalytic effect of the EU financial support and determine whenever possible the actual co-funding rate to be granted. (5 points).

Award criteria	Minimum pass score		Maximum score
Priority and urgency	3		5
Maturity	3		5
Quality	3		5
Impact	3		5
Catalytic effect	3		5
Overall (pass) scores	**15**		**25**

Maximum points: 25 points.

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

Overall threshold: 15 points.

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: up to 31.12.2026 (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.

Beneficiaries will also be invited to check and update information about output indicators.

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): projects of any budget are admitted. The grant awarded may be lower than the amount requested.

Please be aware that you may be asked to request an amendment to reduce the grant awarded if your project encounters major delays during the project implementation. If you do not comply with this request, we may have to terminate the grant *(see art 32)*.

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 rates fixed in the Grant Agreement (maximum **50%** for the costs of studies, maximum **70%** for the costs of works in outermost regions, and maximum **30%** for all other costs categories ('project funding rate')).

You can apply for a higher project funding rate if your project concerns:

- strong cross-border dimension: maximum 50%

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, art 6 and Annex 2)*.

Budget categories for this call:

- A. Personnel costs
  - A.1 Employees, A.2 Natural persons under direct contract, A.3 Seconded persons
  - A.4 SME owners and natural person beneficiaries
- B. Subcontracting costs
- C. Purchase costs
  - C.1 Travel and subsistence
  - C.2 Equipment
  - C.3 Other goods, works and services
- D. Other cost categories
  - D.1 Financial support to third parties
  - D.2 Studies
  - D.3 Synergetic elements, for works
- 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 cost[36] : Yes
- subcontracting costs:
  - country restrictions for subcontracting costs: Yes, subcontracted work must be performed in the eligible countries or target countries
- travel and subsistence unit cost[37]: No (only actual costs)
- equipment costs: full cost
- other cost categories:
  - costs for financial support to third parties: not allowed
  - studies: Yes
  - synergetic elements: Yes (only for 'Works' Actions, not for 'Studies')
  - works in outermost regions: Yes
  - land purchases: No
- indirect cost flat-rate :0%of the eligible direct costs (categories A-D, except volunteers costs, if any
- VAT: VAT is NOT eligible
- other:

[36] 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).

[37] 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).

- in-kind contributions for free are allowed, but cost-neutral, i.e. they cannot be declared as cost
- 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
- eligible cost country restrictions: Yes, only costs for activities carried out in eligible countries or target countries are eligible
- other ineligible costs: Yes, costs related to purchase of land

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 (up to **30%** of the maximum grant amount). The prefinancing will be paid 30 days from entry into force/financial guarantee (if required – whichever is the latest.

There will be no **interim payments** for Studies topics. There will be one or more **interim payments** (with detailed cost reporting) for Works topics.

In addition, for Works topic, you will be expected to submit one or more progress reports not linked to payments.

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)*

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

- rights of use on results: Yes

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

- communication and dissemination plan: No
- additional communication and dissemination activities: Yes
- special logos: No

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

- Member State information: Yes
- specific rules for digital infrastructure projects: Yes
- durability: Yes
- special obligations linked to restrictions due to security:
    - implementation in case of restrictions due to security: 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 EULogin 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 4 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
- Part C containing additional project data. To be filled in directly online.
- Annexes (*see section 5*). Upload them as PDF file (single or multiple depending on the slots; the budget table can be uploaded as Excel file).

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).
- call information on the HaDEA website.

Please also consult the Topic page regularly, since we will use it to publish call updates.

Contact

For individual questions on the Portal Submission System, please contact the IT Helpdesk.

Non-IT related questions should be sent to the following email address: HaDEA-CEF-DIGITAL-CALLS@ec.europa.eu.

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

13. Important

IMPORTANT

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

  The roles should be attributed according to the level of participation in the project. Main participants should participate as **beneficiaries** or **affiliated entities**; other entities can participate as associated partners, subcontractors, third parties giving in-kind contributions. **Associated partners** and third parties giving in-kind contributions should bear their own costs (they will not become formal recipients of EU funding).
- **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 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.