



Internal Security Fund (ISF)

Call for proposals

Digital Investigations and Standardisation

(ISF- 2026-TF2-AG-CYBER)

Call version V2.0
21/09/2026

Call document Template: Version 2.02 – 01 January 2025

HISTORY OF CHANGES for call for proposals ISF-2026-TF2-AG-CYBER			
Version	Publication Date	Change	Page
1.0	15.09.2026	Initial version of the call for proposals	
1.1	21.09.2026	Update, correcting the table for eligibility for the standardisation component	16
Etc...			



EUROPEAN COMMISSION
 DIRECTORATE-GENERAL FOR MIGRATION AND HOME AFFAIRS
 Directorate E – HOME Affairs Funds
E.4 – Union actions and Procurement

CALL FOR PROPOSALS

TABLE OF CONTENTS

0. Introduction	4
1. Background	5
2. Objectives — Themes and priorities — Scope — Activities that can be funded —	
Expected impact	6
Topic 1: ISF-2026-TF2-AG-DIGITAL - Digital Investigations	6
Objectives	6
Themes and priorities - Scope - activities and outcomes	6
Expected impact	7
Additional considerations applicable to this topic	7
Topic 2: ISF-2026-TF2-AG-STANDARD - Standardisation	8
Objectives	8
Themes and priorities - Scope - activities and outcomes	9
Expected impact	9
Additional considerations applicable to this topic	9
3. Available budget	10
4. Timetable and deadlines	10
5. Admissibility and documents	10
6. Eligibility	11
Eligible participants (eligible countries)	11
Specific cases and definitions	12
Consortium composition	14
Eligible activities	14
Other important considerations	14
Duration	15
Maximum EU Grant amount	15
Ethics	15
Security	15
Overview table of Eligibility conditions	16
7. Financial and operational capacity and exclusion	17
Financial capacity	17
Operational capacity	18
Exclusion	18
8. Evaluation and award procedure	20
9. Award criteria	20
10. Legal and financial set-up of the Grant Agreements	21
Starting date and project duration	21
KPIs, milestones and deliverables	21
Form of grant, funding rate and maximum EU grant amount	22
Budget categories and cost eligibility rules	22
Reporting and payment arrangements	24
Prefinancing guarantees	24
Certificates	25
Liability regime for recoveries	25
Provisions concerning the project implementation	25
Other specificities	25
Non-compliance and breach of contract	25
11. How to submit an application	25
12. Help	26
13. Important	28

0. Introduction

This is a call for proposals for EU **action grants** in the field of digital investigations and standardisation under the **Internal Security Fund (ISF)**.

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

- Regulation 2024/2509 ([EU Financial Regulation](#))¹
- the basic act (ISF Regulation (EU) 2021/1149²).

The call is launched in accordance with the [2025-2027] Thematic Facility Work Programme³ and will be managed by the **European Commission, Directorate-General for Migration and Home Affairs (DG HOME)**.

The call covers the following **topics**:

- **ISF-2026-TF2-AG-DIGITAL - Digital Investigations**
- **ISF-2026-TF2-AG-STANDARD - Standardisation**

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, themes and priorities, scope, activities that can be funded and outcomes, the expected results and impact (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)
- the [Online Manual](#) outlines the:
 - procedures to register and submit proposals online via the EU Funding & Tenders Portal ('Portal')
 - recommendations for the preparation of the application
- the [AGA — Annotated Grant Agreement](#) contains:
 - detailed annotations on all the provisions in the Grant Agreement you will have to sign in order to obtain the grant (*including cost eligibility, payment schedule, accessory obligations, etc*).

¹ Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast) ('EU Financial Regulation') (OJ L, 2024/2509, 26.9.2024).

² REGULATION (EU) 2021/1147 of the European Parliament and of the Council of 7 July 2021 establishing the Internal Security Fund (OJ L 251, 15.7.2021, p. 94).

³ Commission Implementing Decision C(2022) 8334 final of 23 November 2022 on the financing of components of the Thematic Facility under the Internal Security Fund and adoption of the Work Programme for 2023 - 2027 as last modified by the [Ninth revised 2023-2027 Work Programme \(non-substantial\)](#)

1. Background

Cybercrime is one of the EU's priorities in the fight against serious and organised crime as part of EMPACT 2026 - 2029. According to the most recent Internet Organised Crime Threat Assessment (IOCTA), cybercrime is becoming more aggressive and confrontational. This can be seen across the various forms of cybercrime, including abuse of encryption, cryptocurrencies, cyber-dependent crimes, digital fraud, identity theft and data breaches.

In general, access to data and to electronic evidence represents a persistent challenge for law enforcement authorities (LEAs) in the area of cybercrime but also in effectively countering other forms of organised and serious crime. Several new legal instruments are in place to facilitate access to digital evidence in the framework of criminal investigations: new EU e-evidence rules,⁴ a second additional Protocol to the Council of Europe Budapest Convention on Cybercrime,⁵ as well as a UN Cybercrime Convention.⁶

The present Call for Proposals aims at funding projects on fighting cybercrime and digital investigations, as a continuation of various initiatives and plans in the field.

In July 2020, the European Commission adopted the ProtectEU⁷ internal security strategy, defining the priority actions that the Commission intends to pursue in the area of internal security at large and specifically also in the area of cybercrime (see Strategic Priority 2 "Tackling evolving threats").

As a follow up to the ProtectEU strategy, the Commission has outlined its plans to enhance capacity and capabilities of law enforcement authorities in the area of digital investigations in its Roadmap on lawful and effective access to data for law enforcement,⁸ which is a fundamental reference for this call for proposals.

The Roadmap is based on the recommendations⁹ and on the concluding report¹⁰ of the High Level Group on Lawful Access to Data, set up by the Commission together with the Presidency of the Council of the European Union.

Moreover, the Commission, through the EU research framework programmes in the field of fighting crime and terrorism (FCT), continuously funds research and innovation projects that, together with law enforcement authorities, work on countering cybercrime, from the abuse of encryption, digital and mobile forensics via cryptocurrencies to identity theft and lawful exchange of electronic evidence.

The Commission also identified standardisation as strategic enabler to ensure that future technologies are designed in manner compatible for targeted lawful access to data and that solutions developed for security purposes are interoperable and compatible with EU rules. This is particularly needed in the area of lawful access to data where standardized data format and communication protocols are needed to enable law enforcement and the judiciary to request and process digital evidence efficiently. In addition, it is important to ensure that the standards that will govern the development

⁴ https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en

⁵ <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224>

⁶ <https://documents.un.org/doc/undoc/gen/n24/426/74/pdf/n2442674.pdf>

⁷ https://home-affairs.ec.europa.eu/news/commission-presents-protecteu-internal-security-strategy-2025-04-01_en

⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0349>

⁹ https://home-affairs.ec.europa.eu/document/download/1105a0ef-535c-44a7-a6d4-a8478fce1d29_en?filename=Recommendations%20of%20the%20HLG%20on%20Access%20to%20Data%20for%20Effective%20Law%20Enforcement_en.pdf

¹⁰ https://home-affairs.ec.europa.eu/document/download/4802e306-c364-4154-835b-e986a9a49281_en?filename=Concluding%20Report%20of%20the%20HLG%20on%20access%20to%20data%20for%20effective%20law%20enforcement_en.pdf

and use of key technologies such as Artificial Intelligence are compatible with law enforcement needs that are often specific.

The Commission launched the European Cybercrime Centre (EC3) at Europol in early 2013. The EC3 is becoming a focal point for cybercrime-related issues and digital forensic including lawful decryption and has been cooperating with Member States and third countries on a number of very successful investigations. Europol was furthermore mandated by the Justice and Home Affairs ministers from the EU Member States at the end of 2019 to create an Innovation Lab to support the law enforcement community in the area of innovation. The role of the Europol Innovation Lab in supporting EU Security research and innovation activities, in monitoring emerging technologies and in developing new ways of using those technologies for law enforcement purposes is also strengthened through the existing mandate of Europol (Regulation (EU) 2022/991).

2. Objectives — Themes and priorities — Scope — Activities that can be funded — Expected impact

Topic 1: ISF-2026-TF2-AG-DIGITAL - Digital Investigations

Objectives

- (1) developing capacity and expertise of law enforcement and judicial authorities;
- (2) contributing to the implementation of EU law and strategic documents;
- (3) fostering cross-border cooperation between law enforcement/judicial authorities and private entities.

Themes and priorities - Scope - activities and outcomes

The main beneficiaries of this call for proposals are law enforcement and/or judicial authorities in EU Member States and third countries that have an agreement with Europol.

Proposals should focus on:

- Enhancing the operational capacity of law enforcement and/or judicial authorities to investigate cyber-attacks and cyber enabled crime, for instance through specific training, investigative techniques and tools (including for) with a focus on top threat priorities (excluding online child sexual abuse, which is covered by specific calls for proposals) as presented in Europol Internet Organised Crime Threat Assessment 2025. Areas that have been identified by EU Member States as needing particular attention include: digital forensics (mobile forensics, computer forensics, network forensics, IoT forensics including automotive forensics, cloud forensics), visual data analysis, malware analysis and reverse engineering capabilities, cryptocurrencies tracing, identifying and disrupting criminal infrastructures, analysis and seizure, efficient storage, processing, analysis and transfer of big data and large datasets, understanding and exploiting “threat intelligence” and metadata, OSINT, crime involving the use of AI by offenders.
- Enhancing the operational capabilities of law enforcement and/or judicial authorities to address the challenges posed by the use of encryption by criminals and its impact on criminal investigations, for instance through training and/or by supporting the establishment, extension and development of points of expertise and their networking at EU level or supporting the development of a toolbox of alternative investigation techniques to obtain needed information encrypted by criminals (with the exclusion of measures that could weaken encryption in general or could have an impact on a larger or indiscriminate number of people)
- Enhancing the capabilities of law enforcement and/or judicial authorities through the use and/or adaptation of Large Language Models and AI-based solutions to

improve analysis, translation, transcription of data as well as detection of AI materials generated for criminal purposes.

- Enhancing the operational capacity of law enforcement and/or judicial authorities to cooperate across borders, for instance supporting the gathering and provision of digital evidence, supporting the secondment of officials, improving the efficiency of 24/7 (permanent) law enforcement contact points for cybercrime, establishment of dedicated platforms
- Enhancing the cooperation between private entities and/or authorities in the area of cybersecurity and law enforcement and/or judicial authorities, taking remedial action, including by setting of appropriate information exchange systems (or interfaces to make better use of existing systems)
- Increasing and enhancing reporting of cybercrime to law enforcement authorities

Expected impact

Projects selected under this call for proposals should aim to achieve one or more of the following outcomes in the field of countering cybercrime and supporting digital investigations:

- increasing operational capacity and capabilities of law enforcement and/or judicial authorities,
- increasing the availability of technical tools for law enforcement, that are ready to be used effectively in investigations and valid for legal proceedings
- increasing awareness on best practices and available solutions as well as building synergies amongst relevant stakeholders will be an asset

Additional considerations applicable to this topic

Taking into account important achievements and policy developments in the area of cybercrime and digital investigations so far, the projects should build on scientific material available in the domain and in particular exploit, where possible, publicly available material resulting from relevant projects supported by the European Commission (e.g. under Horizon Europe, ISF) as well as from any other relevant project.

Much of the R&I effort undertaken so far on countering cybercrime, and supported by EU funding, led to findings and outcomes, promising technological prototypes and organisational solutions that should constitute the basis for further development. There is a strong added value in promoting European innovation, as it leads to reinforcement of existing and development of new civil security practitioners' capabilities. Synergies between Union-funded R&I with the Internal Security Fund can hence facilitate funding to security practitioners and authorities to build on successful research results, support testing, validating or deployment of new methods and technologies stemming from R&I actions.

Projects are not supposed to include a feasibility study or similar scoping exercises: these activities to prepare the practical implementation of the project have to be already carried out as a preliminary step, before the grant agreement is signed.

Proposals that strengthen and clearly link with actions led in the context of EMPACT e.g. through capacity building activities are especially welcomed, in particular those which will contribute to the strategic autonomy of the EU in this domain.

Applications should demonstrate that projects do not duplicate existing work or products and include evidence of user needs. In this respect, applicants are expected to be especially aware of activities deployed by the European Cybercrime Centre (EC3),

the Europol Innovation Lab, as well as relevant projects and networks, such as the European Anti-Cybercrime Technology Development Association (EACTDA) that can contribute to the sustainability of project's result after the end of the project, the European Cybercrime Training and Education Group (ECTEG) that can contribute to the creation of training materials.

When relevant, projects should make use of and build on existing communities of experts in their area of activity: reference to specific communities constituted under previous projects (e.g. CYCLOPES, ULTRA,...) or formed autonomously (for instance those existing on the Europol Platform of Experts) will be considered an asset. Use of existing EC tools or platforms, such as JRC's analytical platform¹¹ for monitoring cryptocurrencies activity, will be considered an asset.

The tools developed in the framework of projects under this Call shall be made available for their use to any law enforcement authority (LEA) in the EU, as well as to Europol, at little or no cost. A commitment to distribute developed tools through the Europol Tools Repository will be considered an asset.

To foster their uptake, usability and maintenance, tools developed under this call should not be thought in isolation. They should be developed when possible following EU guidance and best practices such as those made available by EACTDA and Europol on licensing schemes¹², interoperability¹³ or usability¹⁴.

Law enforcement authorities in the EU should be involved in the full development cycle of the project deliverables. The final tools developed for law enforcement use should be owned by law enforcement in the EU.

Proposals should pay specific attention to the necessary access to realistic datasets for the development, validation and testing of tools. The use of the Europol sandbox can facilitate validation against realistic law enforcement datasets and operational scenarios, thereby supporting a more meaningful assessment of the developed tools. A commitment to test developed tools making use of the [Europol sandbox](#)¹⁵, including setting aside the necessary resources, will be considered an asset. When relevant, the creation of reusable datasets for the trainings, evaluation and testing of solutions is welcome as well.

The applications should clearly demonstrate how this will be implemented, how the ownership will be transferred to the LEA, and how the sustainability of the solution after the end of the project will be ensured.

Topic 2: ISF-2026-TF2-AG-STANDARD - Standardisation

Objectives

(1) developing capacity and expertise of law enforcement and judicial authorities for lawful access to data, using solutions that are interoperable and compatible with EU rules;

(2) contributing to the implementation of EU law;

¹¹ https://joint-research-centre.ec.europa.eu/scientific-activities/digital-finance-research/cipher-monitoring-crypto-markets_en

¹² <https://eactda.eu/licenses.html>

¹³ https://eactda.eu/assets/files/5.technical%20aspects/Tools4LEAs_APIs_How-to-Guide_v1.0.pdf

¹⁴ https://eactda.eu/assets/files/5.technical%20aspects/Tools4LEAs_UIs_How-to-Guide_v1.0.pdf

¹⁵ https://www.europol.europa.eu/sites/default/files/documents/ODIN_Sandbox_Process_EU-funded-project.pdf

(3) fostering cross-border cooperation between law enforcement/judicial authorities and private entities to develop standardised data formats and communication protocols to request and process digital evidence.

Themes and priorities - Scope - activities and outcomes

The main beneficiaries of this call for proposals are law enforcement and/or judicial authorities in EU Member States and third countries that have an agreement with Europol.

Proposals should focus on:

- Providing an analysis of the areas where standardisation for security is needed
- Relevant standardisation activities to enhance the operational capacity of law enforcement and/or judicial authorities to address the challenges posed in identified areas, notably 6G and Internet based communication, digital forensics, vehicles forensics and Artificial Intelligence.
- Raising awareness and supporting participation of security practitioners in relevant standardisation processes
- Pooling resources in Member States to ensure effective participation in relevant standardisation processes
- Designing and developing (in cooperation with the European Cybercrime Training and Education Group, when relevant), delivering and providing access to training to enhance the effectiveness of security practitioners participating in relevant standardisation processes.
- Providing expertise to support the participation of security practitioners in relevant standardisation processes through studies and advice.
- Reflecting on sustainable mechanisms to support an EU approach on standardisation for digital investigation.
- Areas where EU legislative initiatives would benefit from further standardisation activities.

Expected impact

The project selected under this call for proposals should aim to achieve one or more of the following outcomes in the field of standardisation supporting digital investigations:

- structure and enhance security practitioners' contribution in standardisation processes,
- increase awareness and build synergies amongst relevant stakeholders
- nurture a sustainable EU approach for standardisation in the field of digital investigations.

The project should be leading to the delivery of concrete standards to support law enforcement and/or the judiciary.

Additional considerations applicable to this topic

Proposals are expected primarily to contribute to enhancing in a concrete manner relevant standards to support digital investigations and lawful access to data. More strategic contributions for a sustainable EU approach on standardisation for security are considered a plus.

Proposals for this call are invited to involve a broad set of expertise covering security operational needs, technology and standardisation potentially represented by experts from national authorities, academia, technology providers and national standardisation bodies.

Proposals are invited to build on relevant outcomes of European Projects such as FORMOBILE¹⁶ or CYCLOPES¹⁷ and on existing coordination mechanisms, such as the *European Working Group on Standardisation for Public Safety* steered by Europol.

3. Available budget

The available call budget is **EUR 6 500 000**. Specific budget information per topic can be found in the table below.

Topic	Topic budget
1. ISF-2026-TF2-AG-DIGITAL	EUR 5 000 000
2. ISF-2026-TF2-AG-STANDARD	EUR 1 500 000

We expect to fund four projects under topic 1 and one project under topic 2.

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:	15 September 2026
<u>Deadline for submission:</u>	<u>15 December 2026 – 17:00:00 CET</u> (Brussels)
Evaluation:	December 2026 - March 2027
Information on evaluation results:	April 2027 ¹⁸
GA signature:	May 2027

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.

¹⁶ https://www.researchgate.net/publication/344191805_FORMOBILE_-_Report_on_existing_practices_and_standards

¹⁷ <https://www.cyclopes-project.eu/news/public-deliverables>

¹⁸ In the interest of equal treatment of applicants, the Commission cannot provide any information on the outcome of the call for proposals before the official announcement of the results.

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

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

- Application Form Part A — contains administrative information about the participants (future coordinator, beneficiaries and affiliated entities) and the summarised budget for the project (*to be filled in directly online*)
- Application Form Part B — contains the technical description of the project (*template to be downloaded from the Portal Submission System, completed, assembled and re-uploaded*)
- Part C — contains the project's contribution to EU programme key performance indicators (*to be filled in directly online*)
- **mandatory annexes and supporting documents** (*templates to be downloaded from the Portal Submission System, completed, assembled and re-uploaded*):
 - list of previous projects (key projects for the last 4 years, not limited to EU-funded projects): template available in Part B but to be **submitted as a separate annex**¹⁹.
 - detailed budget table: **not applicable**
 - CVs of core project team: **not applicable**
 - activity reports of last year: **not applicable**

At proposal submission, you will have to confirm that you have the **mandate to act** for all applicants. Moreover you will have to confirm that the information in the application is correct and complete and that the participants comply with the conditions for receiving EU funding (especially eligibility, financial and operational capacity, exclusion, etc). Before signing the grant, each beneficiary and affiliated entity will have to confirm this again by signing a declaration of honour (DoH). Proposals without full support will be rejected.

Your application must be **readable, accessible and printable**. (please check carefully the layout of the documents uploaded)

Proposals are limited to maximum **50 pages** (Part B without annexes). 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.:

¹⁹ The list of previous projects is a mandatory annex. In case this annex is not uploaded, the application will be considered inadmissible and will not be assessed.

- EU Member States (including overseas countries and territories (OCTs)), excluding Denmark²⁰,
- third countries that have an operational agreement with Europol.²¹

NB: legal entities established in third countries can participate only as part of a consortium composed of at least two independent legal entities, at least one of which is established in an EU Member State. Do note that when including an entity of a third country, the submission system may give a warning that the organisation is not based in one of the eligible country groups. This warning should not block the submission of your proposal. Do contact us in case it does block your submission.

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*).

Specific cases and definitions

Exceptional funding — Entities from third countries are only exceptionally eligible, if the third country has an operational agreement with Europol and if they are part of a consortium composed of at least two independent entities, at least one of which is established in an EU Member State. Such entities can ONLY participate as co-beneficiaries.

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).

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 persons²².

EU bodies — EU bodies 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'²³.  Please note that if the action will be implemented by the members, they should also participate (either as beneficiaries or as affiliated entities, otherwise their costs will NOT be eligible).

Countries currently negotiating association agreements — Beneficiaries from countries with ongoing negotiations for participation in the programme (*see list of participating countries above*) may participate in the call and can sign grants if the negotiations are concluded before grant signature and if the association covers the call (i.e. is retroactive and covers both the part of the programme and the year when the call was launched).

Israeli applicants — With regard to Israeli entities, please follow the Guidelines on the eligibility of Israeli entities and their activities in the territories occupied by Israel since

²⁰ In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of Regulation (EU) 2021/1149 and is not bound by it or subject to its application.

²¹ A non-EU country is a country, which is not an EU Member State.

²² See Article 200(2)(c) EU Financial Regulation [2024/2509](#).

²³ For the definitions, see Articles 190(2) and 200(2)(c) EU Financial Regulation [2024/2509](#).

June 1967 for grants, prizes and financial instruments funded by the EU from 2014 onwards²⁴.

No projects directly benefitting the Georgian authorities – which include central government, local authorities, agencies and state-owned enterprises – will be allowed. However, if required, regional capacity building events benefiting more than one country involving Georgia can take place at technical level but only if these events are held outside Georgia. The costs of participation for these public officials and similar persons cannot be covered by the EU grant. Assistance to civil society, independent media and countering disinformation is nevertheless possible. Regarding this, do note that under the revised laws, Georgian participants could face criminal liability if they participate or get their travel/accommodation paid for participation in EU-funded events without pre-authorisation by Georgian authorities. Particular caution is therefore required before deciding to invite or fund the participation of Georgian individuals or organisations. A case-by-case risk assessment should be conducted to evaluate whether their participation might be considered to fall under the remit of the law.

EU restrictive measures — Special rules apply for *entities subject to [EU restrictive measures](#) under Article 29 of the Treaty on the European Union (TEU) and Article 215 of the Treaty on the Functioning of the EU (TFEU)*²⁵ and *entities covered by Commission Guidelines No [2013/C 205/05](#)*²⁶. Such entities are not eligible to participate in any capacity, including as beneficiaries, affiliated entities, associated partners, third parties giving in-kind contribution, subcontractors or recipients of financial support to third parties (if any).

EU conditionality measures - Special rules apply for entities subject to measures adopted on the basis of EU Regulation 2020/2092²⁷. Such entities are not eligible to participate in any funded role (beneficiaries, affiliated entities, subcontractors, recipients of financial support to third parties, etc). Currently no such measures are in place.

Following the [Council Implementing Decision \(EU\) 2022/2506](#), as of 16th December 2022, no legal commitments (including the grant agreement itself as well as subcontracts, purchase contracts, financial support to third parties etc.) can be signed with Hungarian public interest trusts established under Hungarian Act IX of 2021²⁸ or any entity they maintain.

Affected entities may continue to apply to calls for proposals. However, in case the Council measures are not lifted, such entities are not eligible to participate in any funded role (beneficiaries, affiliated entities, subcontractors, recipients of financial support to third parties). In this case, co-applicants will be invited to remove or replace that entity and/or to change its status into associated partner. Tasks and budget may be redistributed accordingly.



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

²⁴ 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 (OJ C 205 of 19.07.2013, pp. 9-11).

²⁵ 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](#).

²⁶ 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).

²⁷ Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget (OJ L 325, 20.12.2022, p. 94).

²⁸ As Act IX of 2021 can be amended, the applicants should always refer to the latest update of the relevant Hungarian Act, available in the national legal database NJT.hu (<https://njt.hu>).

The identity of the applicant (and compliance with general eligibility conditions) will be verified through the documents provided in the [Participant Register](#) during legal entity validation (copy of the resolution, decision or other official document establishing the entity, etc).

Consortium composition

Proposals must be submitted by:

for topic 1 - ISF-2026-TF2-AG-DIGITAL:

- minimum 2 applicants (beneficiaries; not affiliated entities) from at least 2 different participating EU Member States
- the following entities can NOT apply as coordinator:
 - profit making entities
 - international organisations²⁹, irrespective of their country of establishment
 - entities established in non-EU countries.

for topic 2 - ISF-2026-TF2-AG-STANDARD:

- at least a single applicant from one participating EU Member State ensuring the participation of practitioners of at least 5 EU Member States in the project, but preferably a consortium composed of applicants from at least 2 different participating EU Member States.
- the following entities can NOT apply:
 - profit making entities
 - international organisations, irrespective of their country of establishment
 - entities established in non-EU countries.

Eligible activities

Eligible activities are the ones set out in section 2 above.

Proposals focusing:

- exclusively on raising the overall level of awareness on Cybercrime and digital investigations, e.g. when targeted at the general public,
- on research without clear links to operational output,
- on specific crime areas such as drugs, financial investigations, trafficking in human beings or child sexual abuse are covered by other EU funding Programmes and/or other calls for proposals and therefore are not considered as relevant for funding under this call Financial support to third parties is not allowed.

Other important considerations

The European Commission welcomes proposals involving applicants from more Member States than the minimum number identified in the eligibility criteria, as long as they are relevant for the design of the action.

All projects need to take into account the safeguarding of fundamental rights protected in the Union when establishing, implementing, developing and rolling out measures to achieve the above-mentioned outcomes.

²⁹ The term "international organisations" is used as defined in Article 156 of the FR (Euratom 2018/1046)

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 should comply with EU policy interests and priorities (*such as environment, social, security, industrial and trade policy, etc*). Projects must also respect EU values and European Commission policy regarding reputational matters (*e.g. activities involving capacity building, policy support, awareness raising, communication, dissemination, etc*)³⁰.

Duration

Projects must have a foreseen maximum duration of 24 months (extensions are possible, if duly justified and through an amendment).

Maximum EU Grant amount

Requested EU contribution to the project's budget ("maximum EU grant amount" per project) ranges between EUR 1 000 000 and EUR 2 500 000 for "Digital Investigations" and must not exceed EUR 1 500 000 for "Standardisation".

Each beneficiary must bear a budget.

Ethics

Projects must comply with:

- highest ethical standards
- EU values based on Article 2 of the Treaty on the European Union and Article 21 of the EU Charter of Fundamental Rights and
- other applicable EU, international and national law.

Applications should pay appropriate attention to the effects of the project on individual rights and freedoms, and indicate the measures taken to limit or remedy such effects.

Applicants must show in their application that they respect ethical principles and EU values based on Article 2 of the Treaty on the European Union and Article 21 of the EU Charter of Fundamental Rights.

Projects involving ethics issues may be made subject to specific ethics rules.

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](#)³¹ 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

³⁰ See, for instance, Guidance on funding for activities related to the development, implementation, monitoring and enforcement of Union legislation and policy.

³¹ See Commission Decision 2015/444/EU, Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

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.

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.

Overview table of Eligibility conditions

	Topic 1 - ISF-2026-TF2-AG-DIGITAL	Topic 2 - ISF-2026-TF2-AG-STANDARD
Consortium composition — minimum number of		
Entities	2	1
Member States participating in ISF(*)	2	1 (ensuring participation of practitioners from 5 EU Member States participating in ISF)
Consortium composition — participation of public bodies (**)		
Consortium composition — participation of non-profit-making public/private entities as		
Coordinators	Yes	Yes
Beneficiaries/affiliated entities	Yes	Yes
Consortium composition — Participation of International Organisations as		
Coordinators	No	No
Beneficiaries	Yes	No

Consortium composition — participation of profitmaking entities as		
Coordinators	No	No
Beneficiaries /affiliated entities	Yes	No
Consortium composition — participation of legal entities established in third countries (***)		
Coordinators	No	No
Beneficiaries	Yes	No
Duration of projects (in months)		
	24	24
Minimum and Maximum EU Grant amount per project (Requested EU contribution)		
Minimum (EUR)	1 000 000	1 000 000
Maximum (EUR)	2 500 000	1 500 000

(*) the rules on eligible countries do not apply to International organisations. International organisations can participate [as coordinator/beneficiaries] regardless of their geographical location. However, being based in an eligible country does not contribute to the fulfilment of the minimum number of eligible countries required in the eligibility criteria related to the consortium composition.

(**) public bodies or, by the competent authority's mandate, a public or non-public implementing agency or body of a Member State participating in the ISF.

(***) legal entities established in third countries can participate only as part of a consortium composed of at least two independent legal entities, at least one of which is established in an EU Member State. Do note that when including an entity of a third country, the submission system may give a warning that the organisation is not based in one of the eligible country groups. This warning should not block the submission of your proposal. Do contact us in case it does block your submission.

7. Financial and operational capacity and exclusion

Financial capacity

Applicants must have **stable and sufficient resources** to successfully implement the projects and contribute their share. Organisations participating in several projects must have sufficient capacity to implement all projects.

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

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

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

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

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

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



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

Operational capacity

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

This capacity will be assessed together with the '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 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) (*template available in Part B*).

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 participate³²:

- 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 misconduct³³ (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- committed fraud, corruption, links to a criminal organisation, money laundering, terrorism-related crimes (including terrorism financing), child labour or human trafficking (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- shown significant deficiencies in complying with main obligations under an EU procurement contract, grant agreement, prize, expert contract, or similar (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- guilty of irregularities within the meaning of Article 1(2) of Regulation No [2988/95](#) (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant)
- created under a different jurisdiction with the intent to circumvent fiscal, social or other legal obligations in the country of origin or created another entity with this purpose (including if done by persons having powers of representation, decision-making or control, beneficial owners or persons who are essential for the award/implementation of the grant).
- intentionally and without proper justification resisted³⁴ an investigation, check or audit carried out by an EU authorising officer (or their representative or auditor), OLAF, the EPPO, or the European Court of Auditors.

Applicants will also be refused if it turns out that³⁵:

- during the award procedure they misrepresented information required as a condition for participating or failed to supply that information

³² See Articles 138 and 143 of EU Financial Regulation [2024/2509](#).

³³ 'Professional misconduct' includes, in particular, the following: violation of ethical standards of the profession; wrongful conduct with impact on professional credibility; breach of generally accepted professional ethical standards; false declarations/misrepresentation of information; participation in a cartel or other agreement distorting competition; violation of IPR; attempting to influence decision-making processes by taking advantage, through misrepresentation, of a conflict of interests, or to obtain confidential information from public authorities to gain an advantage; incitement to discrimination, hatred or violence or similar activities contrary to the EU values where negatively affecting or risking to affect the performance of a legal commitment.

³⁴ 'Resisting an investigation, check or audit' means carrying out actions with the goal or effect of preventing, hindering or delaying the conduct of any of the activities needed to perform the investigation, check or audit, such as refusing to grant the necessary access to its premises or any other areas used for business purposes, concealing or refusing to disclose information or providing false information.

³⁵ See Article 143 of the EU Financial Regulation [2024/2509](#).

- 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 a **two-step evaluation procedure**].

For all eligible applications, in the first step, there will be a pre-selection on the basis of the Relevance award criterion only. In the second step, the successful proposals will be assessed against the full set of award criteria.

An **evaluation committee** 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) 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 'Quality'.
- 2) If this does not allow to determine the priority, a further prioritisation can be done by considering the overall project portfolio and the creation of positive synergies between projects, or other factors related to the objectives of the call..
- 3) 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.

9. Award criteria

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

- **Relevance:** clarity and consistency of the objectives and scope of the project seen against the objectives and expected impact/outcomes (if applicable) as identified in section 2; contribution to the relevant EU strategic documents and/or action plans and legislative context; previous results in the field; European/trans-national dimension (30 points)
- **Quality:** logical links between the identified problems, needs and solutions proposed; methodology for implementing the project (concept and methodology, timetable, monitoring and evaluation); expertise and quality of the consortium and project teams; management structures and procedures; risks and risk management; feasibility of the project within the proposed time frame; cost effectiveness and best value for money (50 points)

- **Impact:** expected short-term and long-term impact of results on target groups/general public; degree of ambition and innovation; appropriate communication strategy, including visibility of EU funding; appropriate dissemination strategy for ensuring sustainability and long-term impact; sustainability of results after EU funding ends; replicability/usability/potential for amplification of the results (20 points).

Award criteria	Minimum pass score	Maximum score
Relevance	21	30
Quality	n/a	40
Impact	n/a	30
Overall (pass) scores	70	100

Maximum points: 100 points.

Individual thresholds for the criterion 'Relevance': 21/30 points.

Overall threshold: 70 points.

Proposals that pass the individual threshold for the criterion 'Relevance' 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: 24 months (extensions are possible, if duly justified and through an amendment).

KPIs, milestones and deliverables

Project proposals should provide key performance indicators (KPIs), both qualitative and quantitative, with baseline and targets to be used to monitor the implementation and to assess the result of the project, as well as measure the outputs and results of the project against programme performance indicators, relevant to the action, included in Annex VIII of Regulation (EU) [AMIF:2021/1147][ISF: 2021/1149][BMVI: 2021/1148], in particular as regards the Specific Objectives stated in Article 3.

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:

- A mid-term progress report

Form of grant, funding rate and maximum EU grant amount

The grant parameters (*maximum EU grant amount, funding rate, total eligible costs, etc.*) will be fixed in the Grant Agreement (*Data Sheet, point 3 and art 5*).

Maximum EU Grant amount per project (Requested EU contribution) : *see section 6 above*. 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 (**90%**).

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 of Model Grant Agreement*).

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
 - A.5 Volunteers
- 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 (*not applicable*)
- E. Indirect costs

Specific cost eligibility conditions for this call:

- personnel costs:

- SME owner/natural person unit cost³⁶: Yes
- volunteers unit cost³⁷: Yes (without indirect costs)
- travel and subsistence unit cost³⁸: Yes³⁹
- equipment costs: depreciation + full cost for listed equipment when this is essential and the only option for achieving the objectives of the project
- other cost categories:
 - costs for financial support to third parties: not allowed
- indirect cost flat-rate: 7% of the eligible direct costs (categories A-D, except volunteers costs and exempted specific cost categories, if any)
- VAT: non-deductible/non refundable VAT is eligible (but please note that since 2013 VAT paid by beneficiaries that are public bodies acting as public authority is NOT eligible)
- divers:
 - in-kind contributions for free are allowed, but cost-neutral, i.e. 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
- Volunteers costs — Volunteers costs are not a classic cost category. There are no costs because volunteers work for free, but they may nonetheless be added to the budget in the form of a pre-fixed unit cost (per volunteer) and thus allow you to benefit from the volunteers' work for the grant (by increasing the amount of reimbursement up to 100% of the normal costs, i.e. cost categories other than volunteers). More information is available in the [AGA — Annotated Grant Agreement, art 6.2.A.5](#).

Specific cost eligibility rules for this call: [n/a]

Equipment and other goods, works and/or services related to 5G/6G mobile network communication equipment, and other technologies linked to the evolution of European communication network must:

1. not be subject to security requirements by third country/ non-associated third country that could affect the implementation of the action (e.g. technology restrictions, national security classification limiting the use of the equipment, etc.);
2. comply with (cyber-)security guidance issued by the Commission, in particular communications on the 5G toolbox²⁰;

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 10 April 2019 authorising the use of unit costs for declaring personnel costs for the work carried out by volunteers under an action or a work programme (C(2019)2646).

³⁸ 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).

³⁹ See [EU Grants AGA — Annotated Grant Agreement](#), art 6 on eligible costs: travel and subsistence costs must be declared using the unit cost according to Annex 2a of the grant agreement. If a particular instance of travel, accommodation or subsistence in the action is not covered by one of the unit costs mentioned in Decision C(2021)35 the actual costs may be used.

3. apply (cyber-)security requirements throughout the life cycle, including the selection and award procedure and criteria for purchases, the use, and also the related services, including installation, upgrading or maintenance;
4. ensure (cyber-)security by adequately protecting the availability, authenticity, integrity, and confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, that equipment.

Reporting and payment arrangements

The reporting and payment arrangements are fixed in the Grant Agreement (*Data Sheet, point 4 and art 21 and 22*).

After grant signature, you will normally receive a **prefinancing** to start working on the project (float of normally **80%** of the maximum grant amount; exceptionally less or no prefinancing). The prefinancing will be paid 30 days from entry into force/financial guarantee (if required) — whichever is the latest.

There will be no **interim payments**.

In addition, 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 you or one of your consortium members has outstanding debts towards the EU (granting authority or other EU bodies). Such debts will be offset by us — in line with the conditions set out in the Grant Agreement (*see art 22*).

Please also note that you are responsible for **keeping records** on all the work done and the costs [unit costs] declared. The Grant Agreement contains additional record-keeping rules (*Data Sheet, point 3 and art 20*).

Prefinancing guarantees

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

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

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

Prefinancing guarantees are normally requested from the coordinator, for the consortium. 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) must be provided during grant preparation, in time to make the prefinancing (scanned copy via Portal AND original by post).

If agreed with us, the bank guarantee may be replaced by a guarantee from a third party.

The guarantee will be released at the end of the grant, in accordance with the conditions laid down in the Grant Agreement (Art 23).

Certificates

Depending on the type of action, size of grant amount and type of beneficiaries, you may be requested to submit different certificates. The types, schedules and thresholds for each certificate are fixed in the Grant Agreement (*Data Sheet, point 4 and art 24*).

Liability regime for recoveries

The liability regime for recoveries will be fixed in the Grant Agreement (*Data Sheet, point 4.4 and art 22*).

For beneficiaries, it is limited joint and several liability with individual ceilings — *each beneficiary up to their maximum grant amount*.

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):*

- rights of use on results: Yes

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

- additional communication and dissemination activities: Yes
- limited communication and visibility to protect persons involved: Yes

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

- EU restrictive measures: Yes
- durability: Yes
- specific rules for humanitarian actions: No
- specific rules for blending operations: Yes

Other specificities

Consortium agreement: Yes

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 in the [Calls for proposals](#) section (or, for calls sent by invitation to submit a proposal, through the link provided in the invitation letter).

Submit your proposal in 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). Excel upload is sometimes possible, depending on the file type.

The proposal must keep to the **page limits** (*see section 5*); excess pages will be disregarded.

Documents must be uploaded to the **right category** in the Submission System, otherwise the proposal may be considered incomplete and thus inadmissible.

The proposal must be submitted **before the call deadline** (*see section 4*). After this deadline, the system is closed and proposals can no longer be submitted.

Once the proposal is submitted, you will receive a **confirmation e-mail** (with date and time of your application). If you do not receive this confirmation e-mail, it means your proposal has NOT been submitted. If you believe this is due to a fault in the Submission System, you should immediately file a complaint via the [IT Helpdesk webform](#), explaining the circumstances and attaching a copy of the proposal (and, if possible, screenshots to show what happened).

Details on processes and procedures are described in the [Online Manual](#). The Online Manual also contains the links to FAQs and detailed instructions regarding the Portal Electronic Exchange System.

12. Help

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

- [Online Manual](#)
- Topic Q&A on the Topic page (for call-specific questions in open calls; not applicable for actions by invitation)

- [Portal FAQ](#) (for general questions).

Questions **received later than 7 calendar days before the deadline** for submitting applications will not be answered. In the interest of equal treatment of applicants, the Commission cannot give a prior opinion on the eligibility of applicants or actions.

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

Contact

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

Non-IT related questions should be sent to the following email address: HOME-ISF@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). **Subcontracting** should normally constitute a limited part and must be performed by third parties (not by one of the beneficiaries/affiliated entities). Subcontracting going beyond 30% of the total eligible costs must be justified in the application.

- **Coordinator** — In multi-beneficiary grants, the beneficiaries participate as consortium (group of beneficiaries). They will have to choose a coordinator, who will take care of the project management and coordination and will represent the consortium towards the granting authority. In mono-beneficiary grants, the single beneficiary will automatically be coordinator.
- **Affiliated entities** — Applicants may participate with affiliated entities (i.e. entities linked to a beneficiary which participate in the action with similar rights and obligations as the beneficiaries, but do not sign the grant and therefore do not become beneficiaries themselves). They will get a part of the grant money and must therefore comply with all the call conditions and be validated (just like beneficiaries); but they do not count towards the minimum eligibility criteria for consortium composition (if any). If affiliated entities participate in your project, please do not forget to provide documents demonstrating their affiliation link to your organisation as part of your application.
- **Associated partners** — Applicants may participate with associated partners (i.e. partner organisations which participate in the action but without the right to get grant money). They participate without funding and therefore do not need to be validated.
- **Consortium agreement** — For practical and legal reasons it is recommended to set up internal arrangements that allow you to deal with exceptional or unforeseen circumstances (in all cases, even if not mandatory under the Grant Agreement). The consortium agreement also gives you the possibility to redistribute the grant money according to your own consortium-internal principles and parameters (for instance, one beneficiary can reattribute its grant money to another beneficiary). The consortium agreement thus allows you to customise the EU grant to the needs inside your consortium and can also help to protect you in case of disputes.

- **Balanced project budget** — Grant applications must ensure a balanced project budget and sufficient other resources to implement the project successfully (*e.g. own contributions, income generated by the action, financial contributions from third parties, etc*). You may be requested to lower your estimated costs, if they are ineligible (including excessive).
- **No-profit rule** — Grants may NOT give a profit (i.e. surplus of revenues + EU grant over costs). This will be checked by us at the end of the project.
- **No cumulation of funding/No double funding** — It is strictly prohibited to cumulate funding from the EU budget from the EU budget (except under EU Synergies actions). Outside such Synergies actions, any given action may receive only ONE grant from the EU budget and cost items may under NO circumstances be declared to two different EU grants. Projects must be designed as different actions, clearly delineated and separated for each grant (without overlaps).
- **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 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 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](#).