



## **GRANT AGREEMENT**

**Project 101227749 — NCC-CZ 2.0**

### **PREAMBLE**

This **Agreement** ('the Agreement') is **between** the following parties:

**on the one part,**

**European Cybersecurity Industrial, Technology and Research Competence Centre** ('granting authority'), under the powers delegated by the European Commission ('European Commission'),

**and**

**on the other part,**

1. 'the coordinator':

**NARODNI URAD PRO KYBERNETICKOU A INFORMACNI BEZPECNOST - NUKIB (NUKIB)**, PIC 907198418, established in MUCEDNICKA 1125/31, BRNO-ZABOVRESKY 616 00, Czechia,

Unless otherwise specified, references to 'beneficiary' or 'beneficiaries' include the coordinator and affiliated entities (if any).

If only one beneficiary signs the grant agreement ('mono-beneficiary grant'), all provisions referring to the 'coordinator' or the 'beneficiaries' will be considered — mutatis mutandis — as referring to the beneficiary.

The parties referred to above have agreed to enter into the Agreement.

By signing the Agreement and the accession forms, the beneficiaries accept the grant and agree to implement the action under their own responsibility and in accordance with the Agreement, with all the obligations and terms and conditions it sets out.

The Agreement is composed of:

Preamble

Terms and Conditions (including Data Sheet)

Annex 1	Description of the action <sup>1</sup>
Annex 2	Estimated budget for the action
Annex 2a	Additional information on unit costs and contributions (if applicable)
Annex 3	Accession forms (if applicable) <sup>2</sup>
Annex 3a	Declaration on joint and several liability of affiliated entities (if applicable) <sup>3</sup>
Annex 4	Model for the financial statements
Annex 5	Specific rules (if applicable)

---

<sup>1</sup> Template published on [Portal Reference Documents](#).

<sup>2</sup> Template published on [Portal Reference Documents](#).

<sup>3</sup> Template published on [Portal Reference Documents](#).

**TERMS AND CONDITIONS**

**TABLE OF CONTENTS**

**GRANT AGREEMENT..... 1**

**PREAMBLE.....1**

**TERMS AND CONDITIONS.....3**

**DATASHEET..... 8**

**CHAPTER 1 GENERAL.....13**

    ARTICLE 1 — SUBJECT OF THE AGREEMENT ..... 13

    ARTICLE 2 — DEFINITIONS.....13

**CHAPTER 2 ACTION..... 14**

    ARTICLE 3 — ACTION..... 14

    ARTICLE 4 — DURATION AND STARTING DATE.....14

**CHAPTER 3 GRANT.....14**

    ARTICLE 5 — GRANT.....14

        5.1 Form of grant.....14

        5.2 Maximum grant amount..... 15

        5.3 Funding rate..... 15

        5.4 Estimated budget, budget categories and forms of funding..... 15

        5.5 Budget flexibility..... 15

    ARTICLE 6 — ELIGIBLE AND INELIGIBLE COSTS AND CONTRIBUTIONS.....16

        6.1 General eligibility conditions..... 16

        6.2 Specific eligibility conditions for each budget category..... 17

        6.3 Ineligible costs and contributions..... 21

        6.4 Consequences of non-compliance.....22

**CHAPTER 4 GRANT IMPLEMENTATION.....23**

**SECTION 1 CONSORTIUM: BENEFICIARIES, AFFILIATED ENTITIES AND OTHER PARTICIPANTS..... 23**

        ARTICLE 7 — BENEFICIARIES.....23

        ARTICLE 8 — AFFILIATED ENTITIES..... 25

        ARTICLE 9 — OTHER PARTICIPANTS INVOLVED IN THE ACTION..... 25

            9.1 Associated partners.....25

            9.2 Third parties giving in-kind contributions to the action.....25

            9.3 Subcontractors.....26

9.4 Recipients of financial support to third parties.....26

ARTICLE 10 — PARTICIPANTS WITH SPECIAL STATUS..... 26

10.1 Non-EU participants..... 26

10.2 Participants which are international organisations.....27

10.3 Pillar-assessed participants..... 27

**SECTION 2 RULES FOR CARRYING OUT THE ACTION.....29**

ARTICLE 11 — PROPER IMPLEMENTATION OF THE ACTION..... 29

11.1 Obligation to properly implement the action..... 29

11.2 Consequences of non-compliance..... 30

ARTICLE 12 — CONFLICT OF INTERESTS..... 30

12.1 Conflict of interests..... 30

12.2 Consequences of non-compliance..... 30

ARTICLE 13 — CONFIDENTIALITY AND SECURITY..... 30

13.1 Sensitive information.....30

13.2 Classified information..... 31

13.3 Consequences of non-compliance..... 31

ARTICLE 14 — ETHICS AND VALUES..... 31

14.1 Ethics.....31

14.2 Values..... 31

14.3 Consequences of non-compliance..... 32

ARTICLE 15 — DATA PROTECTION..... 32

15.1 Data processing by the granting authority..... 32

15.2 Data processing by the beneficiaries..... 32

15.3 Consequences of non-compliance..... 33

ARTICLE 16 — INTELLECTUAL PROPERTY RIGHTS (IPR) — BACKGROUND AND RESULTS —  
ACCESS RIGHTS AND RIGHTS OF USE..... 33

16.1 Background and access rights to background.....33

16.2 Ownership of results.....33

16.3 Rights of use of the granting authority on materials, documents and information received for  
policy, information, communication, dissemination and publicity purposes..... 33

16.4 Specific rules on IPR, results and background..... 34

16.5 Consequences of non-compliance..... 34

ARTICLE 17 — COMMUNICATION, DISSEMINATION AND VISIBILITY..... 35

17.1 Communication — Dissemination — Promoting the action..... 35

17.2 Visibility — European flag and funding statement..... 35

17.3 Quality of information — Disclaimer.....36

17.4 Specific communication, dissemination and visibility rules.....36

17.5 Consequences of non-compliance..... 36

ARTICLE 18 — SPECIFIC RULES FOR CARRYING OUT THE ACTION..... 36

18.1 Specific rules for carrying out the action..... 36

18.2 Consequences of non-compliance..... 36

**SECTION 3 GRANT ADMINISTRATION..... 36**

ARTICLE 19 — GENERAL INFORMATION OBLIGATIONS..... 36

19.1 Information requests..... 36

19.2 Participant Register data updates..... 37

19.3 Information about events and circumstances which impact the action.....37

19.4 Consequences of non-compliance..... 37

ARTICLE 20 — RECORD-KEEPING..... 37

20.1 Keeping records and supporting documents..... 37

20.2 Consequences of non-compliance..... 38

ARTICLE 21 — REPORTING..... 38

21.1 Continuous reporting..... 38

21.2 Periodic reporting: Technical reports and financial statements..... 39

21.3 Currency for financial statements and conversion into euros.....40

21.4 Reporting language.....40

21.5 Consequences of non-compliance.....40

ARTICLE 22 — PAYMENTS AND RECOVERIES — CALCULATION OF AMOUNTS DUE..... 40

22.1 Payments and payment arrangements..... 40

22.2 Recoveries.....41

22.3 Amounts due.....41

22.4 Enforced recovery.....46

22.5 Consequences of non-compliance.....46

ARTICLE 23 — GUARANTEES.....47

23.1 Prefinancing guarantee..... 47

23.2 Consequences of non-compliance.....47

ARTICLE 24 — CERTIFICATES..... 48

24.1 Operational verification report (OVR).....48

24.2 Certificate on the financial statements (CFS).....48

24.3 Certificate on the compliance of usual cost accounting practices (CoMUC)..... 48

24.4 Systems and process audit (SPA).....49

24.5 Consequences of non-compliance.....49

ARTICLE 25 — CHECKS, REVIEWS, AUDITS AND INVESTIGATIONS — EXTENSION OF FINDINGS.....	49
25.1 Granting authority checks, reviews and audits.....	49
25.2 European Commission checks, reviews and audits in grants of other granting authorities.....	51
25.3 Access to records for assessing simplified forms of funding.....	51
25.4 OLAF, EPPO and ECA audits and investigations.....	51
25.5 Consequences of checks, reviews, audits and investigations — Extension of results of reviews, audits or investigations.....	51
25.6 Consequences of non-compliance.....	53
ARTICLE 26 — IMPACT EVALUATIONS.....	53
26.1 Impact evaluation.....	53
26.2 Consequences of non-compliance.....	53
<b>CHAPTER 5 CONSEQUENCES OF NON-COMPLIANCE.....</b>	<b>53</b>
<b>SECTION 1 REJECTIONS AND GRANT REDUCTION.....</b>	<b>53</b>
ARTICLE 27 — REJECTION OF COSTS AND CONTRIBUTIONS.....	53
27.1 Conditions.....	53
27.2 Procedure.....	53
27.3 Effects.....	54
ARTICLE 28 — GRANT REDUCTION.....	54
28.1 Conditions.....	54
28.2 Procedure.....	54
28.3 Effects.....	54
<b>SECTION 2 SUSPENSION AND TERMINATION.....</b>	<b>55</b>
ARTICLE 29 — PAYMENT DEADLINE SUSPENSION.....	55
29.1 Conditions.....	55
29.2 Procedure.....	55
ARTICLE 30 — PAYMENT SUSPENSION.....	55
30.1 Conditions.....	55
30.2 Procedure.....	56
ARTICLE 31 — GRANT AGREEMENT SUSPENSION.....	56
31.1 Consortium-requested GA suspension.....	56
31.2 EU-initiated GA suspension.....	57
ARTICLE 32 — GRANT AGREEMENT OR BENEFICIARY TERMINATION.....	58
32.1 Consortium-requested GA termination.....	58
32.2 Consortium-requested beneficiary termination.....	59
32.3 EU-initiated GA or beneficiary termination.....	60

<b>SECTION 3</b>	<b>OTHER CONSEQUENCES: DAMAGES AND ADMINISTRATIVE SANCTIONS.....</b>	<b>63</b>
ARTICLE 33	DAMAGES.....	63
33.1	Liability of the granting authority.....	64
33.2	Liability of the beneficiaries.....	64
ARTICLE 34	ADMINISTRATIVE SANCTIONS AND OTHER MEASURES.....	64
<b>SECTION 4</b>	<b>FORCE MAJEURE.....</b>	<b>64</b>
ARTICLE 35	FORCE MAJEURE.....	64
<b>CHAPTER 6</b>	<b>FINAL PROVISIONS.....</b>	<b>65</b>
ARTICLE 36	COMMUNICATION BETWEEN THE PARTIES.....	65
36.1	Forms and means of communication — Electronic management.....	65
36.2	Date of communication.....	65
36.3	Addresses for communication.....	65
ARTICLE 37	INTERPRETATION OF THE AGREEMENT.....	66
ARTICLE 38	CALCULATION OF PERIODS AND DEADLINES.....	66
ARTICLE 39	AMENDMENTS.....	66
39.1	Conditions.....	66
39.2	Procedure.....	66
ARTICLE 40	ACCESSION AND ADDITION OF NEW BENEFICIARIES.....	67
40.1	Accession of the beneficiaries mentioned in the Preamble.....	67
40.2	Addition of new beneficiaries.....	67
ARTICLE 41	TRANSFER OF THE AGREEMENT.....	67
ARTICLE 42	ASSIGNMENTS OF CLAIMS FOR PAYMENT AGAINST THE GRANTING AUTHORITY.....	68
ARTICLE 43	APPLICABLE LAW AND SETTLEMENT OF DISPUTES.....	68
43.1	Applicable law.....	68
43.2	Dispute settlement.....	68
ARTICLE 44	ENTRY INTO FORCE.....	68

## DATA SHEET

### 1. General data

Project summary:

Project summary
The goal of the project is to support the activities of National Coordination Centre (NCC-CZ) in the Czech Republic, which is a part of the network of National Coordination Centres. The authority responsible for NCC-CZ is the National Cyber Information and Security Agency (NUKIB), which will be supported by an affiliated entity - Cyber Security Hub (CSH). The NCC-CZ will carry out the activities in line with the relevant European regulation (EU) 2021/887. NCC-CZ will cooperate with the European Competence Centre and with the other NCCs within the Network. The NCC-CZ 2.0 project also includes substantial financial support to third parties with a focus on SMEs and other stakeholders. All the planned activities are described in detail in the project application.

Keywords:

- Cybersecurity
- SME support
- financial support to third parties (FSTP), community support, NCC Network, cross-border cooperation, ECCC

Project number: 101227749

Project name: National Coordination Centre 2.0 – The Czech Republic

Project acronym: NCC-CZ 2.0

Call: DIGITAL-ECCC-2024-DEPLOY-NCC-06

Topic: DIGITAL-ECCC-2024-DEPLOY-NCC-06-MS-COORDINATION

Type of action: DIGITAL Simple Grants

Granting authority: European Cybersecurity Industrial, Technology and Research Competence Centre

Grant managed through EU Funding & Tenders Portal: Yes (eGrants)

Project starting date: fixed date: 1 January 2026

Project end date: 31 December 2029

Project duration: 48 months

Consortium agreement: Yes

### 2. Participants

List of participants:

Nº	Role	Short name	Legal name	Ctry	PIC	Total eligible costs (BEN and AE)	Max grant amount
1	COO	NUKIB	NARODNI URAD PRO KYBERNETICKOU A INFORMACNI BEZPECNOST - NUKIB	CZ	907198418	4 178 350.00	2 089 175.00
1.1	AE	CSH	CYBERSECURITY HUB, ZU	CZ	889292509	819 994.50	409 997.25
<b>Total</b>						4 998 344.50	2 499 172.25

Coordinator:

- NARODNI URAD PRO KYBERNETICKOU A INFORMACNI BEZPECNOST - NUKIB (NUKIB)



### 3. Grant

#### Maximum grant amount, total estimated eligible costs and contributions and funding rate:

Total eligible costs (BEN and AE)	Funding rate (%)	Maximum grant amount (Annex 2)	Maximum grant amount (award decision)
4 998 344.50	50	2 499 172.25	2 499 172.25

**Grant form:** Budget-based

**Grant mode:** Action grant

#### Budget categories/activity types:

- 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 Internally invoiced goods and services
- E. Indirect costs

#### Cost eligibility options:

- Standard supplementary payments
- Average personnel costs (unit cost according to usual cost accounting practices)
- Country restrictions for subcontracting costs
- Limitation for subcontracting
- Travel and subsistence:
  - Travel: Actual costs
  - Accommodation: Actual costs
  - Subsistence: Actual costs
- Equipment: depreciation only
- Costs for providing financial support to third parties (actual cost; max amount for each recipient: EUR 100 000.00)
- Indirect cost flat-rate: 7% of the eligible direct costs (categories A-D, except volunteers costs and exempted specific cost categories, if any)
- VAT: Yes
- Country restrictions for eligible costs
- Other ineligible costs

**Budget flexibility:** Yes (no flexibility cap)

#### 4. Reporting, payments and recoveries

##### 4.1 Continuous reporting (art 21)

**Deliverables:** see Funding & Tenders Portal Continuous Reporting tool

##### 4.2 Periodic reporting and payments

**Reporting and payment schedule** (art 21, 22):

Reporting					Payments	
Reporting periods			Type	Deadline	Type	Deadline (time to pay)
RP No	Month from	Month to				
					Initial prefinancing	30 days from entry into force/10 days before starting date/ financial guarantee (if required) – whichever is the latest
					Interim payment	90 days from receiving periodic report
					Interim payment	90 days from receiving periodic report
					Final payment	90 days from receiving periodic report

**Prefinancing payments and guarantees:**

Prefinancing payment		Prefinancing guarantee		
Type	Amount	Guarantee amount	Division per participant	
Prefinancing 1 (initial)	1 999 337.80	n/a	1 - NUKIB	n/a
			1.1 - CSH	n/a

**Reporting and payment modalities** (art 21, 22):

Mutual Insurance Mechanism (MIM): No

Restrictions on distribution of initial prefinancing: The prefinancing may be distributed only if the minimum number of beneficiaries set out in the call conditions (if any) have acceded to the Agreement and only to beneficiaries that have acceded.

Interim payment ceiling (if any): 90% of the maximum grant amount

No-profit rule: Yes

Late payment interest: ECB + 3.5%

Bank account for payments:

██████████ ██████████

Conversion into euros: Double conversion

Reporting language: Language of the Agreement

#### **4.3 Certificates** (art 24):

Certificates on the financial statements (CFS):

Conditions:

Schedule: only at final payment, if threshold is reached

Standard threshold (beneficiary-level):

- financial statement: requested EU contribution to costs  $\geq$  EUR 325 000.00

#### **4.4 Recoveries** (art 22)

**First-line liability for recoveries:**

Beneficiary termination: Beneficiary concerned

Final payment: Coordinator

After final payment: Beneficiary concerned

**Joint and several liability for enforced recoveries (in case of non-payment):**

Limited joint and several liability of other beneficiaries — up to the maximum grant amount of the beneficiary

Joint and several liability of affiliated entities — n/a

### **5. Consequences of non-compliance, applicable law & dispute settlement forum**

**Applicable law** (art 43):

Standard applicable law regime: EU law + law of Belgium

**Dispute settlement forum** (art 43):

Standard dispute settlement forum:

EU beneficiaries: EU General Court + EU Court of Justice (on appeal)

Non-EU beneficiaries: Courts of Brussels, Belgium (unless an international agreement provides for the enforceability of EU court judgements)

### **6. Other**

**Specific rules (Annex 5):** Yes

**Standard time-limits after project end:**

Confidentiality (for X years after final payment): 5

Record-keeping (for X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Reviews (up to X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Audits (up to X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)



Extension of findings from other grants to this grant (no later than X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

Impact evaluation (up to X years after final payment): 5 (or 3 for grants of not more than EUR 60 000)

## **CHAPTER 1 GENERAL**

### **ARTICLE 1 — SUBJECT OF THE AGREEMENT**

This Agreement sets out the rights and obligations and terms and conditions applicable to the grant awarded for the implementation of the action set out in Chapter 2.

### **ARTICLE 2 — DEFINITIONS**

For the purpose of this Agreement, the following definitions apply:

**Actions** — The project which is being funded in the context of this Agreement.

**Grant** — The grant awarded in the context of this Agreement.

**EU grants** — Grants awarded by EU institutions, bodies, offices or agencies (including EU executive agencies, EU regulatory agencies, EDA, joint undertakings, etc.).

**Participants** — Entities participating in the action as beneficiaries, affiliated entities, associated partners, third parties giving in-kind contributions, subcontractors or recipients of financial support to third parties.

**Beneficiaries (BEN)** — The signatories of this Agreement (either directly or through an accession form).

**Affiliated entities (AE)** — Entities affiliated to a beneficiary within the meaning of Article 187 of EU Financial Regulation 2018/1046<sup>4</sup> which participate in the action with similar rights and obligations as the beneficiaries (obligation to implement action tasks and right to charge costs and claim contributions).

**Associated partners (AP)** — Entities which participate in the action, but without the right to charge costs or claim contributions.

**Purchases** — Contracts for goods, works or services needed to carry out the action (e.g. equipment, consumables and supplies) but which are not part of the action tasks (see Annex 1).

**Subcontracting** — Contracts for goods, works or services that are part of the action tasks (see Annex 1).

**In-kind contributions** — In-kind contributions within the meaning of Article 2(36) of EU Financial

---

<sup>4</sup> For the definition, see Article 187 Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 ('EU Financial Regulation') (OJ L 193, 30.7.2018, p. 1): "**affiliated entities** [are]:

- (a) entities that form a sole beneficiary [(i.e. where an entity is formed of several entities that satisfy the criteria for being awarded a grant, including where the entity is specifically established for the purpose of implementing an action to be financed by a grant)];
- (b) entities that satisfy the eligibility criteria and that do not fall within one of the situations referred to in Article 136(1) and 141(1) and that have a link with the beneficiary, in particular a legal or capital link, which is neither limited to the action nor established for the sole purpose of its implementation".

Regulation 2018/1046, i.e. non-financial resources made available free of charge by third parties.

**Fraud** — Fraud within the meaning of Article 3 of EU Directive 2017/1371<sup>5</sup> and Article 1 of the Convention on the protection of the European Communities' financial interests, drawn up by the Council Act of 26 July 1995<sup>6</sup>, as well as any other wrongful or criminal deception intended to result in financial or personal gain.

**Irregularities** — Any type of breach (regulatory or contractual) which could impact the EU financial interests, including irregularities within the meaning of Article 1(2) of EU Regulation 2988/95<sup>7</sup>.

**Grave professional misconduct** — Any type of unacceptable or improper behaviour in exercising one's profession, especially by employees, including grave professional misconduct within the meaning of Article 136(1)(c) of EU Financial Regulation 2018/1046.

**Applicable EU, international and national law** — Any legal acts or other (binding or non-binding) rules and guidance in the area concerned.

**Portal** — EU Funding & Tenders Portal; electronic portal and exchange system managed by the European Commission and used by itself and other EU institutions, bodies, offices or agencies for the management of their funding programmes (grants, procurements, prizes, etc.).

## **CHAPTER 2 ACTION**

### **ARTICLE 3 — ACTION**

The grant is awarded for the action **101227749 — NCC-CZ 2.0** ('action'), as described in Annex 1.

### **ARTICLE 4 — DURATION AND STARTING DATE**

The duration and the starting date of the action are set out in the Data Sheet (see Point 1).

## **CHAPTER 3 GRANT**

### **ARTICLE 5 — GRANT**

#### **5.1 Form of grant**

The grant is an action grant<sup>8</sup> which takes the form of a budget-based mixed actual cost grant (i.e. a

<sup>5</sup> Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law (OJ L 198, 28.7.2017, p. 29).

<sup>6</sup> OJ C 316, 27.11.1995, p. 48.

<sup>7</sup> Council Regulation (EC, Euratom) No 2988/95 of 18 December 1995 on the protection of the European Communities financial interests (OJ L 312, 23.12.1995, p. 1).

<sup>8</sup> For the definition, see Article 183(2)(a) EU Financial Regulation 2024/2509: '**action grant**' means an EU grant to finance "an action intended to help achieve a Union policy objective".

grant based on actual costs incurred, but which may also include other forms of funding, such as unit costs or contributions, flat-rate costs or contributions, lump sum costs or contributions or financing not linked to costs).

## 5.2 Maximum grant amount

The maximum grant amount is set out in the Data Sheet (see Point 3) and in the estimated budget (Annex 2).

## 5.3 Funding rate

The funding rate for costs is 50% of the action's eligible costs.

Contributions are not subject to any funding rate.

## 5.4 Estimated budget, budget categories and forms of funding

The estimated budget for the action is set out in Annex 2.

It contains the estimated eligible costs and contributions for the action, broken down by participant and budget category.

Annex 2 also shows the types of costs and contributions (forms of funding)<sup>9</sup> to be used for each budget category.

If unit costs or contributions are used, the details on the calculation will be explained in Annex 2a.

## 5.5 Budget flexibility

The budget breakdown may be adjusted — without an amendment (see Article 39) — by transfers (between participants and budget categories), as long as this does not imply any substantive or important change to the description of the action in Annex 1.

However:

- changes to the budget category for volunteers (if used) always require an amendment
- changes to budget categories with lump sums costs or contributions (if used; including financing not linked to costs) always require an amendment
- changes to budget categories with higher funding rates or budget ceilings (if used) always require an amendment
- addition of amounts for subcontracts not provided for in Annex 1 either require an amendment or simplified approval in accordance with Article 6.2
- other changes require an amendment or simplified approval, if specifically provided for in Article 6.2
- flexibility caps: not applicable.

---

<sup>9</sup> See Article 125 EU Financial Regulation 2024/2509.

## ARTICLE 6 — ELIGIBLE AND INELIGIBLE COSTS AND CONTRIBUTIONS

In order to be eligible, costs and contributions must meet the **eligibility** conditions set out in this Article.

### 6.1 General eligibility conditions

The **general eligibility conditions** are the following:

(a) for actual costs:

- (i) they must be actually incurred by the beneficiary
- (ii) they must be incurred in the period set out in Article 4 (with the exception of costs relating to the submission of the final periodic report, which may be incurred afterwards; see Article 21)
- (iii) they must be declared under one of the budget categories set out in Article 6.2 and Annex 2
- (iv) they must be incurred in connection with the action as described in Annex 1 and necessary for its implementation
- (v) they must be identifiable and verifiable, in particular recorded in the beneficiary's accounts in accordance with the accounting standards applicable in the country where the beneficiary is established and with the beneficiary's usual cost accounting practices
- (vi) they must comply with the applicable national law on taxes, labour and social security and
- (vii) they must be reasonable, justified and must comply with the principle of sound financial management, in particular regarding economy and efficiency

(b) for unit costs or contributions (if any):

- (i) they must be declared under one of the budget categories set out in Article 6.2 and Annex 2
- (ii) the units must:
  - be actually used or produced by the beneficiary in the period set out in Article 4 (with the exception of units relating to the submission of the final periodic report, which may be used or produced afterwards; see Article 21)
  - be necessary for the implementation of the action and
- (iii) the number of units must be identifiable and verifiable, in particular supported by records and documentation (see Article 20)

(c) for flat-rate costs or contributions (if any):

- (i) they must be declared under one of the budget categories set out in Article 6.2 and Annex 2



- (ii) the costs or contributions to which the flat-rate is applied must:
  - be eligible
  - relate to the period set out in Article 4 (with the exception of costs or contributions relating to the submission of the final periodic report, which may be incurred afterwards; see Article 21)
- (d) for lump sum costs or contributions (if any):
  - (i) they must be declared under one of the budget categories set out in Article 6.2 and Annex 2
  - (ii) the work must be properly implemented by the beneficiary in accordance with Annex 1
  - (iii) the deliverables/outputs must be achieved in the period set out in Article 4 (with the exception of deliverables/outputs relating to the submission of the final periodic report, which may be achieved afterwards; see Article 21)
- (e) for unit, flat-rate or lump sum costs or contributions according to usual cost accounting practices (if any):
  - (i) they must fulfil the general eligibility conditions for the type of cost concerned
  - (ii) the cost accounting practices must be applied in a consistent manner, based on objective criteria, regardless of the source of funding
- (f) for financing not linked to costs (if any): the results must be achieved or the conditions must be fulfilled as described in Annex 1.

In addition, for direct cost categories (e.g. personnel, travel & subsistence, subcontracting and other direct costs) only costs that are directly linked to the action implementation and can therefore be attributed to it directly are eligible. They must not include any indirect costs (i.e. costs that are only indirectly linked to the action, e.g. via cost drivers).

## 6.2 Specific eligibility conditions for each budget category

For each budget category, the **specific eligibility conditions** are as follows:

### Direct costs

#### **A. Personnel costs**

**A.1 Costs for employees (or equivalent)** are eligible as personnel costs, if they fulfil the general eligibility conditions and are related to personnel working for the beneficiary under an employment contract (or equivalent appointing act) and assigned to the action.

They must be limited to salaries, social security contributions, taxes and other costs linked to the remuneration, if they arise from national law or the employment contract (or equivalent appointing act) and be calculated on the basis of the costs actually incurred, in accordance with the following method:

{daily rate for the person  
multiplied by  
number of day-equivalents worked on the action (rounded up or down to the nearest half-day)}.

The daily rate must be calculated as:

{annual personnel costs for the person  
divided by  
215}.

The number of day-equivalents declared for a person must be identifiable and verifiable (see Article 20).

The total number of day-equivalents declared in EU grants, for a person for a year, cannot be higher than 215.

The personnel costs may also include supplementary payments for personnel assigned to the action (including payments on the basis of supplementary contracts regardless of their nature), if:

- it is part of the beneficiary's usual remuneration practices and is paid in a consistent manner whenever the same kind of work or expertise is required
- the criteria used to calculate the supplementary payments are objective and generally applied by the beneficiary, regardless of the source of funding used.

If the beneficiary uses average personnel costs (unit cost according to usual cost accounting practices), the personnel costs must fulfil the general eligibility conditions for such unit costs and the daily rate must be calculated:

- using the actual personnel costs recorded in the beneficiary's accounts and excluding any costs which are ineligible or already included in other budget categories; the actual personnel costs may be adjusted on the basis of budgeted or estimated elements, if they are relevant for calculating the personnel costs, reasonable and correspond to objective and verifiable information

and

- according to usual cost accounting practices which are applied in a consistent manner, based on objective criteria, regardless of the source of funding.

**A.2 and A.3 Costs for natural persons working under a direct contract** other than an employment contract and costs for **seconded persons by a third party against payment** are also eligible as personnel costs, if they are assigned to the action, fulfil the general eligibility conditions and:

- (a) work under conditions similar to those of an employee (in particular regarding the way the work is organised, the tasks that are performed and the premises where they are performed) and
- (b) the result of the work belongs to the beneficiary (unless agreed otherwise).

They must be calculated on the basis of a rate which corresponds to the costs actually incurred for

the direct contract or secondment and must not be significantly different from those for personnel performing similar tasks under an employment contract with the beneficiary.

**A.4** The work of **SME owners** for the action (i.e. owners of beneficiaries that are small and medium-sized enterprises<sup>10</sup> not receiving a salary) or **natural person beneficiaries** (i.e. beneficiaries that are natural persons not receiving a salary) may be declared as personnel costs, if they fulfil the general eligibility conditions and are calculated as unit costs in accordance with the method set out in Annex 2a.

## B. Subcontracting costs

**Subcontracting costs** for the action (including related duties, taxes and charges, such as non-deductible or non-refundable value added tax (VAT)) are eligible, if they are calculated on the basis of the costs actually incurred, fulfil the general eligibility conditions and are awarded using the beneficiary's usual purchasing practices — provided these ensure subcontracts with best value for money (or if appropriate the lowest price) and that there is no conflict of interests (see Article 12).

Beneficiaries that are 'contracting authorities/entities' within the meaning of the EU Directives on public procurement must also comply with the applicable national law on public procurement.

The beneficiaries must ensure that the subcontracted work is performed in the eligible countries or target countries set out in the call conditions — unless otherwise approved by the granting authority.

Subcontracting may cover only a limited part of the action.

The tasks to be subcontracted and the estimated cost for each subcontract must be set out in Annex 1 and the total estimated costs of subcontracting per beneficiary must be set out in Annex 2 (or may be approved ex post in the periodic report, if the use of subcontracting does not entail changes to the Agreement which would call into question the decision awarding the grant or breach the principle of equal treatment of applicants; 'simplified approval procedure').

## C. Purchase costs

**Purchase costs** for the action (including related duties, taxes and charges, such as non-deductible or non-refundable value added tax (VAT)) are eligible if they fulfil the general eligibility conditions and are bought using the beneficiary's usual purchasing practices — provided these ensure purchases with best value for money (or if appropriate the lowest price) and that there is no conflict of interests (see Article 12).

Beneficiaries that are 'contracting authorities/entities' within the meaning of the EU Directives on public procurement must also comply with the applicable national law on public procurement.

---

<sup>10</sup> For the definition, see Commission Recommendation 2003/361/EC: micro, small or medium-sized enterprise (SME) are enterprises

- engaged in an economic activity, irrespective of their legal form (including, in particular, self-employed persons and family businesses engaged in craft or other activities, and partnerships or associations regularly engaged in an economic activity) and
- employing fewer than 250 persons (expressed in 'annual working units' as defined in Article 5 of the Recommendation) and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.

## C.1 Travel and subsistence

Purchases for **travel, accommodation and subsistence** must be calculated as follows:

- travel: on the basis of the costs actually incurred and in line with the beneficiary's usual practices on travel
- accommodation: on the basis of the costs actually incurred and in line with the beneficiary's usual practices on travel
- subsistence: on the basis of the costs actually incurred and in line with the beneficiary's usual practices on travel .

## C.2 Equipment

Purchases of **equipment, infrastructure or other assets** used for the action must be declared as depreciation costs, calculated on the basis of the costs actually incurred and written off in accordance with international accounting standards and the beneficiary's usual accounting practices.

Only the portion of the costs that corresponds to the rate of actual use for the action during the action duration can be taken into account.

Costs for **renting or leasing** equipment, infrastructure or other assets are also eligible, if they do not exceed the depreciation costs of similar equipment, infrastructure or assets and do not include any financing fees.

## C.3 Other goods, works and services

Purchases of **other goods, works and services** must be calculated on the basis of the costs actually incurred.

Such goods, works and services include, for instance, consumables and supplies, promotion, dissemination, protection of results, translations, publications, certificates and financial guarantees, if required under the Agreement.

## D. Other cost categories

### D.1 Financial support to third parties

**Costs for providing financial support to third parties** (in the form of **grants, prizes** or similar forms of support; if any) are eligible, if and as declared eligible in the call conditions, if they fulfil the general eligibility conditions, are calculated on the basis of the costs actually incurred and the support is implemented in accordance with the conditions set out in Annex 1.

These conditions must ensure objective and transparent selection procedures and include at least the following:

- (a) for grants (or similar):
  - (i) the maximum amount of financial support for each third party ('recipient'); this amount may not exceed the amount set out in the Data Sheet (see Point 3) or otherwise agreed with the granting authority

- (ii) the criteria for calculating the exact amount of the financial support
- (iii) the different types of activity that qualify for financial support, on the basis of a closed list
- (iv) the persons or categories of persons that will be supported and
- (v) the criteria and procedures for giving financial support
- (b) for prizes (or similar):
  - (i) the eligibility and award criteria
  - (ii) the amount of the prize and
  - (iii) the payment arrangements.

## D.2 Internally invoiced goods and services

**Costs for internally invoiced goods and services** directly used for the action may be declared as unit cost according to usual cost accounting practices, if and as declared eligible in the call conditions, if they fulfil the general eligibility conditions for such unit costs and the amount per unit is calculated:

- using the actual costs for the good or service recorded in the beneficiary's accounts, attributed either by direct measurement or on the basis of cost drivers, and excluding any cost which are ineligible or already included in other budget categories; the actual costs may be adjusted on the basis of budgeted or estimated elements, if they are relevant for calculating the costs, reasonable and correspond to objective and verifiable information

and

- according to usual cost accounting practices which are applied in a consistent manner, based on objective criteria, regardless of the source of funding.

'Internally invoiced goods and services' means goods or services which are provided within the beneficiary's organisation directly for the action and which the beneficiary values on the basis of its usual cost accounting practices.

### Indirect costs

## E. Indirect costs

**Indirect costs** will be reimbursed at the flat-rate of 7% of the eligible direct costs (categories A-D, except volunteers costs and exempted specific cost categories, if any).

### Contributions

Not applicable

## 6.3 Ineligible costs and contributions

The following costs or contributions are **ineligible**:

- (a) costs or contributions that do not comply with the conditions set out above (Article 6.1 and 6.2), in particular:
  - (i) costs related to return on capital and dividends paid by a beneficiary
  - (ii) debt and debt service charges
  - (iii) provisions for future losses or debts
  - (iv) interest owed
  - (v) currency exchange losses
  - (vi) bank costs charged by the beneficiary's bank for transfers from the granting authority
  - (vii) excessive or reckless expenditure
  - (viii) deductible or refundable VAT (including VAT paid by public bodies acting as public authority)
  - (ix) costs incurred or contributions for activities implemented during grant agreement suspension (see Article 31)
  - (x) in-kind contributions by third parties
- (b) costs or contributions declared under other EU grants (or grants awarded by an EU Member State, non-EU country or other body implementing the EU budget), except for the following cases:
  - (i) Synergy actions: not applicable
  - (ii) if the action grant is combined with an operating grant<sup>11</sup> running during the same period and the beneficiary can demonstrate that the operating grant does not cover any (direct or indirect) costs of the action grant
- (c) costs or contributions for staff of a national (or regional/local) administration, for activities that are part of the administration's normal activities (i.e. not undertaken only because of the grant)
- (d) costs or contributions (especially travel and subsistence) for staff or representatives of EU institutions, bodies or agencies
- (e) other :
  - (i) costs or contributions for activities that do not take place in one of the eligible countries or target countries set out in the call conditions — unless approved by the granting authority
  - (ii) costs or contributions declared specifically ineligible in the call conditions.

## 6.4 Consequences of non-compliance

---

<sup>11</sup> For the definition, see Article 183(2)(b) EU Financial Regulation 2024/2509: '**operating grant**' means an EU grant to finance "the functioning of a body which has an objective forming part of and supporting an EU policy".

If a beneficiary declares costs or contributions that are ineligible, they will be rejected (see Article 27).

This may also lead to other measures described in Chapter 5.

## **CHAPTER 4 GRANT IMPLEMENTATION**

### **SECTION 1 CONSORTIUM: BENEFICIARIES, AFFILIATED ENTITIES AND OTHER PARTICIPANTS**

#### **ARTICLE 7 — BENEFICIARIES**

The beneficiaries, as signatories of the Agreement, are fully responsible towards the granting authority for implementing it and for complying with all its obligations.

They must implement the Agreement to their best abilities, in good faith and in accordance with all the obligations and terms and conditions it sets out.

They must have the appropriate resources to implement the action and implement the action under their own responsibility and in accordance with Article 11. If they rely on affiliated entities or other participants (see Articles 8 and 9), they retain sole responsibility towards the granting authority and the other beneficiaries.

They are jointly responsible for the *technical* implementation of the action. If one of the beneficiaries fails to implement their part of the action, the other beneficiaries must ensure that this part is implemented by someone else (without being entitled to an increase of the maximum grant amount and subject to an amendment; see Article 39). The *financial* responsibility of each beneficiary in case of recoveries is governed by Article 22.

The beneficiaries (and their action) must remain eligible under the EU programme funding the grant for the entire duration of the action. Costs and contributions will be eligible only as long as the beneficiary and the action are eligible.

The **internal roles and responsibilities** of the beneficiaries are divided as follows:

(a) Each beneficiary must:

- (i) keep information stored in the Portal Participant Register up to date (see Article 19)
- (ii) inform the granting authority (and the other beneficiaries) immediately of any events or circumstances likely to affect significantly or delay the implementation of the action (see Article 19)
- (iii) submit to the coordinator in good time:
  - the prefinancing guarantees (if required; see Article 23)
  - the financial statements and certificates on the financial statements (CFS) (if required; see Articles 21 and 24.2 and Data Sheet, Point 4.3)
  - the contribution to the deliverables and technical reports (see Article 21)

- any other documents or information required by the granting authority under the Agreement
- (iv) submit via the Portal data and information related to the participation of their affiliated entities.
- (b) The coordinator must:
  - (i) monitor that the action is implemented properly (see Article 11)
  - (ii) act as the intermediary for all communications between the consortium and the granting authority, unless the Agreement or granting authority specifies otherwise, and in particular:
    - submit the prefinancing guarantees to the granting authority (if any)
    - request and review any documents or information required and verify their quality and completeness before passing them on to the granting authority
    - submit the deliverables and reports to the granting authority
    - inform the granting authority about the payments made to the other beneficiaries (report on the distribution of payments; if required, see Articles 22 and 32)
  - (iii) distribute the payments received from the granting authority to the other beneficiaries without unjustified delay (see Article 22).

The coordinator may not delegate or subcontract the above-mentioned tasks to any other beneficiary or third party (including affiliated entities).

However, coordinators which are public bodies may delegate the tasks set out in Point (b)(ii) last indent and (iii) above to entities with ‘authorisation to administer’ which they have created or which are controlled by or affiliated to them. In this case, the coordinator retains sole responsibility for the payments and for compliance with the obligations under the Agreement.

Moreover, coordinators which are ‘sole beneficiaries’<sup>12</sup> (or similar, such as European research infrastructure consortia (ERICs)) may delegate the tasks set out in Point (b)(i) to (iii) above to one of their members. The coordinator retains sole responsibility for compliance with the obligations under the Agreement.

The beneficiaries must have **internal arrangements** regarding their operation and co-ordination, to ensure that the action is implemented properly.

If required by the granting authority (see Data Sheet, Point 1), these arrangements must be set out in a written **consortium agreement** between the beneficiaries, covering for instance:

- the internal organisation of the consortium

---

<sup>12</sup> For the definition, see Article 187(2) EU Financial Regulation 2018/1046: “Where several entities satisfy the criteria for being awarded a grant and together form one entity, that entity may be treated as the **sole beneficiary**, including where it is specifically established for the purpose of implementing the action financed by the grant.”



- the management of access to the Portal
- different distribution keys for the payments and financial responsibilities in case of recoveries (if any)
- additional rules on rights and obligations related to background and results (see Article 16)
- settlement of internal disputes
- liability, indemnification and confidentiality arrangements between the beneficiaries.

The internal arrangements must not contain any provision contrary to this Agreement.

## ARTICLE 8 — AFFILIATED ENTITIES

The following entities which are linked to a beneficiary will participate in the action as ‘affiliated entities’:

- **CYBERSECURITY HUB, ZU (CSH)**, PIC 889292509, linked to NARODNI URAD PRO KYBERNETICKOU A INFORMACNI BEZPECNOST - NUKIB (NUKIB)

Affiliated entities can charge costs and contributions to the action under the same conditions as the beneficiaries and must implement the action tasks attributed to them in Annex 1 in accordance with Article 11.

Their costs and contributions will be included in Annex 2 and will be taken into account for the calculation of the grant.

The beneficiaries must ensure that all their obligations under this Agreement also apply to their affiliated entities.

The beneficiaries must ensure that the bodies mentioned in Article 25 (e.g. granting authority, OLAF, Court of Auditors (ECA), etc.) can exercise their rights also towards the affiliated entities.

Breaches by affiliated entities will be handled in the same manner as breaches by beneficiaries. Recovery of undue amounts will be handled through the beneficiaries.

If the granting authority requires joint and several liability of affiliated entities (see Data Sheet, Point 4.4), they must sign the declaration set out in Annex 3a and may be held liable in case of enforced recoveries against their beneficiaries (see Article 22.2 and 22.4).

## ARTICLE 9 — OTHER PARTICIPANTS INVOLVED IN THE ACTION

### 9.1 Associated partners

Not applicable

### 9.2 Third parties giving in-kind contributions to the action

Other third parties may give in-kind contributions to the action (i.e. personnel, equipment, other goods, works and services, etc. which are free-of-charge), if necessary for the implementation.

Third parties giving in-kind contributions do not implement any action tasks. They may not charge costs or contributions to the action and the costs for the in-kind contributions are not eligible.

The third parties and their in-kind contributions should be set out in Annex 1.

### 9.3 Subcontractors

Subcontractors may participate in the action, if necessary for the implementation.

Subcontractors must implement their action tasks in accordance with Article 11. The costs for the subcontracted tasks (invoiced price from the subcontractor) are eligible and may be charged by the beneficiaries, under the conditions set out in Article 6. The costs will be included in Annex 2 as part of the beneficiaries' costs.

The beneficiaries must ensure that their contractual obligations under Articles 11 (proper implementation), 12 (conflict of interest), 13 (confidentiality and security), 14 (ethics), 17.2 (visibility), 18 (specific rules for carrying out action), 19 (information) and 20 (record-keeping) also apply to the subcontractors.

The beneficiaries must ensure that the bodies mentioned in Article 25 (e.g. granting authority, OLAF, Court of Auditors (ECA), etc.) can exercise their rights also towards the subcontractors.

### 9.4 Recipients of financial support to third parties

If the action includes providing financial support to third parties (e.g. grants, prizes or similar forms of support), the beneficiaries must ensure that their contractual obligations under Articles 12 (conflict of interest), 13 (confidentiality and security), 14 (ethics), 17.2 (visibility), 18 (specific rules for carrying out action), 19 (information) and 20 (record-keeping) also apply to the third parties receiving the support (recipients).

The beneficiaries must also ensure that the bodies mentioned in Article 25 (e.g. granting authority, OLAF, Court of Auditors (ECA), etc.) can exercise their rights also towards the recipients.

## ARTICLE 10 — PARTICIPANTS WITH SPECIAL STATUS

### 10.1 Non-EU participants

Participants which are established in a non-EU country (if any) undertake to comply with their obligations under the Agreement and:

- to respect general principles (including fundamental rights, values and ethical principles, environmental and labour standards, rules on classified information, intellectual property rights, visibility of funding and protection of personal data)
- for the submission of certificates under Article 24: to use qualified external auditors which are independent and comply with comparable standards as those set out in EU Directive 2006/43/EC<sup>13</sup>

---

<sup>13</sup> Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts or similar national regulations (OJ L 157, 9.6.2006, p. 87).

- for the controls under Article 25: to allow for checks, reviews, audits and investigations (including on-the-spot checks, visits and inspections) by the bodies mentioned in that Article (e.g. granting authority, OLAF, Court of Auditors (ECA), etc.).

Special rules on dispute settlement apply (see Data Sheet, Point 5).

## 10.2 Participants which are international organisations

Participants which are international organisations (IOs; if any) undertake to comply with their obligations under the Agreement and:

- to respect general principles (including fundamental rights, values and ethical principles, environmental and labour standards, rules on classified information, intellectual property rights, visibility of funding and protection of personal data)
- for the submission of certificates under Article 24: to use either independent public officers or external auditors which comply with comparable standards as those set out in EU Directive 2006/43/EC
- for the controls under Article 25: to allow for the checks, reviews, audits and investigations by the bodies mentioned in that Article, taking into account the specific agreements concluded by them and the EU (if any).

For such participants, nothing in the Agreement will be interpreted as a waiver of their privileges or immunities, as accorded by their constituent documents or international law.

Special rules on applicable law and dispute settlement apply (see Article 43 and Data Sheet, Point 5).

## 10.3 Pillar-assessed participants

Pillar-assessed participants (if any) may rely on their own systems, rules and procedures, in so far as they have been positively assessed and do not call into question the decision awarding the grant or breach the principle of equal treatment of applicants or beneficiaries.

‘Pillar-assessment’ means a review by the European Commission on the systems, rules and procedures which participants use for managing EU grants (in particular internal control system, accounting system, external audits, financing of third parties, rules on recovery and exclusion, information on recipients and protection of personal data; see Article 154 EU Financial Regulation 2018/1046).

Participants with a positive pillar assessment may rely on their own systems, rules and procedures, in particular for:

- record-keeping (Article 20): may be done in accordance with internal standards, rules and procedures
- currency conversion for financial statements (Article 21): may be done in accordance with usual accounting practices
- guarantees (Article 23): for public law bodies, prefinancing guarantees are not needed
- certificates (Article 24):

- certificates on the financial statements (CFS): may be provided by their regular internal or external auditors and in accordance with their internal financial regulations and procedures
- certificates on usual accounting practices (CoMUC): are not needed if those practices are covered by an ex-ante assessment

and use the following specific rules, for:

- recoveries (Article 22): in case of financial support to third parties, there will be no recovery if the participant has done everything possible to retrieve the undue amounts from the third party receiving the support (including legal proceedings) and non-recovery is not due to an error or negligence on its part
- checks, reviews, audits and investigations by the EU (Article 25): will be conducted taking into account the rules and procedures specifically agreed between them and the framework agreement (if any)
- impact evaluation (Article 26): will be conducted in accordance with the participant's internal rules and procedures and the framework agreement (if any)
- grant agreement suspension (Article 31): certain costs incurred during grant suspension are eligible (notably, minimum costs necessary for a possible resumption of the action and costs relating to contracts which were entered into before the pre-information letter was received and which could not reasonably be suspended, reallocated or terminated on legal grounds)
- grant agreement termination (Article 32): the final grant amount and final payment will be calculated taking into account also costs relating to contracts due for execution only after termination takes effect, if the contract was entered into before the pre-information letter was received and could not reasonably be terminated on legal grounds
- liability for damages (Article 33.2): the granting authority must be compensated for damage it sustains as a result of the implementation of the action or because the action was not implemented in full compliance with the Agreement only if the damage is due to an infringement of the participant's internal rules and procedures or due to a violation of third parties' rights by the participant or one of its employees or individual for whom the employees are responsible.

Participants whose pillar assessment covers procurement and granting procedures may also do purchases, subcontracting and financial support to third parties (Article 6.2) in accordance with their internal rules and procedures for purchases, subcontracting and financial support.

Participants whose pillar assessment covers data protection rules may rely on their internal standards, rules and procedures for data protection (Article 15).

The participants may however not rely on provisions which would breach the principle of equal treatment of applicants or beneficiaries or call into question the decision awarding the grant, such as in particular:

- eligibility (Article 6)

- consortium roles and set-up (Articles 7-9)
- security and ethics (Articles 13, 14)
- IPR (including background and results, access rights and rights of use), communication, dissemination and visibility (Articles 16 and 17)
- information obligation (Article 19)
- payment, reporting and amendments (Articles 21, 22 and 39)
- rejections, reductions, suspensions and terminations (Articles 27, 28, 29-32)

If the pillar assessment was subject to remedial measures, reliance on the internal systems, rules and procedures is subject to compliance with those remedial measures.

Participants whose assessment has not yet been updated to cover (the new rules on) data protection may rely on their internal systems, rules and procedures, provided that they ensure that personal data is:

- processed lawfully, fairly and in a transparent manner in relation to the data subject
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed and
- processed in a manner that ensures appropriate security of the personal data.

Participants must inform the coordinator without delay of any changes to the systems, rules and procedures that were part of the pillar assessment. The coordinator must immediately inform the granting authority.

Pillar-assessed participants that have also concluded a framework agreement with the EU, may moreover — under the same conditions as those above (i.e. not call into question the decision awarding the grant or breach the principle of equal treatment of applicants or beneficiaries) — rely on the provisions set out in that framework agreement.

## **SECTION 2 RULES FOR CARRYING OUT THE ACTION**

### **ARTICLE 11 — PROPER IMPLEMENTATION OF THE ACTION**

#### **11.1 Obligation to properly implement the action**

The beneficiaries must implement the action as described in Annex 1 and in compliance with the provisions of the Agreement, the call conditions and all legal obligations under applicable EU, international and national law.

## **11.2 Consequences of non-compliance**

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

## **ARTICLE 12 — CONFLICT OF INTERESTS**

### **12.1 Conflict of interests**

The beneficiaries must take all measures to prevent any situation where the impartial and objective implementation of the Agreement could be compromised for reasons involving family, emotional life, political or national affinity, economic interest or any other direct or indirect interest ('conflict of interests').

They must formally notify the granting authority without delay of any situation constituting or likely to lead to a conflict of interests and immediately take all the necessary steps to rectify this situation.

The granting authority may verify that the measures taken are appropriate and may require additional measures to be taken by a specified deadline.

### **12.2 Consequences of non-compliance**

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28) and the grant or the beneficiary may be terminated (see Article 32).

Such breaches may also lead to other measures described in Chapter 5.

## **ARTICLE 13 — CONFIDENTIALITY AND SECURITY**

### **13.1 Sensitive information**

The parties must keep confidential any data, documents or other material (in any form) that is identified as sensitive in writing ('sensitive information') — during the implementation of the action and for at least until the time-limit set out in the Data Sheet (see Point 6).

If a beneficiary requests, the granting authority may agree to keep such information confidential for a longer period.

Unless otherwise agreed between the parties, they may use sensitive information only to implement the Agreement.

The beneficiaries may disclose sensitive information to their personnel or other participants involved in the action only if they:

- (a) need to know it in order to implement the Agreement and
- (b) are bound by an obligation of confidentiality.

The granting authority may disclose sensitive information to its staff and to other EU institutions and bodies.

It may moreover disclose sensitive information to third parties, if:

- (a) this is necessary to implement the Agreement or safeguard the EU financial interests and
- (b) the recipients of the information are bound by an obligation of confidentiality.

The confidentiality obligations no longer apply if:

- (a) the disclosing party agrees to release the other party
- (b) the information becomes publicly available, without breaching any confidentiality obligation
- (c) the disclosure of the sensitive information is required by EU, international or national law.

Specific confidentiality rules (if any) are set out in Annex 5.

### **13.2 Classified information**

The parties must handle classified information in accordance with the applicable EU, international or national law on classified information (in particular, Decision 2015/444<sup>14</sup> and its implementing rules).

Deliverables which contain classified information must be submitted according to special procedures agreed with the granting authority.

Action tasks involving classified information may be subcontracted only after explicit approval (in writing) from the granting authority.

Classified information may not be disclosed to any third party (including participants involved in the action implementation) without prior explicit written approval from the granting authority.

Specific security rules (if any) are set out in Annex 5.

### **13.3 Consequences of non-compliance**

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

## **ARTICLE 14 — ETHICS AND VALUES**

### **14.1 Ethics**

The action must be carried out in line with the highest ethical standards and the applicable EU, international and national law on ethical principles.

Specific ethics rules (if any) are set out in Annex 5.

### **14.2 Values**

---

<sup>14</sup> Commission Decision 2015/444/EC, Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

The beneficiaries must commit to and ensure the respect of basic EU values (such as respect for human dignity, freedom, democracy, equality, the rule of law and human rights, including the rights of minorities).

Specific rules on values (if any) are set out in Annex 5.

### **14.3 Consequences of non-compliance**

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

## **ARTICLE 15 — DATA PROTECTION**

### **15.1 Data processing by the granting authority**

Any personal data under the Agreement will be processed under the responsibility of the data controller of the granting authority in accordance with and for the purposes set out in the Portal Privacy Statement.

For grants where the granting authority is the European Commission, an EU regulatory or executive agency, joint undertaking or other EU body, the processing will be subject to Regulation 2018/1725<sup>15</sup>.

### **15.2 Data processing by the beneficiaries**

The beneficiaries must process personal data under the Agreement in compliance with the applicable EU, international and national law on data protection (in particular, Regulation 2016/679<sup>16</sup>).

They must ensure that personal data is:

- processed lawfully, fairly and in a transparent manner in relation to the data subjects
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed and
- processed in a manner that ensures appropriate security of the data.

<sup>15</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

<sup>16</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('GDPR') (OJ L 119, 4.5.2016, p. 1).



The beneficiaries may grant their personnel access to personal data only if it is strictly necessary for implementing, managing and monitoring the Agreement. The beneficiaries must ensure that the personnel is under a confidentiality obligation.

The beneficiaries must inform the persons whose data are transferred to the granting authority and provide them with the Portal Privacy Statement.

### **15.3 Consequences of non-compliance**

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

## **ARTICLE 16 — INTELLECTUAL PROPERTY RIGHTS (IPR) — BACKGROUND AND RESULTS — ACCESS RIGHTS AND RIGHTS OF USE**

### **16.1 Background and access rights to background**

The beneficiaries must give each other and the other participants access to the background identified as needed for implementing the action, subject to any specific rules in Annex 5.

‘Background’ means any data, know-how or information — whatever its form or nature (tangible or intangible), including any rights such as intellectual property rights — that is:

- (a) held by the beneficiaries before they acceded to the Agreement and
- (b) needed to implement the action or exploit the results.

If background is subject to rights of a third party, the beneficiary concerned must ensure that it is able to comply with its obligations under the Agreement.

### **16.2 Ownership of results**

The granting authority does not obtain ownership of the results produced under the action.

‘Results’ means any tangible or intangible effect of the action, such as data, know-how or information, whatever its form or nature, whether or not it can be protected, as well as any rights attached to it, including intellectual property rights.

### **16.3 Rights of use of the granting authority on materials, documents and information received for policy, information, communication, dissemination and publicity purposes**

The granting authority has the right to use non-sensitive information relating to the action and materials and documents received from the beneficiaries (notably summaries for publication, deliverables, as well as any other material, such as pictures or audio-visual material, in paper or electronic form) for policy, information, communication, dissemination and publicity purposes — during the action or afterwards.

The right to use the beneficiaries’ materials, documents and information is granted in the form of a royalty-free, non-exclusive and irrevocable licence, which includes the following rights:

- (a) **use for its own purposes** (in particular, making them available to persons working for the granting authority or any other EU service (including institutions, bodies, offices, agencies, etc.) or EU Member State institution or body; copying or reproducing them in whole or in part, in unlimited numbers; and communication through press information services)
- (b) **distribution to the public** (in particular, publication as hard copies and in electronic or digital format, publication on the internet, as a downloadable or non-downloadable file, broadcasting by any channel, public display or presentation, communicating through press information services, or inclusion in widely accessible databases or indexes)
- (c) **editing or redrafting** (including shortening, summarising, inserting other elements (e.g. meta-data, legends, other graphic, visual, audio or text elements), extracting parts (e.g. audio or video files), dividing into parts, use in a compilation)
- (d) **translation**
- (e) **storage** in paper, electronic or other form
- (f) **archiving**, in line with applicable document-management rules
- (g) the right to authorise **third parties** to act on its behalf or sub-license to third parties the modes of use set out in Points (b), (c), (d) and (f), if needed for the information, communication and publicity activity of the granting authority
- (h) **processing**, analysing, aggregating the materials, documents and information received and **producing derivative works**.

The rights of use are granted for the whole duration of the industrial or intellectual property rights concerned.

If materials or documents are subject to moral rights or third party rights (including intellectual property rights or rights of natural persons on their image and voice), the beneficiaries must ensure that they comply with their obligations under this Agreement (in particular, by obtaining the necessary licences and authorisations from the rights holders concerned).

Where applicable, the granting authority will insert the following information:

“© – [year] – [name of the copyright owner]. All rights reserved. Licensed to the [name of granting authority] under conditions.”

## 16.4 Specific rules on IPR, results and background

Specific rules regarding intellectual property rights, results and background (if any) are set out in Annex 5.

## 16.5 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such a breach may also lead to other measures described in Chapter 5.

## ARTICLE 17 — COMMUNICATION, DISSEMINATION AND VISIBILITY

### 17.1 Communication — Dissemination — Promoting the action

Unless otherwise agreed with the granting authority, the beneficiaries must promote the action and its results by providing targeted information to multiple audiences (including the media and the public), in accordance with Annex 1 and in a strategic, coherent and effective manner.

Before engaging in a communication or dissemination activity expected to have a major media impact, the beneficiaries must inform the granting authority.

### 17.2 Visibility — European flag and funding statement

Unless otherwise agreed with the granting authority, communication activities of the beneficiaries related to the action (including media relations, conferences, seminars, information material, such as brochures, leaflets, posters, presentations, etc., in electronic form, via traditional or social media, etc.), dissemination activities and any infrastructure, equipment, vehicles, supplies or major result funded by the grant must acknowledge EU support and display the European flag (emblem) and funding statement (translated into local languages, where appropriate):



Funded by the  
European Union



Co-funded by the  
European Union



Funded by the  
European Union



Co-funded by the  
European Union

The emblem must remain distinct and separate and cannot be modified by adding other visual marks, brands or text.

Apart from the emblem, no other visual identity or logo may be used to highlight the EU support.

When displayed in association with other logos (e.g. of beneficiaries or sponsors), the emblem must be displayed at least as prominently and visibly as the other logos.

For the purposes of their obligations under this Article, the beneficiaries may use the emblem without first obtaining approval from the granting authority. This does not, however, give them the right to

exclusive use. Moreover, they may not appropriate the emblem or any similar trademark or logo, either by registration or by any other means.

### **17.3 Quality of information — Disclaimer**

Any communication or dissemination activity related to the action must use factually accurate information.

Moreover, it must indicate the following disclaimer (translated into local languages where appropriate):

“Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or [name of the granting authority]. Neither the European Union nor the granting authority can be held responsible for them.”

### **17.4 Specific communication, dissemination and visibility rules**

Specific communication, dissemination and visibility rules (if any) are set out in Annex 5.

### **17.5 Consequences of non-compliance**

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

## **ARTICLE 18 — SPECIFIC RULES FOR CARRYING OUT THE ACTION**

### **18.1 Specific rules for carrying out the action**

Specific rules for implementing the action (if any) are set out in Annex 5.

### **18.2 Consequences of non-compliance**

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such a breach may also lead to other measures described in Chapter 5.

## **SECTION 3 GRANT ADMINISTRATION**

## **ARTICLE 19 — GENERAL INFORMATION OBLIGATIONS**

### **19.1 Information requests**

The beneficiaries must provide — during the action or afterwards and in accordance with Article 7 — any information requested in order to verify eligibility of the costs or contributions declared, proper implementation of the action and compliance with the other obligations under the Agreement.

The information provided must be accurate, precise and complete and in the format requested, including electronic format.

## 19.2 Participant Register data updates

The beneficiaries must keep — at all times, during the action or afterwards — their information stored in the Portal Participant Register up to date, in particular, their name, address, legal representatives, legal form and organisation type.

## 19.3 Information about events and circumstances which impact the action

The beneficiaries must immediately inform the granting authority (and the other beneficiaries) of any of the following:

- (a) **events** which are likely to affect or delay the implementation of the action or affect the EU's financial interests, in particular:
  - (i) changes in their legal, financial, technical, organisational or ownership situation (including changes linked to one of the exclusion grounds listed in the declaration of honour signed before grant signature)
  - (ii) linked action information: not applicable
- (b) **circumstances** affecting:
  - (i) the decision to award the grant or
  - (ii) compliance with requirements under the Agreement.

## 19.4 Consequences of non-compliance

If a beneficiary breaches any of its obligations under this Article, the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

## ARTICLE 20 — RECORD-KEEPING

### 20.1 Keeping records and supporting documents

The beneficiaries must — at least until the time-limit set out in the Data Sheet (see Point 6) — keep records and other supporting documents to prove the proper implementation of the action in line with the accepted standards in the respective field (if any).

In addition, the beneficiaries must — for the same period — keep the following to justify the amounts declared:

- (a) for actual costs: adequate records and supporting documents to prove the costs declared (such as contracts, subcontracts, invoices and accounting records); in addition, the beneficiaries' usual accounting and internal control procedures must enable direct reconciliation between the amounts declared, the amounts recorded in their accounts and the amounts stated in the supporting documents
- (b) for flat-rate costs and contributions (if any): adequate records and supporting documents to prove the eligibility of the costs or contributions to which the flat-rate is applied

- (c) for the following simplified costs and contributions: the beneficiaries do not need to keep specific records on the actual costs incurred, but must keep:
  - (i) for unit costs and contributions (if any): adequate records and supporting documents to prove the number of units declared
  - (ii) for lump sum costs and contributions (if any): adequate records and supporting documents to prove proper implementation of the work as described in Annex 1
  - (iii) for financing not linked to costs (if any): adequate records and supporting documents to prove the achievement of the results or the fulfilment of the conditions as described in Annex 1
- (d) for unit, flat-rate and lump sum costs and contributions according to usual cost accounting practices (if any): the beneficiaries must keep any adequate records and supporting documents to prove that their cost accounting practices have been applied in a consistent manner, based on objective criteria, regardless of the source of funding, and that they comply with the eligibility conditions set out in Articles 6.1 and 6.2.

Moreover, the following is needed for specific budget categories:

- (e) for personnel costs: time worked for the beneficiary under the action must be supported by declarations signed monthly by the person and their supervisor, unless another reliable time-record system is in place; the granting authority may accept alternative evidence supporting the time worked for the action declared, if it considers that it offers an adequate level of assurance
- (f) additional record-keeping rules: not applicable

The records and supporting documents must be made available upon request (see Article 19) or in the context of checks, reviews, audits or investigations (see Article 25).

If there are on-going checks, reviews, audits, investigations, litigation or other pursuits of claims under the Agreement (including the extension of findings; see Article 25), the beneficiaries must keep these records and other supporting documentation until the end of these procedures.

The beneficiaries must keep the original documents. Digital and digitalised documents are considered originals if they are authorised by the applicable national law. The granting authority may accept non-original documents if they offer a comparable level of assurance.

## **20.2 Consequences of non-compliance**

If a beneficiary breaches any of its obligations under this Article, costs or contributions insufficiently substantiated will be ineligible (see Article 6) and will be rejected (see Article 27), and the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

## **ARTICLE 21 — REPORTING**

### **21.1 Continuous reporting**

The beneficiaries must continuously report on the progress of the action (e.g. **deliverables, milestones, outputs/outcomes, critical risks, indicators**, etc; if any), in the Portal Continuous Reporting tool and in accordance with the timing and conditions it sets out (as agreed with the granting authority).

Standardised deliverables (e.g. progress reports not linked to payments, reports on cumulative expenditure, special reports, etc; if any) must be submitted using the templates published on the Portal.

## 21.2 Periodic reporting: Technical reports and financial statements

In addition, the beneficiaries must provide reports to request payments, in accordance with the schedule and modalities set out in the Data Sheet (see Point 4.2):

- for additional prefinancings (if any): an **additional prefinancing report**
- for interim payments (if any) and the final payment: a **periodic report**.

The prefinancing and periodic reports include a technical and financial part.

The technical part includes an overview of the action implementation. It must be prepared using the template available in the Portal Periodic Reporting tool.

The financial part of the additional prefinancing report includes a statement on the use of the previous prefinancing payment.

The financial part of the periodic report includes:

- the financial statements (individual and consolidated; for all beneficiaries/affiliated entities)
- the explanation on the use of resources (or detailed cost reporting table, if required)
- the certificates on the financial statements (CFS) (if required; see Article 24.2 and Data Sheet, Point 4.3).

The **financial statements** must detail the eligible costs and contributions for each budget category and, for the final payment, also the revenues for the action (see Articles 6 and 22).

All eligible costs and contributions incurred should be declared, even if they exceed the amounts indicated in the estimated budget (see Annex 2). Amounts that are not declared in the individual financial statements will not be taken into account by the granting authority.

By signing the financial statements (directly in the Portal Periodic Reporting tool), the beneficiaries confirm that:

- the information provided is complete, reliable and true
- the costs and contributions declared are eligible (see Article 6)
- the costs and contributions can be substantiated by adequate records and supporting documents (see Article 20) that will be produced upon request (see Article 19) or in the context of checks, reviews, audits and investigations (see Article 25)
- for the final periodic report: all the revenues have been declared (if required; see Article 22).



Beneficiaries will have to submit also the financial statements of their affiliated entities (if any). In case of recoveries (see Article 22), beneficiaries will be held responsible also for the financial statements of their affiliated entities.

### **21.3 Currency for financial statements and conversion into euros**

The financial statements must be drafted in euro.

Beneficiaries with general accounts established in a currency other than the euro must convert the costs recorded in their accounts into euro, at the average of the daily exchange rates published in the C series of the *Official Journal of the European Union* (ECB website), calculated over the corresponding reporting period.

If no daily euro exchange rate is published in the *Official Journal* for the currency in question, they must be converted at the average of the monthly accounting exchange rates published on the European Commission website (InforEuro), calculated over the corresponding reporting period.

Beneficiaries with general accounts in euro must convert costs incurred in another currency into euro according to their usual accounting practices.

### **21.4 Reporting language**

The reporting must be in the language of the Agreement, unless otherwise agreed with the granting authority (see Data Sheet, Point 4.2).

### **21.5 Consequences of non-compliance**

If a report submitted does not comply with this Article, the granting authority may suspend the payment deadline (see Article 29) and apply other measures described in Chapter 5.

If the coordinator breaches its reporting obligations, the granting authority may terminate the grant or the coordinator's participation (see Article 32) or apply other measures described in Chapter 5.

## **ARTICLE 22 — PAYMENTS AND RECOVERIES — CALCULATION OF AMOUNTS DUE**

### **22.1 Payments and payment arrangements**

Payments will be made in accordance with the schedule and modalities set out in the Data Sheet (see Point 4.2).

They will be made in euro to the bank account indicated by the coordinator (see Data Sheet, Point 4.2) and must be distributed without unjustified delay (restrictions may apply to distribution of the initial prefinancing payment; see Data Sheet, Point 4.2).

Payments to this bank account will discharge the granting authority from its payment obligation.

The cost of payment transfers will be borne as follows:

- the granting authority bears the cost of transfers charged by its bank
- the beneficiary bears the cost of transfers charged by its bank



- the party causing a repetition of a transfer bears all costs of the repeated transfer.

Payments by the granting authority will be considered to have been carried out on the date when they are debited to its account.

## 22.2 Recoveries

Recoveries will be made, if — at beneficiary termination, final payment or afterwards — it turns out that the granting authority has paid too much and needs to recover the amounts undue.

The general liability regime for recoveries (first-line liability) is as follows: At final payment, the coordinator will be fully liable for recoveries, even if it has not been the final recipient of the undue amounts. At beneficiary termination or after final payment, recoveries will be made directly against the beneficiaries concerned.

Beneficiaries will be fully liable for repaying the debts of their affiliated entities.

In case of enforced recoveries (see Article 22.4):

- the beneficiaries will be jointly and severally liable for repaying debts of another beneficiary under the Agreement (including late-payment interest), if required by the granting authority (see Data Sheet, Point 4.4)
- affiliated entities will be held liable for repaying debts of their beneficiaries under the Agreement (including late-payment interest), if required by the granting authority (see Data Sheet, Point 4.4).

## 22.3 Amounts due

### 22.3.1 Prefinancing payments

The aim of the prefinancing is to provide the beneficiaries with a float.

It remains the property of the EU until the final payment.

For **initial prefinancings** (if any), the amount due, schedule and modalities are set out in the Data Sheet (see Point 4.2).

For **additional prefinancings** (if any), the amount due, schedule and modalities are also set out in the Data Sheet (see Point 4.2). However, if the statement on the use of the previous prefinancing payment shows that less than 70% was used, the amount set out in the Data Sheet will be reduced by the difference between the 70% threshold and the amount used.

Prefinancing payments (or parts of them) may be offset (without the beneficiaries' consent) against amounts owed by a beneficiary to the granting authority — up to the amount due to that beneficiary.

For grants where the granting authority is the European Commission or an EU executive agency, offsetting may also be done against amounts owed to other Commission services or executive agencies.

Payments will not be made if the payment deadline or payments are suspended (see Articles 29 and 30).

### 22.3.2 Amount due at beneficiary termination — Recovery

In case of beneficiary termination, the granting authority will determine the provisional amount due for the beneficiary concerned. Payments (if any) will be made with the next interim or final payment.

The **amount due** will be calculated in the following step:

Step 1 — Calculation of the total accepted EU contribution

#### Step 1 — Calculation of the total accepted EU contribution

The granting authority will first calculate the ‘accepted EU contribution’ for the beneficiary for all reporting periods, by calculating the ‘maximum EU contribution to costs’ (applying the funding rate to the accepted costs of the beneficiary), taking into account requests for a lower contribution to costs and CFS threshold cappings (if any; see Article 24.5) and adding the contributions (accepted unit, flat-rate or lump sum contributions and financing not linked to costs, if any).

After that, the granting authority will take into account grant reductions (if any). The resulting amount is the ‘total accepted EU contribution’ for the beneficiary.

The **balance** is then calculated by deducting the payments received (if any; see report on the distribution of payments in Article 32), from the total accepted EU contribution:

$$\begin{aligned} & \{ \text{total accepted EU contribution for the beneficiary} \\ & \text{minus} \\ & \{ \text{prefinancing and interim payments received (if any)} \} \}. \end{aligned}$$

If the balance is **positive**, the amount will be included in the next interim or final payment to the consortium.

If the balance is **negative**, it will be **recovered** in accordance with the following procedure:

The granting authority will send a **pre-information letter** to the beneficiary concerned:

- formally notifying the intention to recover, the amount due, the amount to be recovered and the reasons why and
- requesting observations within 30 days of receiving notification.

If no observations are submitted (or the granting authority decides to pursue recovery despite the observations it has received), it will confirm the amount to be recovered and ask this amount to be paid to the coordinator (**confirmation letter**).

The amounts will later on also be taken into account for the next interim or final payment.

### 22.3.3 Interim payments

Interim payments reimburse the eligible costs and contributions claimed for the implementation of the action during the reporting periods (if any).

Interim payments (if any) will be made in accordance with the schedule and modalities set out the Data Sheet (see Point 4.2).

Payment is subject to the approval of the periodic report. Its approval does not imply recognition of compliance, authenticity, completeness or correctness of its content.

The **interim payment** will be calculated by the granting authority in the following steps:

Step 1 — Calculation of the total accepted EU contribution

Step 2 — Limit to the interim payment ceiling

#### Step 1 — Calculation of the total accepted EU contribution

The granting authority will calculate the ‘accepted EU contribution’ for the action for the reporting period, by first calculating the ‘maximum EU contribution to costs’ (applying the funding rate to the accepted costs of each beneficiary), taking into account requests for a lower contribution to costs, and CFS threshold cappings (if any; see Article 24.5) and adding the contributions (accepted unit, flat-rate or lump sum contributions and financing not linked to costs, if any).

After that, the granting authority will take into account grant reductions from beneficiary termination (if any). The resulting amount is the ‘total accepted EU contribution’.

#### Step 2 — Limit to the interim payment ceiling

The resulting amount is then capped to ensure that the total amount of prefinancing and interim payments (if any) does not exceed the interim payment ceiling set out in the Data Sheet (see Point 4.2).

Interim payments (or parts of them) may be offset (without the beneficiaries’ consent) against amounts owed by a beneficiary to the granting authority — up to the amount due to that beneficiary.

For grants where the granting authority is the European Commission or an EU executive agency, offsetting may also be done against amounts owed to other Commission services or executive agencies.

Payments will not be made if the payment deadline or payments are suspended (see Articles 29 and 30).

### **22.3.4 Final payment — Final grant amount — Revenues and Profit — Recovery**

The final payment (payment of the balance) reimburses the remaining part of the eligible costs and contributions claimed for the implementation of the action (if any).

The final payment will be made in accordance with the schedule and modalities set out in the Data Sheet (see Point 4.2).

Payment is subject to the approval of the final periodic report. Its approval does not imply recognition of compliance, authenticity, completeness or correctness of its content.

The **final grant amount for the action** will be calculated in the following steps:

Step 1 — Calculation of the total accepted EU contribution

Step 2 — Limit to the maximum grant amount

Step 3 — Reduction due to the no-profit rule

### Step 1 — Calculation of the total accepted EU contribution

The granting authority will first calculate the ‘accepted EU contribution’ for the action for all reporting periods, by calculating the ‘maximum EU contribution to costs’ (applying the funding rate to the total accepted costs of each beneficiary), taking into account requests for a lower contribution to costs, CFS threshold cappings (if any; see Article 24.5) and adding the contributions (accepted unit, flat-rate or lump sum contributions and financing not linked to costs, if any).

After that, the granting authority will take into account grant reductions (if any). The resulting amount is the ‘total accepted EU contribution’.

### Step 2 — Limit to the maximum grant amount

If the resulting amount is higher than the maximum grant amount set out in Article 5.2, it will be limited to the latter.

### Step 3 — Reduction due to the no-profit rule

If the no-profit rule is provided for in the Data Sheet (see Point 4.2), the grant must not produce a profit (i.e. surplus of the amount obtained following Step 2 plus the action’s revenues, over the eligible costs and contributions approved by the granting authority).

‘Revenue’ is all income generated by the action, during its duration (see Article 4), for beneficiaries that are profit legal entities.

If there is a profit, it will be deducted in proportion to the final rate of reimbursement of the eligible costs approved by the granting authority (as compared to the amount calculated following Steps 1 and 2 minus the contributions).

The **balance** (final payment) is then calculated by deducting the total amount of prefinancing and interim payments already made (if any), from the final grant amount:

$$\begin{aligned} &\{\text{final grant amount} \\ &\text{minus} \\ &\{\text{prefinancing and interim payments made (if any)}\}\}. \end{aligned}$$

If the balance is **positive**, it will be **paid** to the coordinator.

The final payment (or part of it) may be offset (without the beneficiaries’ consent) against amounts owed by a beneficiary to the granting authority — up to the amount due to that beneficiary.

For grants where the granting authority is the European Commission or an EU executive agency, offsetting may also be done against amounts owed to other Commission services or executive agencies.

Payments will not be made if the payment deadline or payments are suspended (see Articles 29 and 30).

If the balance is **negative**, it will be **recovered** in accordance with the following procedure:

The granting authority will send a **pre-information letter** to the coordinator:

- formally notifying the intention to recover, the final grant amount, the amount to be recovered and the reasons why
- requesting observations within 30 days of receiving notification.

If no observations are submitted (or the granting authority decides to pursue recovery despite the observations it has received), it will confirm the amount to be recovered (**confirmation letter**), together with a **debit note** with the terms and date for payment.

If payment is not made by the date specified in the debit note, the granting authority will **enforce recovery** in accordance with Article 22.4.

### 22.3.5 Audit implementation after final payment — Revised final grant amount — Recovery

If — after the final payment (in particular, after checks, reviews, audits or investigations; see Article 25) — the granting authority rejects costs or contributions (see Article 27) or reduces the grant (see Article 28), it will calculate the **revised final grant amount** for the beneficiary concerned.

The **beneficiary revised final grant amount** will be calculated in the following step:

Step 1 — Calculation of the revised total accepted EU contribution

#### Step 1 — Calculation of the revised total accepted EU contribution

The granting authority will first calculate the ‘revised accepted EU contribution’ for the beneficiary, by calculating the ‘revised accepted costs’ and ‘revised accepted contributions’.

After that, it will take into account grant reductions (if any). The resulting ‘revised total accepted EU contribution’ is the beneficiary revised final grant amount.

If the revised final grant amount is lower than the beneficiary’s final grant amount (i.e. its share in the final grant amount for the action), it will be **recovered** in accordance with the following procedure:

The **beneficiary final grant amount** (i.e. share in the final grant amount for the action) is calculated as follows:

$$\left\{ \begin{array}{l} \text{total accepted EU contribution for the beneficiary} \\ \text{divided by} \\ \text{total accepted EU contribution for the action} \end{array} \right\} \times \left\{ \begin{array}{l} \text{multiplied by} \\ \text{final grant amount for the action} \end{array} \right\}.$$

The granting authority will send a **pre-information letter** to the beneficiary concerned:

- formally notifying the intention to recover, the amount to be recovered and the reasons why and
- requesting observations within 30 days of receiving notification.

If no observations are submitted (or the granting authority decides to pursue recovery despite the observations it has received), it will confirm the amount to be recovered (**confirmation letter**), together with a **debit note** with the terms and the date for payment.

Recoveries against affiliated entities (if any) will be handled through their beneficiaries.

If payment is not made by the date specified in the debit note, the granting authority will **enforce recovery** in accordance with Article 22.4.

## 22.4 Enforced recovery

If payment is not made by the date specified in the debit note, the amount due will be recovered:

- (a) by offsetting the amount — without the coordinator or beneficiary's consent — against any amounts owed to the coordinator or beneficiary by the granting authority.

In exceptional circumstances, to safeguard the EU financial interests, the amount may be offset before the payment date specified in the debit note.

For grants where the granting authority is the European Commission or an EU executive agency, debts may also be offset against amounts owed by other Commission services or executive agencies.

- (b) by drawing on the financial guarantee(s) (if any)
- (c) by holding other beneficiaries jointly and severally liable (if any; see Data Sheet, Point 4.4)
- (d) by holding affiliated entities jointly and severally liable (if any, see Data Sheet, Point 4.4)
- (e) by taking legal action (see Article 43) or, provided that the granting authority is the European Commission or an EU executive agency, by adopting an enforceable decision under Article 299 of the Treaty on the Functioning of the EU (TFEU) and Article 100(2) of EU Financial Regulation 2018/1046.

The amount to be recovered will be increased by **late-payment interest** at the rate set out in Article 22.5, from the day following the payment date in the debit note, up to and including the date the full payment is received.

Partial payments will be first credited against expenses, charges and late-payment interest and then against the principal.

Bank charges incurred in the recovery process will be borne by the beneficiary, unless Directive 2015/2366<sup>17</sup> applies.

For grants where the granting authority is an EU executive agency, enforced recovery by offsetting or enforceable decision will be done by the services of the European Commission (see also Article 43).

## 22.5 Consequences of non-compliance

**22.5.1** If the granting authority does not pay within the payment deadlines (see above), the beneficiaries are entitled to **late-payment interest** at the rate applied by the European Central Bank (ECB) for its main refinancing operations in euros ('reference rate'), plus the rate specified in the

---

<sup>17</sup> Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

Data Sheet (Point 4.2). The reference rate is the rate in force on the first day of the month in which the payment deadline expires, as published in the C series of the *Official Journal of the European Union*.

If the late-payment interest is lower than or equal to EUR 200, it will be paid to the coordinator only on request submitted within two months of receiving the late payment.

Late-payment interest is not due if all beneficiaries are EU Member States (including regional and local government authorities or other public bodies acting on behalf of a Member State for the purpose of this Agreement).

If payments or the payment deadline are suspended (see Articles 29 and 30), payment will not be considered as late.

Late-payment interest covers the period running from the day following the due date for payment (see above), up to and including the date of payment.

Late-payment interest is not considered for the purposes of calculating the final grant amount.

**22.5.2** If the coordinator breaches any of its obligations under this Article, the grant may be reduced (see Article 28) and the grant or the coordinator may be terminated (see Article 32).

Such breaches may also lead to other measures described in Chapter 5.

## ARTICLE 23 — GUARANTEES

### 23.1 Prefinancing guarantee

If required by the granting authority (see Data Sheet, Point 4.2), the beneficiaries must provide (one or more) prefinancing guarantee(s) in accordance with the timing and the amounts set out in the Data Sheet.

The coordinator must submit them to the granting authority in due time before the prefinancing they are linked to.

The guarantees must be drawn up using the template published on the Portal and fulfil the following conditions:

- (a) be provided by a bank or approved financial institution established in the EU or — if requested by the coordinator and accepted by the granting authority — by a third party or a bank or financial institution established outside the EU offering equivalent security
- (b) the guarantor stands as first-call guarantor and does not require the granting authority to first have recourse against the principal debtor (i.e. the beneficiary concerned) and
- (c) remain explicitly in force until the final payment and, if the final payment takes the form of a recovery, until five months after the debit note is notified to a beneficiary.

They will be released within the following month.

### 23.2 Consequences of non-compliance



If the beneficiaries breach their obligation to provide the prefinancing guarantee, the prefinancing will not be paid.

Such breaches may also lead to other measures described in Chapter 5.

## ARTICLE 24 — CERTIFICATES

### 24.1 Operational verification report (OVR)

Not applicable

### 24.2 Certificate on the financial statements (CFS)

If required by the granting authority (see Data Sheet, Point 4.3), the beneficiaries must provide certificates on their financial statements (CFS), in accordance with the schedule, threshold and conditions set out in the Data Sheet.

The coordinator must submit them as part of the periodic report (see Article 21).

The certificates must be drawn up using the template published on the Portal, cover the costs declared on the basis of actual costs and costs according to usual cost accounting practices (if any), and fulfil the following conditions:

- (a) be provided by a qualified approved external auditor which is independent and complies with Directive 2006/43/EC<sup>18</sup> (or for public bodies: by a competent independent public officer)
- (b) the verification must be carried out according to the highest professional standards to ensure that the financial statements comply with the provisions under the Agreement and that the costs declared are eligible.

The certificates will not affect the granting authority's right to carry out its own checks, reviews or audits, nor preclude the European Court of Auditors (ECA), the European Public Prosecutor's Office (EPPO) or the European Anti-Fraud Office (OLAF) from using their prerogatives for audits and investigations under the Agreement (see Article 25).

If the costs (or a part of them) were already audited by the granting authority, these costs do not need to be covered by the certificate and will not be counted for calculating the threshold (if any).

### 24.3 Certificate on the compliance of usual cost accounting practices (CoMUC)

Beneficiaries which use unit, flat rate or lump sum costs or contributions according to usual costs accounting practices (if any) may submit to the granting authority, for approval, a certificate on the methodology stating that their usual cost accounting practices comply with the eligibility conditions under the Agreement.

The certificate must be drawn up using the template published on the Portal and fulfil the following conditions:

---

<sup>18</sup> Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts or similar national regulations (OJ L 157, 9.6.2006, p. 87).



- (a) be provided by a qualified approved external auditor which is independent and complies with Directive 2006/43/EC<sup>19</sup> (or for public bodies: by a competent independent public officer)
- (b) the verification must be carried out according to the highest professional standards to ensure that the methodology for declaring costs according to usual accounting practices complies with the provisions under the Agreement.

If the certificate is approved, amounts declared in line with this methodology will not be challenged subsequently, unless the beneficiary concealed information for the purpose of the approval.

#### **24.4 Systems and process audit (SPA)**

Not applicable

#### **24.5 Consequences of non-compliance**

If a beneficiary does not submit a certificate on the financial statements (CFS) or the certificate is rejected, the accepted EU contribution to costs will be capped to reflect the CFS threshold.

If a beneficiary breaches any of its other obligations under this Article, the granting authority may apply the measures described in Chapter 5.

### **ARTICLE 25 — CHECKS, REVIEWS, AUDITS AND INVESTIGATIONS — EXTENSION OF FINDINGS**

#### **25.1 Granting authority checks, reviews and audits**

##### **25.1.1 Internal checks**

The granting authority may — during the action or afterwards — check the proper implementation of the action and compliance with the obligations under the Agreement, including assessing costs and contributions, deliverables and reports.

##### **25.1.2 Project reviews**

The granting authority may carry out reviews on the proper implementation of the action and compliance with the obligations under the Agreement (general project reviews or specific issues reviews).

Such project reviews may be started during the implementation of the action and until the time-limit set out in the Data Sheet (see Point 6). They will be formally notified to the coordinator or beneficiary concerned and will be considered to start on the date of the notification.

If needed, the granting authority may be assisted by independent, outside experts. If it uses outside experts, the coordinator or beneficiary concerned will be informed and have the right to object on grounds of commercial confidentiality or conflict of interest.

The coordinator or beneficiary concerned must cooperate diligently and provide — within the deadline requested — any information and data in addition to deliverables and reports already submitted

---

<sup>19</sup> Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts or similar national regulations (OJ L 157, 9.6.2006, p. 87).

(including information on the use of resources). The granting authority may request beneficiaries to provide such information to it directly. Sensitive information and documents will be treated in accordance with Article 13.

The coordinator or beneficiary concerned may be requested to participate in meetings, including with the outside experts.

For **on-the-spot visits**, the beneficiary concerned must allow access to sites and premises (including to the outside experts) and must ensure that information requested is readily available.

Information provided must be accurate, precise and complete and in the format requested, including electronic format.

On the basis of the review findings, a **project review report** will be drawn up.

The granting authority will formally notify the project review report to the coordinator or beneficiary concerned, which has 30 days from receiving notification to make observations.

Project reviews (including project review reports) will be in the language of the Agreement, unless otherwise agreed with the granting authority (see Data Sheet, Point 4.2).

### 25.1.3 Audits

The granting authority may carry out audits on the proper implementation of the action and compliance with the obligations under the Agreement.

Such audits may be started during the implementation of the action and until the time-limit set out in the Data Sheet (see Point 6). They will be formally notified to the beneficiary concerned and will be considered to start on the date of the notification.

The granting authority may use its own audit service, delegate audits to a centralised service or use external audit firms. If it uses an external firm, the beneficiary concerned will be informed and have the right to object on grounds of commercial confidentiality or conflict of interest.

The beneficiary concerned must cooperate diligently and provide — within the deadline requested — any information (including complete accounts, individual salary statements or other personal data) to verify compliance with the Agreement. Sensitive information and documents will be treated in accordance with Article 13.

For **on-the-spot visits**, the beneficiary concerned must allow access to sites and premises (including for the external audit firm) and must ensure that information requested is readily available.

Information provided must be accurate, precise and complete and in the format requested, including electronic format.

On the basis of the audit findings, a **draft audit report** will be drawn up.

The auditors will formally notify the draft audit report to the beneficiary concerned, which has 30 days from receiving notification to make observations (contradictory audit procedure).

The **final audit report** will take into account observations by the beneficiary concerned and will be formally notified to them.

Audits (including audit reports) will be in the language of the Agreement, unless otherwise agreed with the granting authority (see Data Sheet, Point 4.2).

## **25.2 European Commission checks, reviews and audits in grants of other granting authorities**

Where the granting authority is not the European Commission, the latter has the same rights of checks, reviews and audits as the granting authority.

## **25.3 Access to records for assessing simplified forms of funding**

The beneficiaries must give the European Commission access to their statutory records for the periodic assessment of simplified forms of funding which are used in EU programmes.

## **25.4 OLAF, EPPO and ECA audits and investigations**

The following bodies may also carry out checks, reviews, audits and investigations — during the action or afterwards:

- the European Anti-Fraud Office (OLAF) under Regulations No 883/2013<sup>20</sup> and No 2185/96<sup>21</sup>
- the European Public Prosecutor's Office (EPPO) under Regulation 2017/1939
- the European Court of Auditors (ECA) under Article 287 of the Treaty on the Functioning of the EU (TFEU) and Article 257 of EU Financial Regulation 2018/1046.

If requested by these bodies, the beneficiary concerned must provide full, accurate and complete information in the format requested (including complete accounts, individual salary statements or other personal data, including in electronic format) and allow access to sites and premises for on-the-spot visits or inspections — as provided for under these Regulations.

To this end, the beneficiary concerned must keep all relevant information relating to the action, at least until the time-limit set out in the Data Sheet (Point 6) and, in any case, until any ongoing checks, reviews, audits, investigations, litigation or other pursuits of claims have been concluded.

## **25.5 Consequences of checks, reviews, audits and investigations — Extension of results of reviews, audits or investigations**

### **25.5.1 Consequences of checks, reviews, audits and investigations in this grant**

Findings in checks, reviews, audits or investigations carried out in the context of this grant may lead to rejections (see Article 27), grant reduction (see Article 28) or other measures described in Chapter 5.

Rejections or grant reductions after the final payment will lead to a revised final grant amount (see Article 22).

<sup>20</sup> Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18/09/2013, p. 1).

<sup>21</sup> Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities (OJ L 292, 15/11/1996, p. 2).

Findings in checks, reviews, audits or investigations during the action implementation may lead to a request for amendment (see Article 39), to change the description of the action set out in Annex 1.

Checks, reviews, audits or investigations that find systemic or recurrent errors, irregularities, fraud or breach of obligations in any EU grant may also lead to consequences in other EU grants awarded under similar conditions ('extension to other grants').

Moreover, findings arising from an OLAF or EPPO investigation may lead to criminal prosecution under national law.

### 25.5.2 Extension from other grants

Results of checks, reviews, audits or investigations in other grants may be extended to this grant, if:

- (a) the beneficiary concerned is found, in other EU grants awarded under similar conditions, to have committed systemic or recurrent errors, irregularities, fraud or breach of obligations that have a material impact on this grant and
- (b) those findings are formally notified to the beneficiary concerned — together with the list of grants affected by the findings — within the time-limit for audits set out in the Data Sheet (see Point 6).

The granting authority will formally notify the beneficiary concerned of the intention to extend the findings and the list of grants affected.

If the extension concerns **rejections of costs or contributions**: the notification will include:

- (a) an invitation to submit observations on the list of grants affected by the findings
- (b) the request to submit revised financial statements for all grants affected
- (c) the correction rate for extrapolation, established on the basis of the systemic or recurrent errors, to calculate the amounts to be rejected, if the beneficiary concerned:
  - (i) considers that the submission of revised financial statements is not possible or practicable or
  - (ii) does not submit revised financial statements.

If the extension concerns **grant reductions**: the notification will include:

- (a) an invitation to submit observations on the list of grants affected by the findings and
- (b) the **correction rate for extrapolation**, established on the basis of the systemic or recurrent errors and the principle of proportionality.

The beneficiary concerned has **60 days** from receiving notification to submit observations, revised financial statements or to propose a duly substantiated **alternative correction method/rate**.

On the basis of this, the granting authority will analyse the impact and decide on the implementation (i.e. start rejection or grant reduction procedures, either on the basis of the revised financial statements or the announced/alternative method/rate or a mix of those; see Articles 27 and 28).

## **25.6 Consequences of non-compliance**

If a beneficiary breaches any of its obligations under this Article, costs or contributions insufficiently substantiated will be ineligible (see Article 6) and will be rejected (see Article 27), and the grant may be reduced (see Article 28).

Such breaches may also lead to other measures described in Chapter 5.

## **ARTICLE 26 — IMPACT EVALUATIONS**

### **26.1 Impact evaluation**

The granting authority may carry out impact evaluations of the action, measured against the objectives and indicators of the EU programme funding the grant.

Such evaluations may be started during implementation of the action and until the time-limit set out in the Data Sheet (see Point 6). They will be formally notified to the coordinator or beneficiaries and will be considered to start on the date of the notification.

If needed, the granting authority may be assisted by independent outside experts.

The coordinator or beneficiaries must provide any information relevant to evaluate the impact of the action, including information in electronic format.

### **26.2 Consequences of non-compliance**

If a beneficiary breaches any of its obligations under this Article, the granting authority may apply the measures described in Chapter 5.

## **CHAPTER 5 CONSEQUENCES OF NON-COMPLIANCE**

### **SECTION 1 REJECTIONS AND GRANT REDUCTION**

## **ARTICLE 27 — REJECTION OF COSTS AND CONTRIBUTIONS**

### **27.1 Conditions**

The granting authority will — at beneficiary termination, interim payment, final payment or afterwards — reject any costs or contributions which are ineligible (see Article 6), in particular following checks, reviews, audits or investigations (see Article 25).

The rejection may also be based on the extension of findings from other grants to this grant (see Article 25).

Ineligible costs or contributions will be rejected.

### **27.2 Procedure**

If the rejection does not lead to a recovery, the granting authority will formally notify the coordinator or beneficiary concerned of the rejection, the amounts and the reasons why. The coordinator or

beneficiary concerned may — within 30 days of receiving notification — submit observations if it disagrees with the rejection (payment review procedure).

If the rejection leads to a recovery, the granting authority will follow the contradictory procedure with pre-information letter set out in Article 22.

### **27.3 Effects**

If the granting authority rejects costs or contributions, it will deduct them from the costs or contributions declared and then calculate the amount due (and, if needed, make a recovery; see Article 22).

## **ARTICLE 28 — GRANT REDUCTION**

### **28.1 Conditions**

The granting authority may — at beneficiary termination, final payment or afterwards — reduce the grant for a beneficiary, if:

- (a) the beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed:
  - (i) substantial errors, irregularities or fraud or
  - (ii) serious breach of obligations under this Agreement or during its award (including improper implementation of the action, non-compliance with the call conditions, submission of false information, failure to provide required information, breach of ethics or security rules (if applicable), etc.), or
- (b) the beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed — in other EU grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant (see Article 25).

The amount of the reduction will be calculated for each beneficiary concerned and proportionate to the seriousness and the duration of the errors, irregularities or fraud or breach of obligations, by applying an individual reduction rate to their accepted EU contribution.

### **28.2 Procedure**

If the grant reduction does not lead to a recovery, the granting authority will formally notify the coordinator or beneficiary concerned of the reduction, the amount to be reduced and the reasons why. The coordinator or beneficiary concerned may — within 30 days of receiving notification — submit observations if it disagrees with the reduction (payment review procedure).

If the grant reduction leads to a recovery, the granting authority will follow the contradictory procedure with pre-information letter set out in Article 22.

### **28.3 Effects**

If the granting authority reduces the grant, it will deduct the reduction and then calculate the amount due (and, if needed, make a recovery; see Article 22).

## **SECTION 2 SUSPENSION AND TERMINATION**

### **ARTICLE 29 — PAYMENT DEADLINE SUSPENSION**

#### **29.1 Conditions**

The granting authority may — at any moment — suspend the payment deadline if a payment cannot be processed because:

- (a) the required report (see Article 21) has not been submitted or is not complete or additional information is needed
- (b) there are doubts about the amount to be paid (e.g. ongoing audit extension procedure, queries about eligibility, need for a grant reduction, etc.) and additional checks, reviews, audits or investigations are necessary, or
- (c) there are other issues affecting the EU financial interests.

#### **29.2 Procedure**

The granting authority will formally notify the coordinator of the suspension and the reasons why.

The suspension will **take effect** the day the notification is sent.

If the conditions for suspending the payment deadline are no longer met, the suspension will be **lifted** — and the remaining time to pay (see Data Sheet, Point 4.2) will resume.

If the suspension exceeds two months, the coordinator may request the granting authority to confirm if the suspension will continue.

If the payment deadline has been suspended due to the non-compliance of the report and the revised report is not submitted (or was submitted but is also rejected), the granting authority may also terminate the grant or the participation of the coordinator (see Article 32).

### **ARTICLE 30 — PAYMENT SUSPENSION**

#### **30.1 Conditions**

The granting authority may — at any moment — suspend payments, in whole or in part for one or more beneficiaries, if:

- (a) a beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed or is suspected of having committed:
  - (i) substantial errors, irregularities or fraud or
  - (ii) serious breach of obligations under this Agreement or during its award (including



improper implementation of the action, non-compliance with the call conditions, submission of false information, failure to provide required information, breach of ethics or security rules (if applicable), etc.), or

- (b) a beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed — in other EU grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant.

If payments are suspended for one or more beneficiaries, the granting authority will make partial payment(s) for the part(s) not suspended. If suspension concerns the final payment, the payment (or recovery) of the remaining amount after suspension is lifted will be considered to be the payment that closes the action.

## 30.2 Procedure

Before suspending payments, the granting authority will send a **pre-information letter** to the beneficiary concerned:

- formally notifying the intention to suspend payments and the reasons why and
- requesting observations within 30 days of receiving notification.

If the granting authority does not receive observations or decides to pursue the procedure despite the observations it has received, it will confirm the suspension (**confirmation letter**). Otherwise, it will formally notify that the procedure is discontinued.

At the end of the suspension procedure, the granting authority will also inform the coordinator.

The suspension will **take effect** the day after the confirmation notification is sent.

If the conditions for resuming payments are met, the suspension will be **lifted**. The granting authority will formally notify the beneficiary concerned (and the coordinator) and set the suspension end date.

During the suspension, no prefinancing will be paid to the beneficiaries concerned. For interim payments, the periodic reports for all reporting periods except the last one (see Article 21) must not contain any financial statements from the beneficiary concerned (or its affiliated entities). The coordinator must include them in the next periodic report after the suspension is lifted or — if suspension is not lifted before the end of the action — in the last periodic report.

## ARTICLE 31 — GRANT AGREEMENT SUSPENSION

### 31.1 Consortium-requested GA suspension

#### 31.1.1 Conditions and procedure

The beneficiaries may request the suspension of the grant or any part of it, if exceptional circumstances — in particular *force majeure* (see Article 35) — make implementation impossible or excessively difficult.

The coordinator must submit a request for **amendment** (see Article 39), with:



- the reasons why
- the date the suspension takes effect; this date may be before the date of the submission of the amendment request and
- the expected date of resumption.

The suspension will **take effect** on the day specified in the amendment.

Once circumstances allow for implementation to resume, the coordinator must immediately request another **amendment** of the Agreement to set the suspension end date, the resumption date (one day after suspension end date), extend the duration and make other changes necessary to adapt the action to the new situation (see Article 39) — unless the grant has been terminated (see Article 32). The suspension will be **lifted** with effect from the suspension end date set out in the amendment. This date may be before the date of the submission of the amendment request.

During the suspension, no prefinancing will be paid. Costs incurred or contributions for activities implemented during grant suspension are not eligible (see Article 6.3).

## 31.2 EU-initiated GA suspension

### 31.2.1 Conditions

The granting authority may suspend the grant or any part of it, if:

- (a) a beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed or is suspected of having committed:
  - (i) substantial errors, irregularities or fraud or
  - (ii) serious breach of obligations under this Agreement or during its award (including improper implementation of the action, non-compliance with the call conditions, submission of false information, failure to provide required information, breach of ethics or security rules (if applicable), etc.), or
- (b) a beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed — in other EU grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant
- (c) other:
  - (i) linked action issues: not applicable
  - (ii) additional GA suspension grounds: not applicable.

### 31.2.2 Procedure

Before suspending the grant, the granting authority will send a **pre-information letter** to the coordinator:

- formally notifying the intention to suspend the grant and the reasons why and

- requesting observations within 30 days of receiving notification.

If the granting authority does not receive observations or decides to pursue the procedure despite the observations it has received, it will confirm the suspension (**confirmation letter**). Otherwise, it will formally notify that the procedure is discontinued.

The suspension will **take effect** the day after the confirmation notification is sent (or on a later date specified in the notification).

Once the conditions for resuming implementation of the action are met, the granting authority will formally notify the coordinator a **lifting of suspension letter**, in which it will set the suspension end date and invite the coordinator to request an amendment of the Agreement to set the resumption date (one day after suspension end date), extend the duration and make other changes necessary to adapt the action to the new situation (see Article 39) — unless the grant has been terminated (see Article 32). The suspension will be **lifted** with effect from the suspension end date set out in the lifting of suspension letter. This date may be before the date on which the letter is sent.

During the suspension, no prefinancing will be paid. Costs incurred or contributions for activities implemented during suspension are not eligible (see Article 6.3).

The beneficiaries may not claim damages due to suspension by the granting authority (see Article 33).

Grant suspension does not affect the granting authority's right to terminate the grant or a beneficiary (see Article 32) or reduce the grant (see Article 28).

## ARTICLE 32 — GRANT AGREEMENT OR BENEFICIARY TERMINATION

### 32.1 Consortium-requested GA termination

#### 32.1.1 Conditions and procedure

The beneficiaries may request the termination of the grant.

The coordinator must submit a request for **amendment** (see Article 39), with:

- the reasons why
- the date the consortium ends work on the action ('end of work date') and
- the date the termination takes effect ('termination date'); this date must be after the date of the submission of the amendment request.

The termination will **take effect** on the termination date specified in the amendment.

If no reasons are given or if the granting authority considers the reasons do not justify termination, it may consider the grant terminated improperly.

#### 32.1.2 Effects

The coordinator must — within 60 days from when termination takes effect — submit a **periodic report** (for the open reporting period until termination).

The granting authority will calculate the final grant amount and final payment on the basis of the report

submitted and taking into account the costs incurred and contributions for activities implemented before the end of work date (see Article 22). Costs relating to contracts due for execution only after the end of work are not eligible.

If the granting authority does not receive the report within the deadline, only costs and contributions which are included in an approved periodic report will be taken into account (no costs/contributions if no periodic report was ever approved).

Improper termination may lead to a grant reduction (see Article 28).

After termination, the beneficiaries' obligations (in particular Articles 13 (confidentiality and security), 16 (IPR), 17 (communication, dissemination and visibility), 21 (reporting), 25 (checks, reviews, audits and investigations), 26 (impact evaluation), 27 (rejections), 28 (grant reduction) and 42 (assignment of claims)) continue to apply.

## 32.2 Consortium-requested beneficiary termination

### 32.2.1 Conditions and procedure

The coordinator may request the termination of the participation of one or more beneficiaries, on request of the beneficiary concerned or on behalf of the other beneficiaries.

The coordinator must submit a request for **amendment** (see Article 39), with:

- the reasons why
- the opinion of the beneficiary concerned (or proof that this opinion has been requested in writing)
- the date the beneficiary ends work on the action ('end of work date')
- the date the termination takes effect ('termination date'); this date must be after the date of the submission of the amendment request.

If the termination concerns the coordinator and is done without its agreement, the amendment request must be submitted by another beneficiary (acting on behalf of the consortium).

The termination will **take effect** on the termination date specified in the amendment.

If no information is given or if the granting authority considers that the reasons do not justify termination, it may consider the beneficiary to have been terminated improperly.

### 32.2.2 Effects

The coordinator must — within 60 days from when termination takes effect — submit:

- (i) a **report on the distribution of payments** to the beneficiary concerned
- (ii) a **termination report** from the beneficiary concerned, for the open reporting period until termination, containing an overview of the progress of the work, the financial statement, the explanation on the use of resources, and, if applicable, the certificate on the financial statement (CFS; see Articles 21 and 24.2 and Data Sheet, Point 4.3)

- (iii) a second **request for amendment** (see Article 39) with other amendments needed (e.g. reallocation of the tasks and the estimated budget of the terminated beneficiary; addition of a new beneficiary to replace the terminated beneficiary; change of coordinator, etc.).

The granting authority will calculate the amount due to the beneficiary on the basis of the report submitted and taking into account the costs incurred and contributions for activities implemented before the end of work date (see Article 22). Costs relating to contracts due for execution only after the end of work are not eligible.

The information in the termination report must also be included in the periodic report for the next reporting period (see Article 21).

If the granting authority does not receive the termination report within the deadline, only costs and contributions which are included in an approved periodic report will be taken into account (no costs/contributions if no periodic report was ever approved).

If the granting authority does not receive the report on the distribution of payments within the deadline, it will consider that:

- the coordinator did not distribute any payment to the beneficiary concerned and that
- the beneficiary concerned must not repay any amount to the coordinator.

If the second request for amendment is accepted by the granting authority, the Agreement is **amended** to introduce the necessary changes (see Article 39).

If the second request for amendment is rejected by the granting authority (because it calls into question the decision awarding the grant or breaches the principle of equal treatment of applicants), the grant may be terminated (see Article 32).

Improper termination may lead to a reduction of the grant (see Article 31) or grant termination (see Article 32).

After termination, the concerned beneficiary's obligations (in particular Articles 13 (confidentiality and security), 16 (IPR), 17 (communication, dissemination and visibility), 21 (reporting), 25 (checks, reviews, audits and investigations), 26 (impact evaluation), 27 (rejections), 28 (grant reduction) and 42 (assignment of claims)) continue to apply.

### 32.3 EU-initiated GA or beneficiary termination

#### 32.3.1 Conditions

The granting authority may terminate the grant or the participation of one or more beneficiaries, if:

- (a) one or more beneficiaries do not accede to the Agreement (see Article 40)
- (b) a change to the action or the legal, financial, technical, organisational or ownership situation of a beneficiary is likely to substantially affect the implementation of the action or calls into question the decision to award the grant (including changes linked to one of the exclusion grounds listed in the declaration of honour)
- (c) following termination of one or more beneficiaries, the necessary changes to the Agreement

(and their impact on the action) would call into question the decision awarding the grant or breach the principle of equal treatment of applicants

- (d) implementation of the action has become impossible or the changes necessary for its continuation would call into question the decision awarding the grant or breach the principle of equal treatment of applicants
- (e) a beneficiary (or person with unlimited liability for its debts) is subject to bankruptcy proceedings or similar (including insolvency, winding-up, administration by a liquidator or court, arrangement with creditors, suspension of business activities, etc.)
- (f) a beneficiary (or person with unlimited liability for its debts) is in breach of social security or tax obligations
- (g) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has been found guilty of grave professional misconduct
- (h) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed fraud, corruption, or is involved in a criminal organisation, money laundering, terrorism-related crimes (including terrorism financing), child labour or human trafficking
- (i) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) was 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)
- (j) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed:
  - (i) substantial errors, irregularities or fraud or
  - (ii) serious breach of obligations under this Agreement or during its award (including improper implementation of the action, non-compliance with the call conditions, submission of false information, failure to provide required information, breach of ethics or security rules (if applicable), etc.)
- (k) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed — in other EU grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant (extension of findings from other grants to this grant; see Article 25)
- (l) despite a specific request by the granting authority, a beneficiary does not request — through the coordinator — an amendment to the Agreement to end the participation of one of its affiliated entities or associated partners that is in one of the situations under points (d), (f), (e), (g), (h), (i) or (j) and to reallocate its tasks, or
- (m) other:
  - (i) linked action issues: not applicable

(ii) additional GA termination grounds: not applicable.

### 32.3.2 Procedure

Before terminating the grant or participation of one or more beneficiaries, the granting authority will send a **pre-information letter** to the coordinator or beneficiary concerned:

- formally notifying the intention to terminate and the reasons why and
- requesting observations within 30 days of receiving notification.

If the granting authority does not receive observations or decides to pursue the procedure despite the observations it has received, it will confirm the termination and the date it will take effect (**confirmation letter**). Otherwise, it will formally notify that the procedure is discontinued.

For beneficiary terminations, the granting authority will — at the end of the procedure — also inform the coordinator.

The termination will **take effect** the day after the confirmation notification is sent (or on a later date specified in the notification; ‘termination date’).

### 32.3.3 Effects

(a) for **GA termination**:

The coordinator must — within 60 days from when termination takes effect — submit a **periodic report** (for the last open reporting period until termination).

The granting authority will calculate the final grant amount and final payment on the basis of the report submitted and taking into account the costs incurred and contributions for activities implemented before termination takes effect (see Article 22). Costs relating to contracts due for execution only after termination are not eligible.

If the grant is terminated for breach of the obligation to submit reports, the coordinator may not submit any report after termination.

If the granting authority does not receive the report within the deadline, only costs and contributions which are included in an approved periodic report will be taken into account (no costs/contributions if no periodic report was ever approved).

Termination does not affect the granting authority’s right to reduce the grant (see Article 28) or to impose administrative sanctions (see Article 34).

The beneficiaries may not claim damages due to termination by the granting authority (see Article 33).

After termination, the beneficiaries’ obligations (in particular Articles 13 (confidentiality and security), 16 (IPR), 17 (communication, dissemination and visibility), 21 (reporting), 25 (checks, reviews, audits and investigations), 26 (impact evaluation), 27 (rejections), 28 (grant reduction) and 42 (assignment of claims)) continue to apply.

(b) for **beneficiary termination**:

The coordinator must — within 60 days from when termination takes effect — submit:

- (i) a **report on the distribution of payments** to the beneficiary concerned
- (ii) a **termination report** from the beneficiary concerned, for the open reporting period until termination, containing an overview of the progress of the work, the financial statement, the explanation on the use of resources, and, if applicable, the certificate on the financial statement (CFS; see Articles 21 and 24.2 and Data Sheet, Point 4.3)
- (iii) a **request for amendment** (see Article 39) with any amendments needed (e.g. reallocation of the tasks and the estimated budget of the terminated beneficiary; addition of a new beneficiary to replace the terminated beneficiary; change of coordinator, etc.).

The granting authority will calculate the amount due to the beneficiary on the basis of the report submitted and taking into account the costs incurred and contributions for activities implemented before termination takes effect (see Article 22). Costs relating to contracts due for execution only after termination are not eligible.

The information in the termination report must also be included in the periodic report for the next reporting period (see Article 21).

If the granting authority does not receive the termination report within the deadline, only costs and contributions included in an approved periodic report will be taken into account (no costs/contributions if no periodic report was ever approved).

If the granting authority does not receive the report on the distribution of payments within the deadline, it will consider that:

- the coordinator did not distribute any payment to the beneficiary concerned and that
- the beneficiary concerned must not repay any amount to the coordinator.

If the request for amendment is accepted by the granting authority, the Agreement is **amended** to introduce the necessary changes (see Article 39).

If the request for amendment is rejected by the granting authority (because it calls into question the decision awarding the grant or breaches the principle of equal treatment of applicants), the grant may be terminated (see Article 32).

After termination, the concerned beneficiary's obligations (in particular Articles 13 (confidentiality and security), 16 (IPR), 17 (communication, dissemination and visibility), 21 (reporting), 25 (checks, reviews, audits and investigations), 26 (impact evaluation), 27 (rejections), 28 (grant reduction) and 42 (assignment of claims)) continue to apply.

## **SECTION 3 OTHER CONSEQUENCES: DAMAGES AND ADMINISTRATIVE SANCTIONS**

### **ARTICLE 33 — DAMAGES**



### **33.1 Liability of the granting authority**

The granting authority cannot be held liable for any damage caused to the beneficiaries or to third parties as a consequence of the implementation of the Agreement, including for gross negligence.

The granting authority cannot be held liable for any damage caused by any of the beneficiaries or other participants involved in the action, as a consequence of the implementation of the Agreement.

### **33.2 Liability of the beneficiaries**

The beneficiaries must compensate the granting authority for any damage it sustains as a result of the implementation of the action or because the action was not implemented in full compliance with the Agreement, provided that it was caused by gross negligence or wilful act.

The liability does not extend to indirect or consequential losses or similar damage (such as loss of profit, loss of revenue or loss of contracts), provided such damage was not caused by wilful act or by a breach of confidentiality.

## **ARTICLE 34 — ADMINISTRATIVE SANCTIONS AND OTHER MEASURES**

Nothing in this Agreement may be construed as preventing the adoption of administrative sanctions (i.e. exclusion from EU award procedures and/or financial penalties) or other public law measures, in addition or as an alternative to the contractual measures provided under this Agreement (see, for instance, Articles 135 to 145 EU Financial Regulation 2018/1046 and Articles 4 and 7 of Regulation 2988/95<sup>22</sup>).

## **SECTION 4 FORCE MAJEURE**

### **ARTICLE 35 — FORCE MAJEURE**

A party prevented by force majeure from fulfilling its obligations under the Agreement cannot be considered in breach of them.

‘Force majeure’ means any situation or event that:

- prevents either party from fulfilling their obligations under the Agreement,
- was unforeseeable, exceptional situation and beyond the parties’ control,
- was not due to error or negligence on their part (or on the part of other participants involved in the action), and
- proves to be inevitable in spite of exercising all due diligence.

Any situation constituting force majeure must be formally notified to the other party without delay, stating the nature, likely duration and foreseeable effects.

---

<sup>22</sup> Council Regulation (EC, Euratom) No 2988/95 of 18 December 1995 on the protection of the European Communities financial interests (OJ L 312, 23.12.1995, p. 1).



The parties must immediately take all the necessary steps to limit any damage due to force majeure and do their best to resume implementation of the action as soon as possible.

## **CHAPTER 6 FINAL PROVISIONS**

### **ARTICLE 36 — COMMUNICATION BETWEEN THE PARTIES**

#### **36.1 Forms and means of communication — Electronic management**

EU grants are managed fully electronically through the EU Funding & Tenders Portal ('Portal').

All communications must be made electronically through the Portal, in accordance with the Portal Terms and Conditions and using the forms and templates provided there (except if explicitly instructed otherwise by the granting authority).

Communications must be made in writing and clearly identify the grant agreement (project number and acronym).

Communications must be made by persons authorised according to the Portal Terms and Conditions. For naming the authorised persons, each beneficiary must have designated — before the signature of this Agreement — a 'legal entity appointed representative (LEAR)'. The role and tasks of the LEAR are stipulated in their appointment letter (see Portal Terms and Conditions).

If the electronic exchange system is temporarily unavailable, instructions will be given on the Portal.

#### **36.2 Date of communication**

The sending date for communications made through the Portal will be the date and time of sending, as indicated by the time logs.

The receiving date for communications made through the Portal will be the date and time the communication is accessed, as indicated by the time logs. Formal notifications that have not been accessed within 10 days after sending, will be considered to have been accessed (see Portal Terms and Conditions).

If a communication is exceptionally made on paper (by e-mail or postal service), general principles apply (i.e. date of sending/receipt). Formal notifications by registered post with proof of delivery will be considered to have been received either on the delivery date registered by the postal service or the deadline for collection at the post office.

If the electronic exchange system is temporarily unavailable, the sending party cannot be considered in breach of its obligation to send a communication within a specified deadline.

#### **36.3 Addresses for communication**

The Portal can be accessed via the Europa website.

The address for paper communications to the granting authority (if exceptionally allowed) is the official mailing address indicated on its website.

For beneficiaries, it is the legal address specified in the Portal Participant Register.

## **ARTICLE 37 — INTERPRETATION OF THE AGREEMENT**

The provisions in the Data Sheet take precedence over the rest of the Terms and Conditions of the Agreement.

Annex 5 takes precedence over the Terms and Conditions; the Terms and Conditions take precedence over the Annexes other than Annex 5.

Annex 2 takes precedence over Annex 1.

## **ARTICLE 38 — CALCULATION OF PERIODS AND DEADLINES**

In accordance with Regulation No 1182/71<sup>23</sup>, periods expressed in days, months or years are calculated from the moment the triggering event occurs.

The day during which that event occurs is not considered as falling within the period.

‘Days’ means calendar days, not working days.

## **ARTICLE 39 — AMENDMENTS**

### **39.1 Conditions**

The Agreement may be amended, unless the amendment entails changes to the Agreement which would call into question the decision awarding the grant or breach the principle of equal treatment of applicants.

Amendments may be requested by any of the parties.

### **39.2 Procedure**

The party requesting an amendment must submit a request for amendment signed directly in the Portal Amendment tool.

The coordinator submits and receives requests for amendment on behalf of the beneficiaries (see Annex 3). If a change of coordinator is requested without its agreement, the submission must be done by another beneficiary (acting on behalf of the other beneficiaries).

The request for amendment must include:

- the reasons why
- the appropriate supporting documents and
- for a change of coordinator without its agreement: the opinion of the coordinator (or proof that this opinion has been requested in writing).

The granting authority may request additional information.

---

<sup>23</sup> Regulation (EEC, Euratom) No 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time-limits (OJ L 124, 8/6/1971, p. 1).

If the party receiving the request agrees, it must sign the amendment in the tool within 45 days of receiving notification (or any additional information the granting authority has requested). If it does not agree, it must formally notify its disagreement within the same deadline. The deadline may be extended, if necessary for the assessment of the request. If no notification is received within the deadline, the request is considered to have been rejected.

An amendment **enters into force** on the day of the signature of the receiving party.

An amendment **takes effect** on the date of entry into force or other date specified in the amendment.

## **ARTICLE 40 — ACCESSION AND ADDITION OF NEW BENEFICIARIES**

### **40.1 Accession of the beneficiaries mentioned in the Preamble**

The beneficiaries which are not coordinator must accede to the grant by signing the accession form (see Annex 3) directly in the Portal Grant Preparation tool, within 30 days after the entry into force of the Agreement (see Article 44).

They will assume the rights and obligations under the Agreement with effect from the date of its entry into force (see Article 44).

If a beneficiary does not accede to the grant within the above deadline, the coordinator must — within 30 days — request an amendment (see Article 39) to terminate the beneficiary and make any changes necessary to ensure proper implementation of the action. This does not affect the granting authority's right to terminate the grant (see Article 32).

### **40.2 Addition of new beneficiaries**

In justified cases, the beneficiaries may request the addition of a new beneficiary.

For this purpose, the coordinator must submit a request for amendment in accordance with Article 39. It must include an accession form (see Annex 3) signed by the new beneficiary directly in the Portal Amendment tool.

New beneficiaries will assume the rights and obligations under the Agreement with effect from the date of their accession specified in the accession form (see Annex 3).

Additions are also possible in mono-beneficiary grants.

## **ARTICLE 41 — TRANSFER OF THE AGREEMENT**

In justified cases, the beneficiary of a mono-beneficiary grant may request the transfer of the grant to a new beneficiary, provided that this would not call into question the decision awarding the grant or breach the principle of equal treatment of applicants.

The beneficiary must submit a request for **amendment** (see Article 39), with

- the reasons why
- the accession form (see Annex 3) signed by the new beneficiary directly in the Portal Amendment tool and

- additional supporting documents (if required by the granting authority).

The new beneficiary will assume the rights and obligations under the Agreement with effect from the date of accession specified in the accession form (see Annex 3).

## **ARTICLE 42 — ASSIGNMENTS OF CLAIMS FOR PAYMENT AGAINST THE GRANTING AUTHORITY**

The beneficiaries may not assign any of their claims for payment against the granting authority to any third party, except if expressly approved in writing by the granting authority on the basis of a reasoned, written request by the coordinator (on behalf of the beneficiary concerned).

If the granting authority has not accepted the assignment or if the terms of it are not observed, the assignment will have no effect on it.

In no circumstances will an assignment release the beneficiaries from their obligations towards the granting authority.

## **ARTICLE 43 — APPLICABLE LAW AND SETTLEMENT OF DISPUTES**

### **43.1 Applicable law**

The Agreement is governed by the applicable EU law, supplemented if necessary by the law of Belgium.

Special rules may apply for beneficiaries which are international organisations (if any; see Data Sheet, Point 5).

### **43.2 Dispute settlement**

If a dispute concerns the interpretation, application or validity of the Agreement, the parties must bring action before the EU General Court — or, on appeal, the EU Court of Justice — under Article 272 of the Treaty on the Functioning of the EU (TFEU).

For non-EU beneficiaries (if any), such disputes must be brought before the courts of Brussels, Belgium — unless an international agreement provides for the enforceability of EU court judgements.

For beneficiaries with arbitration as special dispute settlement forum (if any; see Data Sheet, Point 5), the dispute will — in the absence of an amicable settlement — be settled in accordance with the Rules for Arbitration published on the Portal.

If a dispute concerns administrative sanctions, offsetting or an enforceable decision under Article 299 TFEU (see Articles 22 and 34), the beneficiaries must bring action before the General Court — or, on appeal, the Court of Justice — under Article 263 TFEU.

For grants where the granting authority is an EU executive agency (see Preamble), actions against offsetting and enforceable decisions must be brought against the European Commission (not against the granting authority; see also Article 22).

## **ARTICLE 44 — ENTRY INTO FORCE**

The Agreement will enter into force on the day of signature by the granting authority or the coordinator, depending on which is later.

SIGNATURES

For the coordinator

For the granting authority



## **ANNEX 1**



# **Digital Europe Programme (DIGITAL)**

## **Description of the action (DoA)**

**Part A**

**Part B**

DESCRIPTION OF THE ACTION (PART A)

COVER PAGE

Part A of the Description of the Action (DoA) must be completed directly on the Portal Grant Preparation screens.

PROJECT	
Grant Preparation (General Information screen) — Enter the info.	
Project number:	101227749
Project name:	National Coordination Centre 2.0 – The Czech Republic
Project acronym:	NCC-CZ 2.0
Call:	DIGITAL-ECCC-2024-DEPLOY-NCC-06
Topic:	DIGITAL-ECCC-2024-DEPLOY-NCC-06-MS-COORDINATION
Type of action:	DIGITAL-SIMPLE
Service:	ECCC
Project starting date:	fixed date: 1 January 2026
Project duration:	48 months

TABLE OF CONTENTS

Project summary .....3

List of participants ..... 3

List of work packages .....4

Staff effort ..... 13

List of deliverables ..... 14

List of milestones (outputs/outcomes) ..... 19

List of critical risks ..... 21

Project reviews ..... 24

## PROJECT SUMMARY

<p><b>Project summary</b></p> <p><i>Grant Preparation (General Information screen) — Provide an overall description of your project (including context and overall objectives, planned activities and main achievements, and expected results and impacts (on target groups, change procedures, capacities, innovation etc)). This summary should give readers a clear idea of what your project is about.</i></p> <p><i>Use the project summary from your proposal.</i></p>
<p>The goal of the project is to support the activities of National Coordination Centre (NCC-CZ) in the Czech Republic, which is a part of the network of National Coordination Centres. The authority responsible for NCC-CZ is the National Cyber Information and Security Agency (NUKIB), which will be supported by an affiliated entity - Cyber Security Hub (CSH). The NCC-CZ will carry out the activities in line with the relevant European regulation (EU) 2021/887. NCC-CZ will cooperate with the European Competence Centre and with the other NCCs within the Network. The NCC-CZ 2.0 project also includes substantial financial support to third parties with a focus on SMEs and other stakeholders. All the planned activities are described in detail in the project application.</p>

## LIST OF PARTICIPANTS

<p><b>PARTICIPANTS</b></p> <p><i>Grant Preparation (Beneficiaries screen) — Enter the info.</i></p>					
Number	Role	Short name	Legal name	Country	PIC
1	COO	NUKIB	NARODNI URAD PRO KYBERNETICKOU A INFORMACNI BEZPECNOST - NUKIB	CZ	907198418
1.1	AE	CSH	CYBERSECURITY HUB, ZU	CZ	889292509



## LIST OF WORK PACKAGES

Work packages						
Grant Preparation (Work Packages screen) — Enter the info.						
Work Package No	Work Package name	Lead Beneficiary	Effort (Person-Months)	Start Month	End Month	Deliverables
WP1	Project Management and Coordination	1 - NUKIB	84.00	1	48	D1.1 – Project Management Handbook
WP2	Enhancing Cybersecurity Awareness and Engagement	1.1 - CSH	100.00	1	48	D2.1 – Communication, Dissemination and Exploitation Strategy D2.2 – Awareness Raising Needs Report D2.3 – Awareness and Engagement Campaign Materials D2.4 – Final Awareness and Engagement Impact Report
WP3	Financial Support for Strengthening Cybersecurity Capabilities	1.1 - CSH	134.00	4	48	D3.1 – Strategy Document for FSTP Priorities D3.2 – Call Impact Evaluation I D3.3 – Call Impact Evaluation II D3.4 – Monitoring and Impact Evaluation Report
WP4	Cybersecurity Community Building and Engagement	1 - NUKIB	97.00	1	48	D4.1 – Community Membership Management Report D4.2 – Knowledge Sharing and Engagement Report D4.3 – Final Community Impact Report

**Work package WP1 – Project Management and Coordination**

<b>Work Package Number</b>	WP1	<b>Lead Beneficiary</b>	1 - NUKIB
<b>Work Package Name</b>	Project Management and Coordination		
<b>Start Month</b>	1	<b>End Month</b>	48

**Objectives**

The objectives of the WP 1 Project Management and Coordination are:

- Ensure effective coordination and oversight: Establish and maintain efficient project coordination mechanisms, including regular consortium meetings, communication channels, and collaborative tools, to streamline interactions among both project partners.
- Project monitoring and evaluation: Implement monitoring and evaluation processes to track project progress, assess milestones, and ensure alignment with project objectives.
- Financial management and reporting: Oversee financial planning, budgeting, and expenditure tracking. Prepare periodic financial reports in compliance with funding requirements, ensuring transparency and efficient use of resources.
- Documentation and deliverables management: Coordinate the timely completion and submission of all project deliverables. Ensure quality control processes are applied to maintain high standards across all outputs.
- Risk management and mitigation: Identify potential risks related to project implementation and develop risk management strategies to mitigate them effectively. Monitor and address emerging risks throughout the project lifecycle. These objectives will provide a structured foundation for effective project management, ensuring that all project activities are executed efficiently and aligned with the overall strategic goals.

**Description**

WP1 will provide a structured foundation for effective project management, ensuring that all project activities are executed efficiently and aligned with the overall strategic goals.

T1.1 Project team and consortium coordination: Coordination and management of the NCC-CZ 2.0 project team, including regular meetings to monitor progress, address needs, and ensure effective communication among partners. Facilitation of GeA and PSC meetings to provide oversight, align strategies, and support decision-making within the consortium. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB), AE (CSH). No In-kind Contributions and Subcontracting.

T1.2 Project monitoring and reporting: Tracking project progress against objectives, deliverables, timelines, and budgets while ensuring quality standards and alignment with project goals. Monitoring and evaluation of milestones, along with regular reporting to document achievements, address risks and ensure timely submission of all deliverables. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB), AE (CSH). No In-kind Contributions and Subcontracting.

T1.3 Financial management: Financial planning, including budget preparation, updates, and management of purchase requests and expenditures. Ensuring compliance with procurement procedures, accurate financial tracking, and reporting. Preparation of financial reports to maintain transparency, ensure efficient resource use, and align financial activities with project objectives and regulations. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB), AE (CSH). No In-kind Contributions and Subcontracting.

T1.4 Risk management and mitigation: Identification, assessment, and management of project risks through a risk assessment framework and regular evaluations. Development and implementation of mitigation strategies to minimize impacts on project objectives. Maintaining an updated risk list to enable proactive responses and effective management throughout the project lifecycle. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB), AE (CSH). No In-kind Contributions and Subcontracting.

**Work package WP2 – Enhancing Cybersecurity Awareness and Engagement**

<b>Work Package Number</b>	WP2	<b>Lead Beneficiary</b>	1.1 - CSH
<b>Work Package Name</b>	Enhancing Cybersecurity Awareness and Engagement		

<b>Start Month</b>	<b>1</b>	<b>End Month</b>	<b>48</b>
--------------------	----------	------------------	-----------

### Objectives

The objectives of the WP 2 Enhancing Cybersecurity Awareness and Engagement are:

- Mapping awareness-raising needs: Building on the initial NCC-CZ Needs Analysis, NCC-CZ 2.0 will target outreach based on previously identified gaps in cybersecurity education, R&D, and related fields, ensuring activities are aligned with evolving priorities.
- Targeting awareness raising in cybersecurity: Expanding on NCC-CZ's initial activities, NCC-CZ 2.0 will focus on enhancing cybersecurity awareness among SMEs, academic and research institutions, public organizations, and NGOs, particularly in R&D and EU funding opportunities, focusing also on current topics and challenges, to foster active engagement.
- Ensuring visibility of project outcomes and results: Using dissemination strategies from NCC-CZ, NCC-CZ 2.0 will effectively communicate project activities through social media, events, and digital platforms, maximizing reach and adoption within the cybersecurity community.
- Supporting synergies between national and EU initiatives: NCC-CZ 2.0 will align with national and EU cybersecurity efforts by coordinating with stakeholders to harmonize standards and integrate complementary training activities, enhancing the reach and relevance of cybersecurity skills development.
- Support project development and collaboration: Provide information and guidance on relevant EU funding programs, including Digital Europe Programme (DEP) and Horizon Europe (HE) and facilitate collaboration among community members through idea-pitching meet-ups, networking events, working groups, and thematic discussions, promoting joint projects and initiatives.

These objectives will establish a framework for NCC-CZ 2.0 to enhance cybersecurity awareness, engagement, and collaboration, ensuring impactful and aligned activities.

#### KPIs

- Number of awareness-raising, capacity building and training events organized and/or attended: 60
- Number of stakeholders reached through events: 250
- Number of stakeholders engaged through awareness campaigns: 1 000
- Number of Technology Open Days organised: 8
- Number of awareness-raising and capacity building webinars organised: 16

### Description

WP2 will establish a framework for NCC-CZ 2.0 to enhance cybersecurity awareness, engagement, and collaboration, ensuring impactful and aligned activities.

T2.1 Identifying and planning awareness raising activities: Identification of current awareness-raising needs in cybersecurity, addressing gaps in education, R&D, funding opportunities, and related areas, building on the initial Needs Analysis from the NCC-CZ project. Outreach to SMEs, research institutions, academia, public entities, and NGOs through webinars, expert meetings, events, and direct stakeholder engagement. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB), AE (CSH). No In-kind Contributions and Subcontracting.

T2.2 Amplifying project visibility and stakeholder reach: This task focuses on enhancing the visibility of NCC-CZ 2.0 activities and outcomes by building on proven communication strategies from the NCC-CZ project. Through targeted use of social media, digital platforms, and strategic event participation, this task aims to reach a broad audience, optimize outreach, and maximize engagement from key stakeholders within the cybersecurity community. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB), AE (CSH). No In-kind Contributions and Subcontracting.

T2.3 Strengthening collaboration across the NCC Network: Leveraging partnerships with other NCCs, this task aims to facilitate collaboration and knowledge sharing across the NCC

Network. NCC-CZ 2.0 will actively seek partnerships with other NCCs, including those in the neighbouring countries to enable best-practice exchanges and collaborate in awareness-raising initiatives. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB), AE (CSH). No In-kind Contributions and Subcontracting.

T2.4 Skills development and engagement: Mapping and promotion of activities addressing the cybersecurity skills shortage, including educational workshops, bootcamps, and campaigns to attract young talents. Collaboration with community members to improve access to a skilled cybersecurity talent pool. Ensure collaboration with relevant entities at the national and/or EU level to achieve synergies and avoid duplication of efforts through Technology Open Days focused on sharing of best practices and innovative solutions and capacity building webinars. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB), AE (CSH). No In-kind Contributions and Subcontracting.

T2.5 Project development and support: Provision of information on current funding calls under DEP and Horizon Europe, including partner search announcements and guidance on proposal preparation. Support for forming project consortia and fostering collaboration among members to develop joint project proposals. Dissemination of community-developed tools and materials through a public repository and connection with relevant stakeholders to maximize impact. Ensure alignment with NCPs for DEP and HE programs. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB), AE (CSH). No In-kind Contributions and Subcontracting.

**Work package WP3 – Financial Support for Strengthening Cybersecurity Capabilities**

Work Package Number	WP3	Lead Beneficiary	1.1 - CSH
Work Package Name	Financial Support for Strengthening Cybersecurity Capabilities		
Start Month	4	End Month	48

Objectives
<p>This WP 3 Financial Support for Strengthening Cybersecurity Capabilities focuses on enhancing the existing NCC-CZ FSTP mechanism and strategically implementing it to support high-impact projects within the cybersecurity domain. Drawing on lessons learned from previous NCC-CZ FSTP calls, this WP will refine and optimize the FSTP processes to maximize efficiency, transparency, and impact. The WP 3 will also conduct continuous needs assessments within the cybersecurity landscape, ensuring that the financial support provided aligns with emerging challenges, technological advancements and current needs.</p> <p>The implementation of this WP will involve three strategic calls for proposals over the project’s duration, with each call tailored to address priority areas identified through ongoing analysis. These calls will aim to strengthen cybersecurity capabilities among small and medium-sized enterprises (SMEs) and other eligible entities, thereby contributing to societal cybersecurity resilience and supporting the EU's goals of digital sovereignty and strategic autonomy. This WP will adopt a more SME-focused approach, while also ensuring an allocation for other types of entities to address diverse needs and priorities identified throughout the project.</p> <ul style="list-style-type: none"><li>▪ Strengthen the existing FSTP mechanism: Build on the established FSTP framework developed within the NCC-CZ project, refining processes based on prior implementation experiences. This includes optimizing the application, evaluation, and monitoring procedures to ensure streamlined and effective support distribution.</li><li>▪ Identify needs and set priorities: Conduct continuous needs assessments to understand the cybersecurity challenges and needs within the target ecosystem. Based on the findings, develop a strategic document that outlines the types of projects and activities to prioritize, ensuring that the FSTP funding addresses the most critical needs.</li><li>▪ Implement three calls for proposals: Over the four-year project, launch three targeted FSTP calls, each strategically designed to focus on identified high-impact areas. These calls will address current cybersecurity needs, adapting based on the outcomes of previous rounds to maximize impact and relevance.</li><li>▪ Implement comprehensive project management and impact evaluation: Oversee the entire lifecycle of FSTP supported projects, including application processing, project selection, implementation monitoring, contract administration, and reporting. Conduct impact evaluations to measure project outcomes and assess the overall effectiveness of FSTP support, ensuring alignment with project goals and strategic impact.</li></ul> <p>KPIs</p> <ul style="list-style-type: none"><li>• Number of supported projects aligned with EU and Czech cybersecurity priorities: 25</li><li>• Number of entities benefiting from FSTP cascade financing: 25</li><li>• Number of entities provided with information and technical support related to funding opportunities: 50</li><li>• Number of webinars focused on FSTP calls and project drafting: 8</li></ul> <p>Areas of support</p> <p>The expected areas of support within the FSTP calls for proposals are designed to enhance cybersecurity resilience and strategic autonomy in alignment with EU priorities. At this stage, these areas are outlined in general terms; their descriptions and focus will be refined through ongoing analyses and continuous needs assessments conducted throughout the NCC-CZ 2.0 project’s lifecycle. This adaptive approach ensures that the support remains relevant to emerging cybersecurity challenges and technological advancements. These following preliminary areas of support have been identified:</p> <ul style="list-style-type: none"><li>▪ Development of innovative cybersecurity solutions by SMEs: Priority will be given to supporting SMEs in developing innovative cybersecurity solutions that address specific, high-impact security needs. This area focuses on fostering technological innovation within the SME sector, contributing to the broader ecosystem’s resilience and adaptability.</li></ul>

- Adoption of advanced cybersecurity solutions: Supporting the uptake and implementation of state-of-the-art cybersecurity technologies within SMEs is crucial to raising the security standards across sectors. This category will prioritize projects that help SMEs adopt robust and scalable cybersecurity solutions, promoting industry-wide improvements in cybersecurity readiness.

- Enhancement of cybersecurity governance and best practices: Many SMEs lack formalized governance frameworks for cybersecurity. This area will support projects aimed at developing or implementing cybersecurity governance and best practices within SMEs, helping them establish effective policies and procedures.

- Cybersecurity resilience support for NGOs, academic and research organizations, and other stakeholders: Recognizing the broader community's role in cybersecurity, this category will support actions by non-SME entities, such as NGOs or academic and research institutions, that foster public awareness, education, and research in cybersecurity resilience. Examples include creating educational resources, organizing youth events or competitions, developing information hubs linking to training opportunities, and hosting conferences, webinars, or workshops on current cybersecurity topics, including those for exercise and training communities on topics directly related to exercise, training and education.

Financial support will be made available across the preliminary defined areas to assist entities in achieving compliance with EU legislative requirements (e.g., NIS2, CRA, CSA) within the FSTP framework.

Criteria for giving support and evaluation process:

To ensure effective selection and impactful outcomes, all submitted projects will be evaluated based on a set of transparent criteria focused on quality, feasibility, and impact.

The evaluation process will align with the established processes of NCC-CZ FSTP Mechanism and the NCC-Council, building on the framework of the first NCC-CZ project, with necessary adjustments based on current needs and lessons learned.

The evaluation process is structured as a round-based call, ensuring that the exact time of submission within the call's time-frame does not influence the outcome of the evaluation. Each project is thoroughly assessed by at least two independent experts: a designated reviewer, who conducts a detailed evaluation, and a NCC-CZ Council Rapporteur, who provides additional insight and context for the evaluation. After these individual evaluations are completed, the NCC-Council convenes to discuss the project in depth. This process ensures that a wide range of perspectives is considered, including the alignment of the project with strategic goals and its potential impact. Based on this discussion, the NCC-Council formulates a recommendation, either supporting or rejecting the project for funding. This recommendation is then forwarded to the Director of NUKIB, who makes the final decision regarding project approval or rejection, ensuring a balanced and transparent decision-making process.

The evaluation process will apply the following key criteria:

- Relevance to priority areas: Projects will be assessed on their alignment with the priority areas of support, as well as their ability to address specific cybersecurity needs identified through the project's ongoing analyses.

- Innovation and technological advancement: This criterion evaluates the degree of innovation in the proposed project. Priority will be given to projects that contribute novel approaches or technologies, especially those that have potential for significant advancements in cybersecurity.

- Feasibility and implementation capacity: Projects must demonstrate realistic plans and resources for implementation, including technical and organizational capacity. This includes evaluating the applicant's experience, capabilities, and readiness to execute the proposed project effectively.

- Impact and strategic contribution: Projects will be assessed on their potential impact within the Czech Republic or for entities based in the Czech Republic, also projects that align with EU strategic autonomy in cybersecurity and demonstrate broad, scalable benefits will be prioritized.

- Sustainability and long-term benefits: Evaluators will consider the project's potential for sustainable impact within the Czech Republic, including how its benefits will continue beyond the initial funding period and its potential for industry-wide adoption or replication.

- Cost-effectiveness and efficient use of funds: Projects will be reviewed for their budgetary alignment and cost-effectiveness, ensuring that requested funding is reasonable and will be used efficiently to achieve the stated objectives. Conditions for implementing the grants for financial support:

- The following eligibility conditions (among others) will be specified in the calls for proposals; if the applicant is a legal entity, it will provide the following

evidence with its application: information on the beneficial owner of the legal person in accordance with the law regulating the registration of beneficial owners in the form of a full statement of the valid data and data that have been deleted without replacement or replaced by new data, if it is a registering person; where the applicant for funding is a foreign legal person, it shall provide evidence of its beneficial owner either by means of an extract from a foreign register similar to the register of beneficial owners or, where no such foreign register exists, by providing the identification data of all persons who are the beneficial owner of the foreign legal person, and submit documents showing the relationship of



all persons to the foreign legal person, in particular an extract from a foreign register similar to the commercial register, a list of shareholders, a decision of the statutory body on the payment of a share of profits, the memorandum of association, the articles of association or the articles of association, information on the identification of the persons in whom the legal person (i.e. the applicant) has a shareholding and the amount of that shareholding.

- The Applicant's Affidavit of Eligibility will require the Applicant to certify that: he meets the condition of no conflict of interest between the Applicant or its stakeholders on the one hand and the Provider of the support on the other hand, he is not a legal person whose beneficial owner is a public official referred to in Section 4c of Act No 159/2006 Coll., on Conflict of Interest, as amended, or a legal person controlled by it, he does not have any beneficial owner listed among the persons subject to sanctions applicable under Act on the Implementation of International Sanctions, in conjunction with Act on Restrictive Measures against Certain Serious Acts in International Relations (Sanctions Act), or under European legislation [e.g. Article 29 of the Treaty on European Union (TEU), Article 215 of the Treaty on the Functioning of the EU (TFEU)], he ensures the registration of the legally required data on its beneficial owners within the meaning of Act No 37/2021 Coll. on the registration of beneficial owners.

- Maximum amount per third party: 100 000 EUR; taking into consideration that amounts of more than 60 000 EUR per third party are necessary because the nature of the actions under this call is such that their objectives would otherwise be impossible or overly difficult to achieve as stated in the call document

- Funding rate: mandatory co-financing of 50% by the supported third party with other amounts based on a type of entity not excluded

- Criteria for calculating the exact amounts: budget categories and cost eligibility rules will be in line with the Call document and DEP rules

- Types of activity that qualify (closed list): innovation, concept development and experimentation, proof-of-concept delivery, demonstration, analysis, organisation of events and courses, networking, awareness raising activities, capacity building, methodology, software, guidelines and best practices, technical documentation and user's manuals, data repositories, evaluation frameworks, feasibility studies, audits and implementation of compliance measures

- Person/categories of persons to be supported: SMEs, start-ups\*, academic and research organizations\*\*, NGOs

The group of targeted stakeholders may be adjusted for individual calls based on the topic of the call.

The calls will be administered under the following conditions as specified in the Call document:

- the calls must be open, published widely and conform to EU standards concerning transparency, equal treatment, conflict of interest and confidentiality

- the calls must be published on the Funding & Tenders Portal, and on the participants' websites

- the calls must remain open for at least two months

- if call deadlines are changed this must immediately be published on the Portal and all registered applicants must be informed of the change

- the outcome of the call must be published on the participants' websites, including a description of the selected projects, award dates, project durations, and final

recipient legal names and countries

- the calls must have a clear European dimension.

\*start-up is understood as a business entity that is newly established or a start-up company (established up to 3 years before the submission of the project application), which is developing rapidly on the basis of an innovative business concept using advanced technologies and has a high potential for economic growth.

\* for academic and research organisation, a following definition of a "research and knowledge dissemination organisation" will be used as defined in the Communication from the Commission - Framework for State aid for research and development and innovation (2014/C 198/01)

## Description

WP 3 focuses on enhancing the existing NCC-CZ FSTP mechanism and strategically implementing it to support high-impact projects within the cybersecurity domain. Drawing on lessons learned from previous NCC-CZ FSTP calls, this WP will refine and optimize the FSTP processes to maximize efficiency, transparency, and impact. The WP 3 will also conduct continuous needs assessments within the cybersecurity landscape, ensuring that the financial support provided aligns with emerging challenges, technological advancements and current needs. The implementation of this WP will involve three strategic calls for proposals over the project's duration, with each call tailored to address priority areas identified through ongoing analysis. These calls will aim to strengthen cybersecurity capabilities among small and medium-sized enterprises (SMEs) and other eligible entities, thereby

contributing to societal cybersecurity resilience and supporting the EU's goals of digital sovereignty and strategic autonomy. This WP will adopt a more SME-focused approach, while also ensuring an allocation for other types of entities to address diverse needs and priorities identified throughout the project.

Each FSTP call will clearly define which EU/CZ policies will the supported project contribute to, including specific and measurable KPIs to be achieved in individual projects (number of entities/products aligned/in compliance with EU/

CZ regulatory requirements or strategies; number of actions to support SMEs and/or public institutions to implement innovative and state of the art cybersecurity solutions into their operations, measurable improvement in cybersecurity posture in supported entities, etc.). The specific focus of the upcoming Calls will thus address the current security situation as well as developments within the national and European context.

**T3.1 Needs assessment and strategy development:** The project team will conduct continuous assessments to identify emerging cybersecurity needs and update funding priorities for FSTP calls. Before publishing each call for proposals, the project team will develop an updated strategy document that outlines priority areas and types of projects to be supported based on identified needs and priorities. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB) AE (CSH). No In-kind Contributions and Subcontracting.

**T3.2 Implementation of FSTP calls and project selection:** This task will focus on execution of three FSTP calls for proposals over the project duration. This task includes preparing, publishing, and promoting the calls, managing the application process, and conducting transparent evaluations to select high-impact projects aligned with identified priority areas. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB) AE (CSH). No In-kind Contributions and Subcontracting.

**T3.3 Monitoring, impact evaluation, and reporting:** The project team will oversee the implementation of selected projects, ensuring compliance with funding conditions and alignment with project objectives, conduct impact evaluations at the end of each call cycle, and produce reports on outcomes, progress, and lessons learned for each FSTP call. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB) AE (CSH). No In-kind Contributions and Subcontracting.

**T3.4 Enhancement of FSTP mechanism:** The project team aims to continuously improve the FSTP mechanism based on feedback from each call wave. Refinements will focus on optimizing application, evaluation, and monitoring processes to ensure transparency, efficiency, and effective support distribution for high-impact cybersecurity projects. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB) AE (CSH). No In-kind Contributions and Subcontracting.

## Work package WP4 – Cybersecurity Community Building and Engagement

<b>Work Package Number</b>	WP4	<b>Lead Beneficiary</b>	1 - NUKIB
<b>Work Package Name</b>	Cybersecurity Community Building and Engagement		
<b>Start Month</b>	1	<b>End Month</b>	48

### Objectives

This WP 4 Cybersecurity Community Building and Engagement focuses on growing and managing the cybersecurity community while enhancing collaboration, knowledge sharing, and capacity building among stakeholders like SMEs, academia, public administration, and NGOs. It aims to expand the community, strengthen its ability to address cybersecurity challenges, and establish process for EU Cybersecurity Competence Community management. These efforts align with NCC-CZ and ECCC objectives to support the EU's cybersecurity resilience and strategic autonomy.

This work package is dedicated to fostering the growth, management, and impactful engagement of the cybersecurity community. It aims to strengthen collaboration, knowledge sharing, and capacity building among diverse stakeholders, including SMEs, academic and research organizations, public administration, and NGOs. By leveraging targeted recruitment, structured management processes, and tailored activities, this WP will expand the community's size and enhance its ability to address evolving cybersecurity challenges.

The WP will also prioritize creating sustainable systems for managing community memberships and amplifying the impact of community-driven initiatives. These efforts will align with the broader objectives of the NCC-CZ and the ECCC, contributing to the overall resilience and strategic autonomy of the EU in cybersecurity.

Objectives:

- Expand and strengthen the cybersecurity community: Foster collaboration within the national cybersecurity community by strengthening network ties, promoting active participation in activities, encouraging cooperation and promoting membership in the European Cybersecurity Competence Community. Expand the community by attracting and retaining diverse members through clear communication of membership benefits and added value provided by the NCC-CZ, ECCC, and the Network. Ensure alignment with national-level activities and create synergies with the CYRIS group coordinated by NUKIB.

<ul style="list-style-type: none"><li>▪ Cooperate across the NCC Network: Support cross-border collaboration with other national communities across EU member states by fostering cooperation and aligning activities with other NCCs within the Network. Emphasize collaboration and coordination across the NCC Network through knowledge sharing, best-practice exchange, and connecting national communities to strengthen the EU-wide cybersecurity ecosystem. Build on existing partnerships with neighbouring NCCs, such as NCC-SK and NCC-AT, while exploring opportunities for joint activities and furthering regional cooperation to address shared cybersecurity challenges.</li><li>▪ Manage community membership processes: Set-up processes and manage the assessment of membership applications to the Cybersecurity Competence Community, ensuring compliance with national legislation, ECCC guidelines and integration with EU-wide processes and maintain and enhance technical tools, for example a communication platform, to streamline interactions and collaboration among members.</li><li>▪ Promote knowledge sharing and networking activities: Organize and support activities such as workshops, webinars, and conferences to facilitate collaboration, knowledge exchange, and engagement with national and EU stakeholders.</li><li>▪ Amplify community achievements and deliverables: Disseminate the results of community efforts, such as educational materials and tools, by creating a public repository of reusable resources and connecting providers with relevant stakeholders.</li><li>▪ Provide expertise and contribute to the strategic tasks of the ECCC: Ensure active involvement of the NCC-CZ in ECCC activities, taking into account relevant challenges on the national and regional level.</li></ul> <p>KPIs</p> <ul style="list-style-type: none"><li>▪ Number of community members engaged: 270</li><li>▪ Number of actions to foster expertise and synergies within the community: 50</li><li>▪ Number of collaborative actions with NCCs and ECCC: 30</li><li>▪ Number of reusable resources shared in the public repository: 30</li><li>▪ Number of organised community meetings: 8</li><li>▪ Numbers of activities aimed at the promotion of membership in EU Cybersecurity Competence Community: 5</li></ul>
--

Description
<p>WP 4 Cybersecurity Community Building and Engagement focuses on growing and managing the cybersecurity community while enhancing collaboration, knowledge sharing, and capacity building among stakeholders like SMEs, academia, public administration, and NGOs. It aims to expand the community, strengthen its ability to address cybersecurity challenges, and establish process for EU Cybersecurity Competence Community management. These efforts align with NCC-CZ and ECCC objectives to support the EU's cybersecurity resilience and strategic autonomy. This work package is dedicated to fostering the growth, management, and impactful engagement of the cybersecurity community. It aims to strengthen collaboration, knowledge sharing, and capacity building among diverse stakeholders, including SMEs, academic and research organizations, public administration, and NGOs. By leveraging targeted recruitment, structured management processes, and tailored activities, this WP will expand the community's size and enhance its ability to address evolving cybersecurity challenges. The WP will also prioritize creating sustainable systems for managing community memberships and amplifying the impact of community-driven initiatives. These efforts will align with the broader objectives of the NCC-CZ and the ECCC, contributing to the overall resilience and strategic autonomy of the EU in cybersecurity.</p> <p>T4.1 Community growth and engagement: This task focuses on fostering a collaborative cybersecurity ecosystem by combining strategic recruitment efforts with active community engagement. It involves developing and implementing targeted recruitment strategies to attract new members from SMEs, academic and research organizations, public administration, and NGOs, while promoting membership benefits through campaigns, webinars, and event participation. At the same time, it aims to strengthen national and EU-level network connections, share best practices, and build strong cross-sector relationships to enhance collaboration. By actively engaging stakeholders and encouraging their involvement, the task supports the growth of a cybersecurity community on the national and EU level. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB) AE (CSH). No In-kind Contributions and Subcontracting.</p> <p>T4.2 Membership management and technical support: Management of the EU Cybersecurity Competence Community membership lifecycle, including application processing, compliance checks, and regular data updates. Development and upkeep of a national NCC-CZ registration portal, fully compatible with the EU Atlas database, with the implementation of automated solutions, such as APIs, to enable seamless data transfer between NCC-CZ and Atlas. Maintenance and enhancement of technical tools (for example communication platform to ensure smooth interaction between national community representatives, Czech members in the EU Cybersecurity Competence Community members and the NCC-CZ). Participants on this tasks are NUKIB and CSH, roles COO (NUKIB) AE (CSH). No In-kind Contributions and Subcontracting.</p>




T4.3 Knowledge sharing and networking activities: Organization of workshops, events, webinars, working group meetings, and conferences to foster collaboration, knowledge sharing, and engagement, along with active participation in similar activities organized by NUKIB and other entities (for example CyberCon, Prague Cyber Security Conference). This includes hosting initiatives that emphasize cross-sector collaboration, emerging cybersecurity topics, and ensuring compliance with EU legislation. Coordination with the CYRIS group and other national stakeholders ensures alignment and maximizes impact. Joint activities with other NCCs will also be included, focusing on sharing best practices and exploring opportunities for collaborative actions. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB) AE (CSH). No In-kind Contributions and Subcontracting.

T4.4 ECCC support and active involvement: Active participation in ECCC working groups and other activities, providing expertise, and contributing to strategic tasks while addressing national and regional cybersecurity challenges. Aligning national priorities with ECCC objectives. Participants on this tasks are NUKIB and CSH, roles COO (NUKIB) AE (CSH). No In-kind Contributions and Subcontracting.

STAFF EFFORT

Staff effort per participant					
Grant Preparation (Work packages - Effort screen) — Enter the info.					
Participant	WP1	WP2	WP3	WP4	Total Person-Months
1 - NUKIB	70.00	40.00	100.00	70.00	280.00
1.1 - CSH	14.00	60.00	34.00	27.00	135.00
Total Person-Months	84.00	100.00	134.00	97.00	415.00

## LIST OF DELIVERABLES

<b>Deliverables</b> <i>Grant Preparation (Deliverables screen) — Enter the info.</i> <i>The labels used mean:</i> <i>Public — fully open ( automatically posted online)</i> <i>Sensitive — limited under the conditions of the Grant Agreement</i> <i>EU classified —RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision <a href="#">2015/444</a></i>						
Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D1.1	Project Management Handbook	WP1	1 - NUKIB	R — Document, report	SEN - Sensitive	2
D2.1	Communication, Dissemination and Exploitation Strategy	WP2	1 - NUKIB	R — Document, report	SEN - Sensitive	4
D2.2	Awareness Raising Needs Report	WP2	1.1 - CSH	R — Document, report	SEN - Sensitive	6
D2.3	Awareness and Engagement Campaign Materials	WP2	1 - NUKIB	R — Document, report	PU - Public	18
D2.4	Final Awareness and Engagement Impact Report	WP2	1.1 - CSH	R — Document, report	PU - Public	48
D3.1	Strategy Document for FSTP Priorities	WP3	1 - NUKIB	R — Document, report	SEN - Sensitive	8
D3.2	Call Impact Evaluation I	WP3	1.1 - CSH	R — Document, report	SEN - Sensitive	22
D3.3	Call Impact Evaluation II	WP3	1.1 - CSH	R — Document, report	SEN - Sensitive	34
D3.4	Monitoring and Impact Evaluation Report	WP3	1.1 - CSH	R — Document, report	SEN - Sensitive	48
D4.1	Community Membership Management Report	WP4	1 - NUKIB	R — Document, report	SEN - Sensitive	24
D4.2	Knowledge Sharing and Engagement Report	WP4	1.1 - CSH	R — Document, report	PU - Public	36
D4.3	Final Community Impact Report	WP4	1 - NUKIB	R — Document, report	SEN - Sensitive	48

**Deliverable D1.1 – Project Management Handbook**

<b>Deliverable Number</b>	D1.1	<b>Lead Beneficiary</b>	1 - NUKIB
<b>Deliverable Name</b>	Project Management Handbook		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	SEN - Sensitive
<b>Due Date (month)</b>	2	<b>Work Package No</b>	WP1

Description			
<p>The Project Management Handbook is a core document that consolidates essential project activities, providing guidance on administration, procedures, communication, knowledge management, and monitoring. It outlines objectives, roles, responsibilities, and workflows, ensuring team alignment and supporting consistent, efficient project management.</p> <p>Electronic document, English</p>			

**Deliverable D2.1 – Communication, Dissemination and Exploitation Strategy**

<b>Deliverable Number</b>	D2.1	<b>Lead Beneficiary</b>	1 - NUKIB
<b>Deliverable Name</b>	Communication, Dissemination and Exploitation Strategy		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	SEN - Sensitive
<b>Due Date (month)</b>	4	<b>Work Package No</b>	WP2

Description			
<p>The strategy will identify key communication channels for distributing information to target groups, design an approach to maximize the project's reach and outputs, and guide implementation across activities. It will also include an exploitation plan to ensure the long-term use of project results.</p> <p>Electronic document, English</p>			

**Deliverable D2.2 – Awareness Raising Needs Report**

<b>Deliverable Number</b>	D2.2	<b>Lead Beneficiary</b>	1.1 - CSH
<b>Deliverable Name</b>	Awareness Raising Needs Report		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	SEN - Sensitive
<b>Due Date (month)</b>	6	<b>Work Package No</b>	WP2

Description			
<p>A report identifying gaps in cybersecurity awareness based on updated needs analysis, targeting SMEs, research institutions, public organizations, and other stakeholders.</p> <p>Electronic document, English</p>			

**Deliverable D2.3 – Awareness and Engagement Campaign Materials**

<b>Deliverable Number</b>	D2.3	<b>Lead Beneficiary</b>	1 - NUKIB
<b>Deliverable Name</b>	Awareness and Engagement Campaign Materials		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	PU - Public
<b>Due Date (month)</b>	18	<b>Work Package No</b>	WP2

Description
Creation and distribution of materials (e.g. brochures, presentations, and digital media content) to support awareness campaigns. Various, Czech/English

### Deliverable D2.4 – Final Awareness and Engagement Impact Report

Deliverable Number	D2.4	Lead Beneficiary	1.1 - CSH
Deliverable Name	Final Awareness and Engagement Impact Report		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	48	Work Package No	WP2

Description
A comprehensive report summarizing the outcomes of all awareness and engagement efforts, including engagement metrics, success stories, and sustainability plans. Electronic document, English

### Deliverable D3.1 – Strategy Document for FSTP Priorities

Deliverable Number	D3.1	Lead Beneficiary	1 - NUKIB
Deliverable Name	Strategy Document for FSTP Priorities		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	8	Work Package No	WP3

Description
A strategy document defining priority areas and project types for FSTP support will be developed at the start of the project. This document will serve as a guiding framework throughout the project's duration, with the flexibility to be updated as needed to incorporate additional priority areas based on evolving needs and emerging cybersecurity challenges. Electronic document, English

### Deliverable D3.2 – Call Impact Evaluation I

Deliverable Number	D3.2	Lead Beneficiary	1.1 - CSH
Deliverable Name	Call Impact Evaluation I		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	22	Work Package No	WP3

Description
Call Impact Evaluation I is focused on evaluating the impacts of the first call, drawing on interim results from the ongoing supported projects. The report will assess how these projects align with the call objectives, contribute to cybersecurity resilience, and address the needs of target groups. It will also evaluate the relevance and impact of the thematic focus of the first call, providing evidence to support the selection of an appropriate topic for the next call wave. Additionally, the report will highlight any emerging challenges or limitations observed during implementation, offering insights for improving 2nd call design and impact.

**Deliverable D3.3 – Call Impact Evaluation II**

<b>Deliverable Number</b>	D3.3	<b>Lead Beneficiary</b>	1.1 - CSH
<b>Deliverable Name</b>	Call Impact Evaluation II		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	SEN - Sensitive
<b>Due Date (month)</b>	34	<b>Work Package No</b>	WP3

**Description**

Call Impact Evaluation II is focused on evaluating the potential impacts of the first two calls, drawing on interim results from the ongoing supported projects. The report will assess how these projects align with the call objectives, contribute to cybersecurity resilience, and address the needs of target groups. It will also evaluate the relevance and impact of the thematic focus of the first two waves of calls, providing evidence to support the selection of an appropriate topic for the next call wave. Additionally, the report will highlight any emerging challenges or limitations observed during implementation, offering insights for improving 3rd call design and impact.

**Deliverable D3.4 – Monitoring and Impact Evaluation Report**

<b>Deliverable Number</b>	D3.4	<b>Lead Beneficiary</b>	1.1 - CSH
<b>Deliverable Name</b>	Monitoring and Impact Evaluation Report		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	SEN - Sensitive
<b>Due Date (month)</b>	48	<b>Work Package No</b>	WP3

**Description**

A report evaluating the outcomes and impacts of supported projects, including their alignment with objectives, challenges encountered, and contributions to cybersecurity resilience. It will also include a summary of FSTP mechanism improvements, process enhancements, and recommendations for future refinements to optimize impact. Reports detailing the evaluation and selection process for each call wave, including application summaries, scoring results, and justifications for selected projects. These reports will ensure transparency and document the rationale behind project selection.

Electronic document, English

**Deliverable D4.1 – Community Membership Management Report**

<b>Deliverable Number</b>	D4.1	<b>Lead Beneficiary</b>	1 - NUKIB
<b>Deliverable Name</b>	Community Membership Management Report		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	SEN - Sensitive
<b>Due Date (month)</b>	24	<b>Work Package No</b>	WP4

**Description**

A report detailing the recruitment efforts, growth metrics, and the membership lifecycle process. Includes an overview of applications processed, compliance checks, and the functionality of technical tools.

Electronic document, English

**Deliverable D4.2 – Knowledge Sharing and Engagement Report**

<b>Deliverable Number</b>	D4.2	<b>Lead Beneficiary</b>	1.1 - CSH
<b>Deliverable Name</b>	Knowledge Sharing and Engagement Report		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	PU - Public
<b>Due Date (month)</b>	36	<b>Work Package No</b>	WP4

Description
A comprehensive report summarizing all knowledge-sharing and networking activities, including workshops, webinars, working group meetings, and conferences. Highlighting outcomes, participant feedback, and recommendations for future initiatives. Including information on collaboration activities within the NCC Network. Electronic document, English

**Deliverable D4.3 – Final Community Impact Report**

<b>Deliverable Number</b>	D4.3	<b>Lead Beneficiary</b>	1 - NUKIB
<b>Deliverable Name</b>	Final Community Impact Report		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	SEN - Sensitive
<b>Due Date (month)</b>	48	<b>Work Package No</b>	WP4

Description
A detailed final report evaluating the outcomes of community-building activities, including membership growth, knowledge-sharing events, skills development initiatives, and project collaborations. Includes recommendations for sustainability. Electronic document, English

## LIST OF MILESTONES

Milestones					
Grant Preparation (Milestones screen) — Enter the info.					
Milestone No	Milestone Name	Work Package No	Lead Beneficiary	Means of Verification	Due Date (month)
1	First project review	WP1	1 - NUKIB	First project report Description: First project report of the project is prepared/submitted.	18
2	Second project review	WP1	1 - NUKIB	Second project report Description: Second project report of the project is prepared/submitted.	36
3	Final project review and project closure	WP1	1 - NUKIB	Final project report Description: All activities are finished, final project report is prepared/submitted.	48
4	Completion of initial awareness activities	WP2	1.1 - CSH	Submission of the Awareness Raising Needs Report and materials. Description: First round of targeted awareness-raising activities implemented, including needs report and engagement materials, organised events, etc. Outcomes include documented participation metrics and feedback analysis.	18
5	Final evaluation of awareness and engagement efforts	WP2	1.1 - CSH	Submission of the Final Awareness and Engagement Impact Report Description: Comprehensive evaluation of all awareness and engagement activities conducted during the project. This includes a summary of lessons learned, metrics of engagement, and recommendations for sustaining the impact.	48
6	Publication of first wave of calls	WP3	1 - NUKIB	Call published on the F&T Portal Description: A complete set of published call documents, including eligibility criteria, application guidelines, and evaluation criteria.	12



<b>Milestones</b> <i>Grant Preparation (Milestones screen) — Enter the info.</i>					
<b>Milestone No</b>	<b>Milestone Name</b>	<b>Work Package No</b>	<b>Lead Beneficiary</b>	<b>Means of Verification</b>	<b>Due Date (month)</b>
7	Publication of second wave of calls	WP3	1 - NUKIB	Call published on the F&T Portal Description: A complete set of published call documents, including eligibility criteria, application guidelines, and evaluation criteria.	24
8	Publication of third wave of calls	WP3	1 - NUKIB	Call published on the F&T Portal Description: A complete set of published call documents, including eligibility criteria, application guidelines, and evaluation criteria.	36
9	Impact evaluation	WP3	1.1 - CSH	Monitoring and Impact Evaluation Report Description: Comprehensive evaluation of all supported projects across the three waves, including impact assessment, summary of outcomes and recommendations of FSTP mechanism improvements.	48
10	Repository of Community Resources	WP4	1 - NUKIB	Repository is active and available. Description: A repository featuring reusable educational materials, tools, and other resources either developed by national/European community members or specifically selected to support their needs. The repository will be continuously updated.	30
11	Completion of initial key community support activities	WP4	1 - NUKIB	Submission of the Knowledge Sharing and Skills Development Report. Description: Organization of at least 60% of planned workshops, webinars, and working group meetings. Includes collection of feedback for improvement.	36
12	Final evaluation of community growth and impact	WP4	1 - NUKIB	Submission of the Final Community Impact Report Description: Comprehensive evaluation of community growth, knowledge-sharing	48

Milestones					
Grant Preparation (Milestones screen) — Enter the info.					
Milestone No	Milestone Name	Work Package No	Lead Beneficiary	Means of Verification	Due Date (month)
				activities, skills development initiatives, and project collaborations.	

LIST OF CRITICAL RISKS

Critical risks & risk management strategy			
Grant Preparation (Critical Risks screen) — Enter the info.			
Risk number	Description	Work Package No(s)	Proposed Mitigation Measures
1	Communication issues in a project can lead to misunderstandings, delays, and decreased productivity. Common challenges include unclear instructions, lack of regular updates, and misalignment between team members. Effective communication is essential to keep every member of the project team informed, aligned, and focused on project goals. Impact: medium; Likelihood: low	WP4, WP2, WP3, WP1	To mitigate communication issues, regular meetings will be held to ensure continuous project progress. The Project Management Handbook will set procedures for the day-to-day management administration and communication, also for operational tasks. Establishing clear channels, documenting decisions, and maintaining consistent updates will keep the team aligned and reduce misunderstandings.
2	Human resources are crucial to any project, as they provide the expertise, skills, and motivation needed to move the project forward. A well-coordinated team enables effective problem-solving and maintains productivity, ensuring the project meets its goals efficiently. Impact: high; Likelihood: medium	WP4, WP2, WP3, WP1	Lack of human resources can be mitigated by prioritizing critical tasks and concentrating team efforts on areas that most impact project goals. Workloads will be redistributed to allow team members to temporarily cover not only their roles if needed. Where necessary, temporary staff/external help might be needed to relieve pressure on core team members. By regularly assessing resource needs, we will adapt as necessary to ensure key project milestones remain achievable, even with limited personnel.
3	Outreach efforts fail to engage the intended audience	WP4, WP2, WP3	The impact of project activities will be carefully assessed within the project team. A detailed

<b>Critical risks &amp; risk management strategy</b> <i>Grant Preparation (Critical Risks screen) — Enter the info.</i>			
<b>Risk number</b>	<b>Description</b>	<b>Work Package No(s)</b>	<b>Proposed Mitigation Measures</b>
	fully, resulting in reduced visibility, engagement, or influence compared to project goals. Impact: high; Likelihood: low		analysis with possible strategies to fight the unpleasant situation can be prepared. Based on the analysis, the PSC will identify and, if necessary, adopt the most effective strategy to counter the risk - whether through engaging in more suitable forums, refining communication targeting, or implementing other targeted adjustments.
4	The project may not achieve the expected quantity or quality of deliverables or KPIs initially set in its objectives. This shortfall could impact overall project success, effectiveness, or funding compliance. Impact: high; Likelihood: low	WP4, WP2, WP3	To mitigate the risk of not reaching proposed project output values (DELs, KPIs), realistic planning of the project outputs, supported by long-term measures and thorough analytical preparations before the project begins will be utilised. Throughout the project, progress will be regularly monitored to identify any shortcomings early. If needed, the resources will be reallocated, timelines adjusted, or high-impact activities to maximize output prioritized. Regular feedback loops, performance reviews, and adjustments to the project scope or methods will help ensure outputs stay aligned with objectives.
5	The risk of withdrawal of a project team member can disrupt workflow, reduce available expertise, and may delay project timelines if their role is critical and not easily filled. Impact: medium; Likelihood: medium	WP4, WP2, WP3, WP1	Project manager ensures that the project remains transparent and robust, incorporating methods of substitutability and horizontal information sharing. By cross-training team members and documenting key responsibilities, a system where others can step in seamlessly if needed will be created. Additionally, setting up conditions in a motivational and long-term way can help retain team members, reducing the likelihood of unexpected departures and promoting continuity throughout the project.
6	Activities fall behind the planned timeline, causing delays in reaching milestones or completing deliverables. This can lead to a cascading effect, impacting subsequent tasks, resource allocation, and potentially the overall project success if adjustments are not made promptly. Impact: high; Likelihood: low	WP4, WP2, WP3, WP1	To mitigate the risk, it is necessary to regularly consult the timetable and set up control mechanisms to catch delays early. Realistic project planning will ensure sufficient time and resources are allocated to each phase, reducing the chance of setbacks. With a highly experienced team in place, we can quickly address any issues that arise, adjusting resources or timelines as needed to keep the project on track. Regular check-ins and clear roles will help maintain alignment with the schedule and ensure that any minor deviations are managed promptly.
7	Consortium partner may not meet commitments or could exit unexpectedly, potentially causing disruptions, resource gaps, or delays in achieving project goals. Impact: high; Likelihood: low	WP4, WP2, WP3, WP1	Consortium members were selected based on established strategic cooperation in previous projects and activities, ensuring a foundation of reliability. Clear agreements on roles and expectations, combined with contingency plans for task redistribution or replacement partners, will provide flexibility and ensure the project continues smoothly despite any hanges.

<b>Critical risks &amp; risk management strategy</b> <i>Grant Preparation (Critical Risks screen) — Enter the info.</i>			
<b>Risk number</b>	<b>Description</b>	<b>Work Package No(s)</b>	<b>Proposed Mitigation Measures</b>
8	Potentially caused by underestimated costs, unexpected price increases, or additional resource needs. This risk can be heightened by inflation or fluctuations in the CZK currency ratio, which may increase expenses beyond the initial projections, impacting the ability to cover ongoing or future project activities and threatening project completion or quality if not managed effectively. Impact: high; Likelihood: medium	WP4, WP2, WP3, WP1	We will focus on realistic planning for cost setting and spending, backed by the Consortium agreement, and ensure thorough financial coordination. Economic conditions will be regularly monitored and the budget will be adjusted as needed. Fixed-price contracts will be used where possible to limit exposure to cost increases, and periodic budget reviews will allow us to catch any overspending early, keeping the project financially stable.
9	Potential applicants may overlook or deprioritize the project's open calls due to other funding options on the national level. This could result in fewer applications, reducing the diversity and/or quality of participants and impacting the project's outreach and objectives. Impact: high; Likelihood: medium	WP3	The focus will be on identifying areas and topics not already supported by other national programs. By emphasizing the project's added value - such as cross-border collaboration and international visibility - we can distinguish it from other funding providers. Targeted outreach, partnerships, and informational sessions will further highlight how this funding complements, rather than duplicates, existing opportunities, effectively engaging a broader audience.
10	Engagement on the national level is crucial for the success of the project. The lack of involvement of relevant entities in the NCC-CZ activities, including the lack of interest of national entities in joining the European Cybersecurity Competence Community might undermine the NCC-CZ's ability to carry out the assigned tasks. Impact: medium; Likelihood: medium	WP4, WP2, WP3	A Communication and Dissemination Strategy will be developed at the beginning of the project to specify target audience and channels to mitigate this risk. Furthermore, regular stakeholder workshops and clear communication channels will be established to keep members informed and involved. Customized engagement plans and incentives can further motivate participation, while feedback mechanisms ensure that members' input is valued. To further motivate entities to join the Competence Community, the NCC Network and ECCC must work together to identify and share the benefits.

PROJECT REVIEWS

Project Reviews			
Grant Preparation (Reviews screen) — Enter the info.			
Review No	Timing (month)	Location	Comments
RV1	18	TBD	Mid-term review
RV2	36	TBD	Mid-term review
RV3	48	TBD	Final review



## ANNEX 1



# Digital Europe Programme (DIGITAL)

## Description of the action (DoA)

### Part B



**DESCRIPTION OF THE ACTION (PART B)**

<b>HISTORY OF CHANGES</b>		
<b>Date</b>	<b>Page/section</b>	<b>Nature of change and reason / justification of change proposed (if applicable)</b>
3.4.2025	DoA Part A - WP3: Financial Support for Strengthening Cybersecurity Capabilities	The launch of the work package activities and duration has changed due to comments from the evaluation (inconsistency with the Gantt chart). Activities (FSTP) will start with the beginning of Q2 2026. The individual tasks of the work packages will be implemented in continuity and, with the exception of WP3, will be implemented throughout the duration of the project.
4.4.2025	DoA PartA - WP3: Financial Support for Strengthening Cybersecurity Capabilities	On the basis of the recommendations, the description for work package 3 was further refined regarding the targeting of the upcoming Calls in terms of the setting of the KPIS and the targeting of individual EU policies and strategies. ("Each FSTP call will clearly define which EU/CZ policies will the supported project contribute to, including specific and measurable KPIs to be achieved in individual projects (number of entities/products aligned/in compliance with EU/CZ regulatory requirements or strategies; number of actions to support SMEs and/or public institutions to implement innovative and state of the art cybersecurity solutions into their operations, measurable improvement in cybersecurity posture in supported entities, etc. The specific focus of the upcoming Calls will thus address the current security situation as well as developments within the national and European context.")
4.4.2025	DoA part B - 2.2 Implementation plan and efficient use of resources	Following a request for clarification in the evaluation, an explanation for the person-month volume in some of the work packages has been added to section 2.2.
4.4.2025	DoA part B - 2.1 Maturity	According to the results of the evaluation, the formulation for the evaluation process was refined using the experience from the first FSTP Calls (implementation of the NCC-CZ project).
4.4.2025	DoA part B - 2.2 Implementation plan and efficient use of resources	According to the recommendations of the evaluation, a passage on the preparation of an internal analytical study was added to WP2 to help refine and target the implementation of awareness raising campaigns.
4.4.2025	DoA part B - 3.1 Expected outcomes and deliverables	On the basis of the recommendations, a partial refinement of the indicators in terms of target groups was added, taking into account SMEs.
15.4.2025	4.2 Work packages, activities, resources and timing	Purchase and equipment tables have been added and an explanation has been added to the Other cost (FSTP scheme) table
15.4.2025	DoA PartA - Milestones	The milestones for the overall project implementation period (48 months) were reviewed. Milestone descriptions (Means of Verification) have been added.
15.4.2025	DoA PartA - WPs	The information in the proposal has been transferred to the Work Package Description area.
15.4.2025	DoA PartA - Deliverables	Information regarding the type of document and the language of the deliverables has been added to the description.



15.4.2025	DoA part B – Section 1.1	Information on measurable key performance indicators (KPIs) has been added.
15.4.2025	DoA part B – Section 1.2	Information was added on how the implementation of the project activities will contribute at EU level to long-term EU policies and strategies.
29.4.2025	DoA Part A – Work Packages	A more detailed description of work packages has been added.
29.4.2025	DoA Part A – Critical risks	Likelihood and impact were added for each identified critical risk.
29.4.2025	DoA Part A - Deliverables	Additional deliverables (evaluation reports) have been added to define and refine the topics and agenda of planned Calls and to incorporate feedback from previous Calls.
29.4.2025	DoA Part B – Section 1.1	Key performance indicators have been added to the objectives table.



**TABLE OF CONTENTS**

<b>ANNEX 1 .....</b>	<b>1</b>
<b>DESCRIPTION OF THE ACTION (PART B) .....</b>	<b>2</b>
<b>1. RELEVANCE .....</b>	<b>5</b>
1.1 Objectives and activities.....	5
1.2 Contribution to long-term policy objectives, policies and strategies — Synergies .....	7
1.3 Digital technology supply chain .....	9
1.4 Financial obstacles .....	9
<b>2. IMPLEMENTATION .....</b>	<b>9</b>
2.1 Maturity .....	9
2.2 Implementation plan and efficient use of resources .....	10
2.3 Capacity to carry out the proposed work .....	14
<b>3. IMPACT .....</b>	<b>21</b>
3.1 Expected outcomes and deliverables — Dissemination and communication .....	21
3.2 Competitiveness and benefits for society .....	25
3.3 Environmental sustainability and contribution to European Green Deal goals .....	25
<b>4. WORK PLAN, WORK PACKAGES, ACTIVITIES, RESOURCES AND TIMING .....</b>	<b>26</b>
4.1 Work plan .....	26
4.2 Work packages, activities, resources and timing .....	27
<i>Work Package 1</i> .....	27
<i>Work Package 2</i> .....	28
<i>Work Package 3</i> .....	29
<i>Work Package 4</i> .....	30
<i>Purchases and equipment</i> .....	31
<i>Other cost categories</i> .....	32
<i>Timetable</i> .....	34
<b>5. OTHER .....</b>	<b>36</b>
5.1 Ethics .....	36
5.2 Security .....	36
<b>6. DECLARATIONS .....</b>	<b>36</b>

#@APP-FORM-DEP@#

#@PRJ-SUM-PS@# [This document is tagged. Do not delete the tags; they are needed for the processing.]



## 1. RELEVANCE

### 1.1 Objectives and activities

#### Objectives and activities

*Describe how the project is aligned with the objectives and activities as described in the Call document.*

*How does the project address the general objectives and themes and priorities of the call? What is the project's contribution to the overall Digital Europe Programme objectives?*

This project aims to **facilitate the fulfilment of the tasks assigned to the National Coordination Centres (NCCs)** under *Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*. The Czech Republic's National Coordination Centre (NCC-CZ) consortium, led by the primary beneficiary and project coordinator — the National Cyber and Information Security Agency (NUKIB) - in collaboration with its affiliated entity, CyberSecurity Hub (CSH), is fully dedicated to meeting the objectives outlined in Regulation (EU) 2021/887 while being in line with the objectives and activities described in the Call document.

The National Coordination Centre 2.0 – The Czech Republic (NCC-CZ 2.0) project is designed to ensure the **sustainable operation of NCC-CZ**, thereby reinforcing Union's digital sovereignty and fostering a secure, resilient, and interconnected digital landscape. Through enhancing NCC-CZ's capacity, the project will enable the NCC to effectively serve as the main national point of contact for the community while engaging actively within the broader NCC Network to strengthen cybersecurity capabilities across Europe. This will directly contribute to building and advancing the European Cybersecurity Competence Community. In alignment with EU legislation and policies, NCC-CZ will play a vital role in supporting the cybersecurity community, with a focus on small and medium-sized enterprises (SMEs), to adopt and leverage advanced and innovative cybersecurity solutions.

A key element of this project is to provide **financial support to third parties (FSTP)**, fostering the adoption and use of state-of-the-art cybersecurity solutions. This funding will equip organizations with the latest cybersecurity tools and strategies, significantly boosting their resilience and readiness to tackle evolving cyber threats. These efforts will be harmonized with other NCC-CZ activities, including acting as a central national point for cybersecurity coordination, promoting cross-border project participation, and establishing links with ECCC and related European initiatives such as the European Digital Innovation Hubs (EDIHs).

This project directly **supports the objectives of the Digital Europe Programme (DEP)**, with a primary focus on one of its five key capacity areas: cybersecurity. Additional connections to other capacity areas, such as advanced digital skills, are anticipated through various projects and initiatives led by NCC-CZ and its partner institutions.

The **activities of the NCC-CZ 2.0 project are deeply intertwined with the strategic objectives and scope outlined in the Call document**. Both share a commitment to enhancing cybersecurity capacities, fostering community engagement, and supporting the adoption of advanced cybersecurity solutions across diverse stakeholders. By integrating effective project management (WP 1), targeted financial support (WP 3), community building (WP 4), and awareness-raising initiatives (WP 2), NCC-CZ 2.0 directly aligns with the call's mission. This strong synergy ensures that the project not only contributes to the EU's strategic goals in cybersecurity but also effectively addresses the call's priorities. The table below provides an overview of how the NCC-CZ 2.0 project aligns with the set objectives and specifies the WPs relevant for each area.

These objectives will be achieved through actions planned in individual WPs and measured through following KPIs identified in section 3.1:

- Number of awareness-raising, capacity building and training events organized and/or attended: 60
- Number of stakeholders reached through events: 250
- Number of stakeholders engaged through awareness campaigns: 1 000
- Number of Technology Open Days organised: 8
- Number of awareness-raising and capacity building webinars organised: 16
- Number of supported projects aligned with EU and Czech cybersecurity priorities: 25
- Number of entities benefiting from FSTP cascade financing: 25
- Number of entities provided with information and technical support related to funding opportunities: 50
- Number of webinars focused on FSTP calls and project development: 8



- Number of community members engaged: 270
- Number of actions to foster expertise and synergies within the community: 50
- Number of collaborative actions with NCCs and ECCC: 30
- Number of reusable resources shared in the public repository: 30
- Number of organised community meetings: 8
- Number of activities aimed at the promotion of membership in EU Cybersecurity Competence Community: 5

Objectives and Scope of the Call Document	Relevant Work Packages	Key performance indicator (KPIs)
foster the Cybersecurity Competence Community	WP2, WP4	number of actions to foster expertise and synergies within the community: 50
support priority areas such as the implementation of EU legislation (Directive 2022/2555, CRA, CSA)	WP2, WP3, WP4	number of supported projects aligned with EU and Czech cybersecurity priorities: 25
support the operation of the NCCs and enable them to support the cybersecurity community, including SMEs, for the uptake and dissemination of state-of-the-art cybersecurity solutions and strengthen cybersecurity capacities.	WP2, WP3, WP4	number of stakeholders engaged through awareness campaigns: 1 000 number of Technology Open Days organised: 8
acting as contact points at the national level for the Cybersecurity Competence Community to support the ECCC in achieving its objectives and missions;	WP2, WP4	number of awareness-raising, capacity building and training events organized and/or attended: 60
providing expertise and actively contributing to the strategic tasks of the ECCC, taking into account relevant national and regional challenges for cybersecurity in different sectors;	WP4	number of reusable resources shared in the public repository: 30
promoting, encouraging, and facilitating the participation of civil society, industry in particular start-ups and SMEs, academic and research communities, and other actors at Member State level in cross-border projects and cybersecurity actions funded through all relevant Union programmes;	WP3, WP4	number of entities provided with information and technical support related to funding opportunities: 50
providing technical assistance to stakeholders by supporting the stakeholders in their application phase for projects managed by the ECCC, and in full compliance with the rules of sound financial management, especially on conflict of interests. This should be done in	WP4	number of collaborative actions with NCCs and ECCC: 30



close coordination with relevant NCPs set up by Member States;		
seeking to establish synergies with relevant activities at national, regional, and local levels, such as addressing cybersecurity in national policies on research, development, and innovation in the area of, and in particular in those policies stated in the national cybersecurity strategies;	WP2, WP3, WP4	number of organised community meetings: 8
where relevant, implementing specific actions for which grants have been awarded by the ECCC, including through provision of financial support to third parties in line with Article 204 of Regulation (EU, Euratom) 2018/1046 under the conditions specified in the grant agreements concerned; such support should in particular aim at strengthening the uptake and dissemination of state-of-the-art cybersecurity solutions (notably by SMEs);	WP3	number of entities benefiting from FSTP cascade financing: 25 number of webinars focused on FSTP calls and project development: 8
promoting and disseminating the relevant outcomes of the work of the Network and the ECCC at national, regional, or local level;	WP2, WP4	number of activities aimed at the promotion of membership in EU Cybersecurity Competence Community: 5
assessing requests for becoming part of the Cybersecurity Competence Community by entities established in the same Member State as the NCC;	WP4	number of community members engaged: 270
advocating and promoting involvement by relevant entities in the activities arising from the ECCC, the Network of National Coordination Centres, and the Cybersecurity Competence Community, and monitoring, as appropriate, the level of engagement with actions awarded for cybersecurity research, developments, and deployments.	WP2, WP3, WP4	number of awareness-raising and capacity building webinars organised: 16 number of stakeholders reached through events: 250

#@COM-PL-CP@#

## 1.2 Contribution to long-term policy objectives, policies and strategies — Synergies

### Contribution to long-term policy objectives, policies and strategies — Synergies

*Describe how the project contributes to long-term policy objectives of the call's domain/area and to the relevant policies and strategies, and how it is based on a sound needs analysis in line with the activities at European and national level.*

*What challenge does the project aim to address?*

*The objectives should be specific, measurable, achievable, relevant and time-bound within the duration of the project.*



The growing reliance on digital technologies and the escalating need to address cybersecurity threats highlight the importance of close cooperation within the European Union (EU). On the **European level**, this project aligns with the policy objectives of the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC), as outlined in Article 4 of Regulation 2021/887. It does so by prioritizing and supporting initiatives aimed at strengthening cybersecurity capacities, capabilities, and knowledge, particularly for SMEs, the research and academic community, the public sector, and civil society. The project also aligns with key Union policy objectives, including **the EU's Cybersecurity Strategy for the Digital Decade** and its considerable investment plans in cybersecurity. Through the ECCC and the Network of NCCs, the EU aims to direct up to €4.5 billion in public and private investments (via Digital Europe Program and Horizon Europe, as well as the Recovery Plan for Europe) over 2021-2027. As part of the NCC-CZ 2.0 project, the participation of Czech entities in EU funding programs will be supported, along with the provision of FSTP in relevant areas. **The Cybersecurity Skills Academy**, supported by the ECCC, NCCs, and EU funding, will address critical cybersecurity skill gaps by better aligning financial resources with identified needs. The NCC-CZ 2.0 project will support training activities, foster skills development, address the skills shortage, promote skills-sharing initiatives, and raise awareness in related areas.

Moreover, the project aims to address challenges identified in EU legislation, including **the Cyber Solidarity Act**, by supporting national efforts for the establishment of a National Cyber Hub and coordinating with the ECCC, given the crucial role of the Competence Centre in the process of launching the procedure for the acquisition of the tools, infrastructure, and services. The NCC-CZ will disseminate information on open calls, provide methodological support in application phase, leverage its involvement in the ECCC Working Group on Cyber Hubs and ensure connections with other NCCs/EU Member States. Apart from the European Cybersecurity Alert System, the ECCC will play a key role in implementing the **Cybersecurity Emergency Mechanism**. Therefore, this project contributes to creating a strong European cybersecurity ecosystem, mostly by supporting Czech expert community and its involvement in related initiatives and activities. The project also aims to **contribute to the implementation of key EU legislation**, including NIS2, the Cybersecurity Act (CSA), and the Cyber Resilience Act (CRA), by providing support to entities with the implementation in various ways, for example through providing FSTP, organizing knowledge-sharing activities, sharing best practices and providing up-to-date information on developments on the EU level. The project also aims to enhance cybersecurity skills by supporting awareness-raising and training activities for targeted stakeholders in relevant areas from the Regulation.

At the **national level**, capacity building and raising cybersecurity awareness are key priorities outlined in the **National Cyber Security Strategy of the Czech Republic for 2021-2025**, published by NUKIB. The establishment of a fully functional NCC in the Czech Republic is also identified as a primary goal in the **National Plan for Research and Development in Cyber and Information Security for 2022-2025**. This Plan emphasizes fostering an expert community that includes public administration bodies, academic and research institutions, and industry actors within the security sector. It further supports providing information on EU cybersecurity priorities and programs at the national level and promotes cybersecurity education programs. This project contributes directly to the long-term policy objectives within this domain by enhancing NUKIB's ongoing efforts to support the Czech cybersecurity community. These efforts include sharing information from national and EU levels, organizing regular expert meetings of the **Cyber Research and Innovations in Security (CYRIS) group**, previously known as *Platform for Research and Development in Cyber and Information Security*, and encouraging engagement in national and cross-border projects.

The consortium leverages the complementarity between the CyberSecurity Hub (CSH), a partner in the NCC-CZ 2.0 project, and its role as the coordinator of the **Cybersecurity Innovation Hub (CIH) and European Digital Innovation Hub (EDIH)**. As part of the EDIH network, CIH provides extensive expertise and resources for fostering innovation and collaboration in cybersecurity. This dual role enables the consortium to integrate insights and best practices from the EDIH network into NCC-CZ activities, enhancing synergies between national and EU-level initiatives and aligning with long-term EU cybersecurity objectives. This collaboration supports not only the development of advanced cybersecurity solutions but also the widespread adoption of such technologies, particularly among SMEs, public sector organisations and other relevant stakeholders.

The project specifically aims to contribute to long term EU policies and strategies related to cybersecurity by supporting

- strengthening of the ECCC's goals by boosting the cybersecurity capacity of SMEs, academia, and public entities in line with Regulation (EU) 2021/887.
- supporting of the EU Cybersecurity Strategy by driving adoption of advanced cyber solutions, enhancing digital resilience, and improving coordination across Member States.




- aiding in implementing key EU legislation (NIS2, CRA, CSA, Cyber Solidarity Act) through awareness campaigns, financial support, and tailored guidance for compliance.
- advancing the cross-border collaboration by forging partnerships with other NCCs and promoting joint research, innovation, and knowledge-sharing.
- addressing the cybersecurity skills gap by delivering training, workshops, and webinars aligned with EU-level initiatives like the Cybersecurity Skills Academy.
- leveraging the available EU funds (e.g., Digital Europe Programme, Horizon Europe) to strengthen market-ready cybersecurity products and services by promoting participation of stakeholders in relevant calls
- fostering the EU strategic autonomy by helping SMEs deploy cutting-edge cybersecurity technologies and reinforcing pan-European expertise.

#§COM-PLE-CP§#

### 1.3 Digital technology supply chain

#### Digital technology supply chain

*Explain to what extent the project would reinforce and secure the digital technology supply chain in the EU.*


 This criterion might not be applicable to all topics — for details refer to the Call document.

Not applicable as stated in the call document.

### 1.4 Financial obstacles

#### Financial obstacles

*Describe to what extent the project can overcome financial obstacles such as the lack of market finance.*

 This criterion might not be applicable to all topics — for details refer to the Call document.

Not applicable as stated in the Call document.

#§PRJ-OBJ-PO§# #§REL-EVA-RE§# #@QUA-LIT-QL@# #@MAT-URI-MU@#

## 2. IMPLEMENTATION

### 2.1 Maturity

#### Maturity

*Explain the maturity of the project, i.e. the state of preparation and the readiness to start the implementation of the proposed activities.*

The collaboration between NUKIB and CSH to establish and ensure the functioning of the NCC in the Czech Republic was officially initiated with the signing of a **memorandum of cooperation** in December 2021. Since November 2022, the NCC-CZ consortium has been recognized by the European Commission as having the necessary **capacity to manage funds**. This recognition underscores NCC-CZ's readiness and commitment to executing its responsibilities. The NCC-CZ is now operational and actively fulfilling its tasks in accordance with EU Regulation 2021/887.

The NCC-CZ 2.0 project is well prepared for implementation. NCC-CZ is a strong consortium that has well developed cooperation with established routine of regular meetings to coordinate the NCC-CZ's responsibilities and activities. Currently, mechanisms are in place to support effective and efficient NCC-CZ 2.0 project operations, with a comprehensive range of departments within NUKIB actively engaged in partnership with CSH. A multidisciplinary **expert project team**, leveraging the project experience from





both NUKIB and CSH, is fully operational, providing essential support across the legal, financial, and administrative aspects critical to NCC-CZ 2.0's project.

The **collaboration between NUKIB and CSH** on two ongoing projects, *National Coordination Centre in the Czech Republic* (NCC-CZ, project number: 101127941) and *Building Testing and Certification Capabilities in the Czech Republic* (TEST-CERT-CZ, project number: 101127940), has been very successful. Both organizations bring together experts who work cohesively to ensure that project objectives are met efficiently and effectively. The expertise from both NUKIB and CSH teams has facilitated smooth progress, enabling all project deliverables to be submitted on time and in full compliance with the required standards\*. This well-functioning collaboration is pivotal for the NCC-CZ 2.0 project, which builds on the insights, outputs and experiences gained from the first NCC-CZ project and provides a solid foundation for NCC-CZ 2.0, where refined processes and lessons learned will be crucial to achieving even more ambitious goals. Leveraging the established partnership, both organizations are prepared to enhance and expand the impact of NCC-CZ, ensuring that the NCC-CZ project's second phase advances with the same precision and commitment that have characterized their work on NCC-CZ and TEST-CERT-CZ.

The NCC-CZ 2.0 project will build upon the newly established **FSTP mechanism**, that was tested and proven functional, leading to the launch of the first NCC-CZ call. This experience has generated valuable and needed expertise which will be key in securing FSTP activities in the proposed project. Lessons learned, particularly in managing applications, evaluation process, and funds allocation, will be instrumental in driving future project success.

Based on the experience from the capacity building of the FSTP and the implementation of the first Calls, the Calls under the FSTP will take more account of quantitative evaluation measures (higher degree of objectivity of the evaluation). A pool of external expert evaluators has been secured under the NCC-CZ project and can be used for the Calls under the NCC-CZ 2.0. Evaluators will be trained on the criteria and focus for each Call and on the use of quantitative scales. Within the NCC-CZ, an expert platform has been created for the second stage evaluation (NCC-CZ Council), individual council rapporteurs will prepare the second stage evaluation and in the third stage one of each application is discussed by the NCC-CZ Council and competitively evaluated.

**NCC-CZ's active engagement in the activities of the NCC Network and ECCC** will be utilised in the project, collaborating closely with other NCCs and maintaining strong connections with partners from other EU Member States. NCC-CZ also actively participates in European-level initiatives, providing inputs, suggestions, and feedback, and is involved in meetings and the work of various working groups on the ECCC level.

To conclude, the NCC-CZ consortium's readiness for NCC-CZ 2.0 project implementation can be demonstrated by the following key factors:

- **Organizational readiness:** Building on prior projects that successfully established NCC-CZ's operational structure, the consortium has implemented essential processes and roles needed for smooth cooperation and implementation in line with project management best practices and contractual requirements.
- **FSTP competence:** Key processes for launching calls, administering submitted applications, and managing related financial operations are established, with a commitment to incorporate lessons learned and continuously refine these processes.
- **National and European ecosystem integration:** NCC-CZ is already embedded within the national cybersecurity ecosystem, having established cooperation with key stakeholders, including EDIH, National Contact Points (NCPs) for the Digital Europe and Horizon Europe programmes, and other national-level partners. NCC-CZ maintains close connections with representatives of the national cybersecurity community and actively collaborates within the NCC Network and with the ECCC, demonstrating its functionality and integration at both the European and national levels.

\*Accurate as of the time of project application submission.

#\$MAT-URI-MU\$# #@\$CON-MET-CM@\$# #@\$PRJ-MGT-PM@\$# #@\$FIN-MGT-FM@\$# #@\$RSK-MGT-RM@\$#

## 2.2 Implementation plan and efficient use of resources

### Implementation plan

Show that the implementation work plan is sound by explaining the rationale behind the proposed work packages and how they contribute to achieve the objectives of the project.

Explain the coherence between the objectives, activities, planned resources and project management processes.

Show how the project integrates, builds on and follows up on any pre-existing work or EU funded projects. Provide details (including architecture and deliverables) about pre-existing technical solutions.

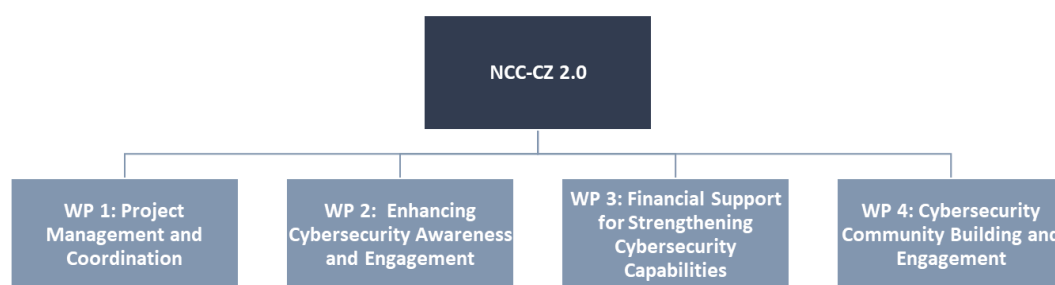


The **NCC-CZ 2.0 implementation plan** is designed to ensure that each work package (WP) is strategically aligned with the project's objectives, creating a coherent and interconnected structure to achieve the expected outcomes. Each WP includes clearly defined, measurable activities that directly support the project's goals, underpinned by a robust management framework to ensure effective oversight, efficient resource allocation, and proactive risk mitigation.

**Awareness-raising activities** help identify needs and engage stakeholders, preparing them to leverage project opportunities. These efforts are complemented by **FSTP mechanism**, which address identified needs and drive innovation and capacity building, particularly among SMEs but also other stakeholders.

**Community-building initiatives** further enhance collaboration, knowledge-sharing, and cross-border synergies, creating a dynamic and integrated approach that amplifies the project's overall impact and strengthens cybersecurity resilience.

The **structure of the WPs** is illustrated in the graph below, with each WP explained in greater detail.



The objective of **WP 1: Project Management and Coordination** is to ensure the efficient execution of NCC-CZ 2.0 project through robust coordination, monitoring, financial oversight, and risk management. Key tasks include facilitating project team and consortium meetings to align strategies and ensure effective communication, tracking progress against objectives and deliverables, managing financial resources with transparency, and proactively addressing risks with mitigation strategies. These activities ensure smooth project execution and alignment with strategic goals.

**WP 2: Enhancing Cybersecurity Awareness and Engagement** aims to identify and address gaps in cybersecurity awareness, education, and R&D to strengthen the overall cybersecurity ecosystem. Building on insights from the initial NCC-CZ project, this WP targets key stakeholders, including SMEs, academic and research institutions, public organizations, and NGOs, through tailored awareness-raising activities and outreach efforts. It aims to enhance visibility and engagement by leveraging proven dissemination strategies, social media, and digital platforms. Additionally, it supports collaboration within the cybersecurity community by fostering synergies between national and EU initiatives, providing guidance on EU funding opportunities, and promoting the development of joint projects. This WP also emphasizes skills development and community engagement to address the cybersecurity talent shortage and ensure sustainable impact. Q2-Q3 2026 will include an internal study and strategy for the appropriate implementation of awareness raising campaigns (focus on current ECCC/NKC activities, content of FSTP calls, information on funding sources, general information on the cybersecurity environment, matchmaking and brokerage events of relevant institutions in the Czech national pool, etc.).

**WP 3: Financial Support for Strengthening Cybersecurity Capabilities** focuses on enhancing and implementing the NCC-CZ FSTP mechanism to support high-impact projects that strengthen cybersecurity resilience and align with EU and national priorities. This WP builds on the lessons learned from previous NCC-CZ FSTP calls to refine processes for application, evaluation, and monitoring, ensuring efficiency, transparency, and maximum impact. It includes conducting continuous needs assessments to adapt funding priorities to emerging challenges and technological advancements. Over the course of the project, three strategic calls for proposals will be launched, targeting primarily SMEs, but potentially also NGOs, academic and research institutions, and other stakeholders. The funding will support innovative solutions, the adoption of advanced cybersecurity technologies, and the development of governance frameworks, contributing to societal resilience and the EU's goals of digital sovereignty and strategic autonomy.

**WP 4: Cybersecurity Community Building and Engagement** focuses on developing a robust, collaborative cybersecurity ecosystem that enhances the capacity of diverse stakeholders, including SMEs, academic institutions, public administration, and NGOs. This work package emphasizes growing and managing the cybersecurity community by fostering collaboration, facilitating knowledge exchange, and promoting active engagement. It includes structured processes for managing EU Cybersecurity





Competence Community memberships, aligning national efforts with EU initiatives, providing support to the ECCC and strengthening cross-border collaboration within the NCC Network. WP 4 also prioritizes organizing and participating in workshops, webinars, and conferences to address emerging cybersecurity challenges, share best practices, and build synergies. Additionally, it aims to create a repository of reusable educational materials, tools and other documents to amplify the community's impact. These efforts align with NCC-CZ and ECCC objectives to enhance cybersecurity resilience and support the EU's strategic autonomy.

Also, the NCC-CZ 2.0 project builds upon **existing knowledge and outcomes** developed during the initial Digital Europe Programme (DEP) funded project NCC-CZ, which began in November 2023. It will also build upon the internal mechanisms and external partnerships developed not only during the NCC-CZ project, but also during the TEST-CERT-CZ project, ensuring that foundational work is maximized rather than duplicated. The experience gained from previous projects, particularly within the FSTP framework, is fully utilized and integrated into the current project scope, reducing initial set-up times, accelerating the achievement of key milestones and supporting innovative objectives. Deliverables from prior projects provide a solid baseline, allowing the project team to focus on innovative aspects and advanced functionalities that push the project beyond its starting point. This structure demonstrates both a clear connection between objectives and actions and a sound, evidence-based rationale for the chosen approach.

The transition between projects will also serve as an opportunity to **enhance processes and incorporate lessons learned**. NCC-CZ launched its operations with a strong foundation, as an organization with established structures and a clearly defined mandate to carry out tasks as laid out in Regulation (EU) 2021/887. Carrying out the NCC-CZ project funded under the DEP posed initial challenges that required additional organizational measures. However, the team already included skilled personnel, and the project received strong support from NCC-CZ's top management. These favourable preconditions, along with the effective project implementation, led to the development and operation of comprehensive structures covering all areas of project management - from task planning and coordination to quality control, financial management, and reporting. Additionally, NCC-CZ has positioned itself as a recognized leader in the Czech cybersecurity community, building strong connections with government institutions, businesses, and academia.

Based on the experience from the implementation of the NCC-CZ project, which built capacity for the FSTP as a completely new grant scheme in the Czech Republic, a significant administrative complexity and the need to strengthen the staff capacity of the implementation team, especially for the economic, legal and administrative areas, was identified. In order to ensure the high volume of activities in the WP2 area, there is also an increase in the necessary volume of person-months. In order to increase the outreach and impact, special equipment will be procured under WP2 (e.g. registration equipment for CYRIS events), but always within the 3E principle.

### Project management, quality assurance and monitoring and evaluation strategy

*Describe the measures planned to ensure that the project implementation is of high quality and completed in time.*

*Describe the methods to ensure good quality of monitoring, planning and control activities.*

*Describe the evaluation methods and indicators (quantitative and qualitative) to monitor and verify the outreach and coverage of the activities and results. The indicators proposed to measure progress should be specific, measurable, achievable, relevant and time-bound.*

**Operational procedures** will be established at the project's outset to ensure effective and efficient implementation and reporting, fully aligned with the contractual framework and best management practices. Therefore, to ensure high-quality and timely project implementation, a robust framework for monitoring, planning, and control activities will be established. These procedures will be further elaborated in the Project Management Handbook, building on the established processes already implemented successfully within the NCC-CZ consortium in the NCC-CZ and TEST-CERT-CZ projects. Drawing from this proven framework, with adjustments as needed, the Handbook will provide a detailed guide to ensure consistency and quality across all aspects of project implementation. A dedicated project team will oversee all stages of the project, using set procedures to track progress and address issues proactively. Regular project progress reviews and milestone assessments will be conducted to keep the project on schedule and maintain quality standards.

**Consortium management:** To ensure effective consortium collaboration, a clear communication framework will be established, facilitating seamless information flow between both partners. Regular meetings between NUKIB and CSH (whose representatives together form the General Assembly) will be held to review progress, address challenges, and align on strategic decisions. The Project Coordinator, supported by Work Package Leaders (WPLs), will oversee task distribution and ensure that all partners



adhere to agreed timelines and quality standards. This approach will promote transparency, accountability, and efficiency across the consortium, fostering a collaborative environment that is responsive to project needs and objectives.

**Project team management:** The NCC-CZ 2.0 project will be managed in line with the project work plan, ensuring that all requirements for reporting, information sharing, and compliance are met. Work Package Leaders (WPLs) will be responsible for tasks within each WP, while the coordinator, supported by the Project Steering Committee (PSC) composed of all WPLs and project team members, will oversee quality assurance management. The PSC will meet regularly to track the project progress and ensure that all deliverables meet required standards for conformity and quality. Key performance indicators (KPIs) will be reviewed and analysed regularly to ensure the project stays on course.


To monitor and verify the outreach and impact of the planned project activities, a set of both quantitative and qualitative indicators will be developed. **Quantitative indicators**, such as the number of projects submitted and supported, number of stakeholders impacted, number of events organised or attended, number of participants engaged, survey response rates, number of social media posts and engagements, number of newsletters and number of newsletter subscribers, will track the scale of impact and engagement. These metrics will provide concrete data on the dissemination and impact of the NCC-CZ activities. **Qualitative indicators** will for example assess participant satisfaction, feedback on project activities and expert feedback. All indicators shall be specific, measurable, achievable, relevant, and time-bound (SMART), enabling the project team to monitor progress effectively and make data-driven adjustments as needed to meet project goals and maximize results.

The **indicators (KPIs)** established in the NCC-CZ 2.0 project are further detailed in Section 3.1 "Expected Outcomes and Deliverables - Dissemination and Communication."

#### Cost effectiveness and financial management *(n/a for prefixed Lump Sum Grants)*

*Describe the measures adopted to ensure that the proposed results and objectives will be achieved in the most cost-effective way.*

*Indicate the arrangements adopted for the financial management of the project and, in particular, how the financial resources will be allocated and managed within the consortium.*

 **Do NOT compare and justify the costs of each work package, but summarize briefly why your budget is cost effective.**

**Consortium resources management:** NUKIB, in the role of a project coordinator, will manage the distribution of funds to partners in alignment with the Grant Agreement (GeA) and Consortium Agreement (CA), also addressing any incorrect, inappropriate, or unauthorized adjustments throughout the project. Key figures comparing planned and actual results, efforts, and costs per WP and partner will be internally reported regularly, both within the PSC and GeA meetings. This internal reporting will serve as a foundation for preparing periodic reports.

**Financial manager role:** In order to ensure that the proposed results and objectives are achieved in the most cost-effective way, a dedicated position of Financial Manager within the project team is planned. The NCC-CZ 2.0 financial manager will oversee the flow of financial resources, approve financial operations, and monitor budget expenditures to ensure alignment with the project's financial plan. The financial manager will be responsible for ensuring that funds are allocated and utilized effectively across the consortium, mitigating risks of overspending or under-utilization. Additionally, the financial manager will conduct regular financial reporting, coordinate audits as required and facilitate transparent communication between consortium members regarding financial matters. This structured financial oversight will support the smooth operation of the project, allowing each partner to manage their resources efficiently and contributing to the successful achievement of project objectives. Regular communication between both consortium partners is expected, the affiliated entity will provide all of the needed information to the project coordinator. All financial operations will adhere to national legislation and follow the internal processes and standards of NUKIB.

**Cost-effective measures:** To ensure that the proposed results and objectives are achieved in the most cost-effective way, the project employs budget planning and resource allocation practices. Each activity has been evaluated to optimize costs without compromising quality, focusing on efficient use of resources. Cost-sharing measures among consortium partners, combined with using existing infrastructure and expertise, reduce the need for additional expenses. Regular financial monitoring and adjustments ensure that spending remains aligned with project goals. The NCC-CZ 2.0's proposed budget is cost-effective as it prioritizes essential activities, streamlines operational costs, and maximizes impact through resource management.

2.3 Capacity to carry out the proposed work

**Consortium cooperation and division of roles (if applicable)**

*Describe the participants (Beneficiaries, Affiliated Entities and Associated Partners, if any) and explain how they will work together to implement the project. How will they bring together the necessary expertise? How will they complement each other?*

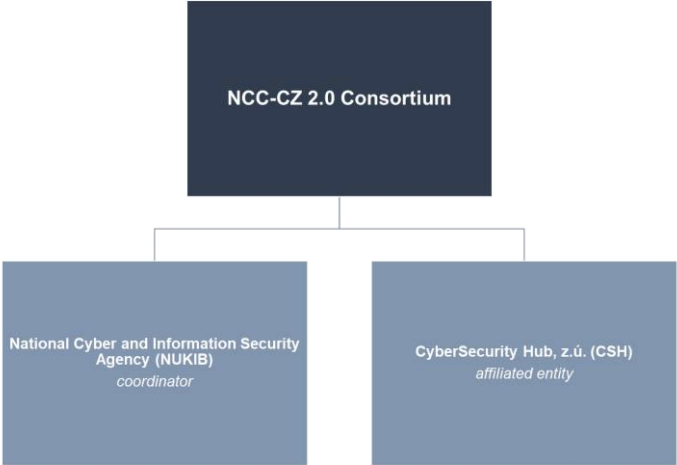
*In what way does each of the participants contribute to the project? Show that each has a valid role and adequate resources to fulfil that role.*

**Note:** When building your consortium you should think of organisations that can help you reach objectives and solve problems.

The tasks of the NCC-CZ are carried out by a **consortium** consisting of NÚKIB acting as the project coordinator and CSH in the role of an affiliated entity. As already mentioned, the cooperation was commenced by signing of the memorandum of cooperation in December 2021. NUKIB and CSH closely cooperates within the established mechanisms (GeA, PSC) and meets regularly. Together, the NCC-CZ consortium has been recognised by the European Commission as having the necessary capacity to manage funds.

The chart below illustrates the **structure of the NCC-CZ 2.0 consortium**, consisting of two key entities:

- **National Cyber and Information Security Agency (NUKIB)** - identified as the coordinator of the consortium.
- **CyberSecurity Hub, z.ú. (CSH)** - labeled as an affiliated entity.



```
graph TD; A[NCC-CZ 2.0 Consortium] --> B[National Cyber and Information Security Agency (NUKIB) coordinator]; A --> C[CyberSecurity Hub, z.ú. (CSH) affiliated entity];
```

**NUKIB** is the central administrative body in the Czech Republic for cyber security, including the protection of classified information in information and communication systems and cryptographic protection. NUKIB acts as the main entity regarding the communication with EU and ECCC including the representation of the Czech Republic in the ECCC Governing Board. Within NUKIB, the main department responsible for the NCC-CZ is the R&D Unit, however, other departments and sub-departments provide additional support, such as the Department of International Cooperation and the European Union; Training, Exercise and Education Department; National Strategy and Policy Unit as well as Economy, Project management and Legal departments. The R&D Unit is responsible for activating and coordinating the national ecosystem in cyber and information security, focusing on research and development (R&D). This includes leading the CYRIS group, preparing the *National Plan for Research and Development in Cyber and Information Security*, and facilitating involvement in relevant R&D&I projects. The key mission of the CYRIS group is to provide a platform for regular meetings of representatives from all sectors (academic, public and private) forming the national research and development community in cybersecurity and information security. CYRIS facilitates information sharing on current developments in digital technology and cybersecurity research, creates opportunities for forming project consortia, and enables discussions on challenges faced by the national research community. Through these activities, the R&D Unit plays a central role in advancing R&D initiatives and fostering collaboration across the Czech cybersecurity landscape.

NUKIB is supported by the **CSH** in fulfilling tasks under Regulation 2021/887. Founded by three leading Czech public universities, CSH specializes in cybersecurity research, education, and innovation. CSH brings key competencies to NCC-CZ: strong industry networks, established mechanisms for managing FSTP, and extensive experience in coordinating national and European projects (such as the *Czech*





National Cybersecurity Competence Centre NC3, CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence C4e, and EU pilot projects Concordia and CyberSec4Europe). CSH will support NUKIB in handling several NCC tasks, focusing on the national cybersecurity ecosystem, including FSTP, awareness-raising, match-making, outreach to industry, and providing technical and legal support. As part of the Cybersecurity Innovation Hub (CIH) which fulfils the role of an EDIH in cybersecurity in the Czech Republic, CSH will align NCC-CZ and EDIH activities, leveraging complementary goals to avoid duplication and maximize impact. This complementary role of CSH strengthens the consortium's capacity to address the project's objectives by integrating resources, methodologies, and insights from the EDIH network. The collaboration with CIH ensures the alignment of the NCC-CZ project with EU priorities for innovation and digital transformation, reinforcing the project's ability to foster impactful, cross-border collaborations and provide high-quality support to SMEs and other stakeholders.

The **roles and responsibilities within the project team** are outlined in the table *Project teams and staff* below and described in greater detail in the appendix, which includes the CVs of individual team members, covering previous work experience, current job occupation, and tasks related to the NCC-CZ.

### Project teams and staff

*Describe the project teams and how they will work together to implement the project.*

*List the staff included in the project budget (budget category A) by function/profile (e.g. project manager, senior expert/advisor/researcher, junior expert/advisor/researcher, trainers/teachers, technical personnel, administrative personnel etc. — use the same profiles as in the detailed budget table, if any (n/a for prefixed Lump Sum Grants)) and describe briefly their tasks.*

Name and function	Organisation	Role/tasks/professional profile and expertise
 Project Coordinator	NUKIB	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>Project Coordinator</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>responsible for smooth cooperation among consortia members</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>head of the Research and Development Unit of NUKIB, coordinating R&amp;D activities and implementing the National R&amp;D Plan for Cyber and Information Security. He also represents the Czech Republic on the ECCC Governing Board. Previously, he worked at the Ministry of Interior, focusing on international security research collaboration, consortium building, and research mission planning</li> </ul>
 Project Manager	NUKIB	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>Project Manager</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>complex and operational management of the project, i.e. in particular planning of activities, task management, controlling the progress of work within the given schedule and in relation to defined milestones</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>works in the Research and Development Unit of the NUKIB, managing the NCC-CZ and TEST-CERT-CZ projects. He oversees project deliverables, risk management, compliance with Digital Europe Programme rules, and coordination with the ECCC. He also contributed to developing FSTP policies and administering the first call within the NCC-CZ project. With over 12 years of experience managing EU-funded projects, he previously worked at the</li> </ul>









		South Moravian Region and the Moravian Library in Brno, focusing on project preparation, management, and stakeholder coordination
<div> <div></div> <div></div> </div> Project Administrator	NUKIB	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>Project Administrator</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>project implementation through administrative, organizational, and financial support, including preparing documentation, coordinating meetings, and monitoring budgets, setting up and working on FSTP mechanism</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>works in the Research and Development Unit of the NUKIB, specializing in project management and the FSTP mechanism. She oversees project coordination and administration, including launching calls and evaluating proposals, while ensuring smooth operation and compliance in projects like NCC-CZ, TEST-CERT-CZ, and CZQCI. Previously, she managed documentary production projects at Post Bellum, handling planning, budgeting, and team leadership, and coordinated volunteer projects at Masaryk University's MUNI POMÁHÁ initiative</li> </ul>
<div> <div></div> <div></div> </div> NCC-CZ expert	NUKIB	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>NCC-CZ expert</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>advancing NCC-CZ activities, national and cross-border cooperation, awareness-raising initiatives, coordinating with other NCCs within the NCC Network</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>works in the Research and Development Unit of the NUKIB, focusing on cybersecurity research and European cooperation. She oversees the Czech National Coordination Centre (NCC-CZ) under EU Regulation 2021/887, coordinating national cybersecurity R&amp;D and fostering cross-border collaboration. At the European level, she serves as an alternate member of the ECCC Governing Board. Previously, Nikola worked with the Association for International Affairs on project coordination in model diplomacy and collaborated with the Czech Government's European Affairs Information Department and Masaryk University's International Institute of Political Science</li> </ul>
<div> <div></div> <div></div> </div> Legal Manager	NUKIB	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>Legal Manager</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>managing the legal aspect of the project using the experience from previous projects, ensuring that the documentation of FSTP complies with legal regulations, carrying out legal review of other documentation and activities</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>head of the Legal Unit at the NUKIB. He oversees a team handling cybersecurity law, classified information protection, labour law, contract law, administrative processes, and court representation. Vit provides legal support for projects like NCC-CZ and TEST-CERT-CZ, ensuring compliance with</li> </ul>



		Czech and EU legislation and offering legal analyses. Previously, he worked at the Office for the Protection of Competition's State Aid Department and in the law firm of JUDr. Helena Pilařová, focusing on general legal matters
<div> <div></div> <div></div> </div> <p>Legal Advisor</p>	NUKIB	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>Legal Advisor</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>creation of legally relevant part of project documentation, ensuring compliance of the terms of the call and entire process with national legislation as well as European law</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>lawyer at the NUKIB, specializing in public procurement and legal support for projects like NCC-CZ and TEST-CERT-CZ. She has contributed to establishing the FSTP mechanism and ensuring compliance with national and EU legislation. Her work also includes handling classified information, drafting contracts, and providing legal advice in NUKIB's core areas. Previously, she worked at MT Legal and the Office for the Protection of Competition, focusing on public procurement and tender reviews</li> </ul>
<div> <div></div> <div></div> </div> <p>Financial Manager</p>	NUKIB	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>Financial Manager</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>approving of financial operations, monitoring budget expenditures to ensure alignment with the financial plan of the project</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>financial manager in the Financial Department of the NUKIB, responsible for overseeing financial operations and budget alignment for the NCC-CZ and TEST-CERT-CZ projects. Her role includes managing financial resources, approving operations, and monitoring expenditures. Previously, she worked at the Transport Research Centre as an economist, managing research division finances and project reporting, and at Masaryk University's Personnel Department, focusing on staff cost reporting for research projects</li> </ul>
<div> <div></div> <div></div> </div> <p>Financial Administrator</p>	NUKIB	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>Financial Administrator</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>setting up the project's financial mechanisms, ensuring the approval of financial flows as Budget Administrator, managing project financing reports in compliance with national legislation, adhering to methodologies of the Ministry of Finance within the State Budget, ensuring project records in required national information systems</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>works in the Budget Department of the NUKIB, managing funding for the NCC-CZ, TEST-CERT-CZ, and CZQCI projects. She oversees budget issues within Chapter 378 of the state budget and provides methodological guidance on national funding for project teams. Previously, she worked at the State Veterinary Administration as a budget manager for State Veterinary Institutes and at the Municipality of Brno as</li> </ul>



		a departmental economist, handling public procurement, budget preparation, and financial administration
 Organization & Administration Officer	NUKIB	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>Organization &amp; Administration Officer</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>administering and registering contracts and all related project documentation, managing project expenses from an administrative perspective, participating in organizing conferences and other events related to projects</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>works as a coordinator and project assistant at the NUKIB. She manages departmental and divisional documentation, coordinates internal communication, submits documents for approval, and oversees external communication through information systems. She also administers NUKIB's revenue and expenditure. Previously, Magdalena worked as a librarian at the University of Defence Language Center, where she organized documents and provided reference and information services using information systems</li> </ul>
 Methodological Advisor	NUKIB	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>Methodological Advisor</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>methodological support on EU funds, reporting project progress related to these funds to the project manager</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>coordinator and EU funds specialist at the Project Management Unit of the NUKIB. He ensures efficient processes for projects funded by EU resources, including team and knowledge coordination, EU resource planning, and methodological support for EU-co-financed projects. He also assists with preparing and submitting funding applications. Previously, Jiří worked at the Ministry of Education, Youth and Sports as the Garant of Controlling, where he led compliance verification for grants, ensured adherence to Czech and EU regulations, and managed public administration control processes</li> </ul>
 Event & PR manager	NUKIB	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>Event &amp; PR manager</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>planning, organizing, and promoting events while managing public relations efforts to enhance the NCC-CZ's and project's visibility and engagement with its target audiences</li> </ul>
 Coordination Lead	CSH	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>Coordination Lead</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>coordinating NCC activities at CSH and with NUKIB; managing the project tema and activities at CSH; ensuring complementarity between NCC and EDIH initiatives; managing operational aspects and quality assurance related to FSTP mechanism</li> </ul> <p><u>Professional profile and expertise:</u></p>







		<ul style="list-style-type: none"> <li>▪ founding member of Czech National Cybersecurity Competence Centre (NC3) and the Centre of Excellence of Cybersecurity and Cybercrime (C3e). As a manager, researcher, and lecturer at Masaryk University, he leads numerous cybersecurity projects, including Cybersecurity Innovation Hub and REWIRE. His legal background, coupled with extensive IT and managerial experience, strengthens his role in strategic project management</li> </ul>
<div>██████████</div> <div>Strategic Lead</div>	CSH	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>▪ Strategic Lead</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>▪ strategic leading NCC tasks carried out by CyberSecurity Hub; aligning NCC activities with strategic goals; overseeing the implementation of NCC activities</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>▪ director of Cybersecurity Hub and CERIT at Masaryk University. He has extensive leadership experience, including as the former General Director of CzechInvest. He leads the Czech Cybersecurity Innovation Hub and various strategic projects focused on cybersecurity and ICT innovation</li> </ul>
<div>██████████</div> <div>NCC Operations Support</div>	CSH	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>▪ NCC Operations Support</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>▪ assisting with NCC operations and coordination with NUKIB; supporting FSTP deployment, drafting and reviewing deliverables</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>▪ lawyer and researcher with expertise in cybersecurity law and online platforms. He has contributed to multiple projects at NC3 and C3e and serves as a lecturer and consultant on cybersecurity, electronic identification, and consumer protection. His extensive experience in international law and research strengthens the NCC's operational support</li> </ul>
<div>██████████</div> <div>Communication and Dissemination Lead</div>	CSH	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>▪ Communication and Dissemination Lead</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>▪ leading communication and dissemination activities for NCC-CZ 2.0; managing events, community engagement, and strategic outreach efforts</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>▪ specializes in strategic communications and public engagement in cybersecurity. He has managed communication for the European CONCORDIA H2020 consortium and contributed to NC3 and C3e initiatives. His experience in information security awareness and human factors in cybersecurity enhances his ability to effectively disseminate project outcomes and engage stakeholders</li> </ul>
<div>██████████</div> <div>Financial Manager</div>	CSH	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>▪ Financial Manager</li> </ul> <p><u>Tasks:</u></p>





		<ul style="list-style-type: none"> <li>setting up financial mechanisms at CSH; managing financial reporting and audits; ensuring efficient handling of cascading financing mechanisms, financial support in FSTP mechanisms</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>he has over a decade of expertise in financial and project management, including experience with NC3 and CERIT projects. He has previously managed major investment projects and eGovernment initiatives, making him well-equipped to oversee financial compliance and reporting in NCC-CZ</li> </ul>
 Project and Financial Administrator	CSH	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>Project and Financial Administrator</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>providing administrative support for NCC-CZ activities; assisting with project and financial management; supporting the project team</li> </ul> <p><u>Professional profile and expertise:</u></p> <ul style="list-style-type: none"> <li>extensive experience managing complex projects in cybersecurity and research. She has worked on NC3 and C3e projects and brings a strong background in financial planning, budgeting, and project administration, ensuring efficient support for NCC-CZ 2.0's operations</li> </ul>
 Event Administrator	CSH	<p><u>Role:</u></p> <ul style="list-style-type: none"> <li>Event Administrator</li> </ul> <p><u>Tasks:</u></p> <ul style="list-style-type: none"> <li>administration and coordination of events, support to the participants and speakers</li> </ul>

#### Outside resources (subcontracting, seconded staff, etc)

*If you do not have all skills/resources in-house, describe how you intend to get them (contributions of members, partner organisations, subcontracting, etc.) and for which role/tasks/professional profile/expertise*

*If there is subcontracting, please also complete the table in section 4.*

The NCC-CZ 2.0 project tasks will be carried out by staff from NUKIB and CSH. The objective is to concentrate as many resources as possible internally by standard hiring process. However, the project team may be complemented with **external collaborators** as needed, particularly for specialized areas. These may include support for graphic design for NCC-CZ materials, assistance in event organization (position of event manager), and help with promotion and dissemination activities, such as social media management and outreach (position of project PR manager). All external contributions will comply with national funding regulations and the conditions outlined in the call document, ensuring alignment with project standards and objectives.

Also, **additional experts** from other departments within NUKIB and CSH might complement the project team (as described above) on an ad-hoc basis.

#### Consortium management and decision-making (if applicable)

*Explain the management structures and decision-making mechanisms within the consortium. Describe how decisions will be taken and how regular and effective communication will be ensured. Describe methods to ensure planning and control.*

**Note:** The concept (including organisational structure and decision-making mechanisms) must be adapted to the complexity and scale of the project.



For the NCC-CZ 2.0 project to operate efficiently, a comprehensive **management and administrative structure** must be established. This structure has already been set-up and tested for the NCC-CZ and TEST-CERT-CZ projects and will be utilized for the follow-up project as well, with potential adjustments based on lessons learned and best practices.

The overall coordination and management of the project fall under the responsibility of the project coordinator, NUKIB, which will work closely with CSH to ensure the project is carried out in line with the set requirements. The **consortium's decision-making** body, the **General Assembly (GeA)**, comprises representatives from both consortium partners and is responsible for making key strategic decisions. Members of the GeA will meet regularly to assess the consortium collaboration and the progress of project implementation. Representatives from both institutions will also meet regularly as part of the **Project Steering Committee (PSC)** meetings to ensure ongoing alignment and effective coordination in fulfilling project activities.

To mitigate management and decision-making risks, the consortium will adhere to the terms outlined in the **Consortium Agreement (CA)** and Grant Agreement (GA), as well as specific provisions in this project proposal. The CA will provide a legal foundation for the consortium collaboration within the project, ensuring clear governance and regulations for all consortium members, facilitating smooth collaboration, and defining protocols for conflict resolution. **Internal decision-making processes** will adhere to established consortium documentation, including the *Project Management Handbook*, which will encompass the *Coordination Matrix* and *Workflow Plan*. These will specify communication processes, procedures, and responsibilities, ensuring that planning, control, and consistent, effective communication are maintained at all levels of the consortium. This structured approach promotes transparency, accountability, and efficient collaboration throughout the project.

#§CON-SOR-SS§# #§QUA-LIT-QL§# #IMP-ACT-IA@# #COM-DIS-VIS-CDV@#

### 3. IMPACT

#### 3.1 Expected outcomes and deliverables — Dissemination and communication

##### Expected outcomes and deliverables

*Define and explain the extent to which the project will achieve the expected impacts listed in Call document.*

The NCC-CZ 2.0 project is designed to deliver impactful outcomes and concrete deliverables that fully align with the objectives outlined in the Call document, contributing to a strengthened cybersecurity ecosystem and higher cyber resilience of SMEs and other entities across the EU. The activities and deliverables in this project aim to build a resilient cybersecurity community, promote the uptake of advanced cybersecurity solutions among targeted stakeholders, and enhance the role of the NCC-CZ in supporting EU cybersecurity priorities.

##### Key expected outcomes and deliverables:

##### Work Package 2: Enhancing Cybersecurity Awareness and Engagement

This WP contributes to the strengthened cybersecurity capacities of stakeholders by raising awareness and engaging diverse actors, such as SMEs, public institutions, and NGOs, in discussions on current and emerging cybersecurity challenges. Through targeted awareness campaigns, workshops, and communication activities, the WP supports the dissemination of state-of-the-art cybersecurity solutions and fosters a better understanding of their adoption.

##### Expected outcomes

- Improved awareness of cybersecurity challenges and solutions among SMEs, academic and research institutions, NGOs, and public organizations.
- Increased stakeholder engagement through targeted awareness-raising campaigns and communication activities.
- Strengthened visibility of NCC-CZ activities and results, fostering greater participation in cybersecurity initiatives.
- Enhanced alignment between national and EU cybersecurity awareness efforts.

##### Deliverables

- **D2.1 Communication, Dissemination and Exploitation Strategy (M4):** A detailed strategy guiding communication, dissemination, and exploitation of project results.
- **D2.2 Awareness Raising Needs Report (M6):** Identifies cybersecurity awareness gaps and priorities for targeted activities.



- **D2.3 Awareness and Engagement Campaign Materials (M18):** Materials supporting awareness campaigns, including brochures, presentations, and digital content.
- **D2.4 Final Awareness and Engagement Impact Report (M48):** Summarizes outcomes of all awareness and engagement activities, including lessons learned and sustainability plans.

#### KPIs

- **Number of awareness-raising, capacity building and training events organized and/or attended:** 60
- **Number of stakeholders reached through events:** 250
- **Number of stakeholders engaged through awareness campaigns:** 1 000
- **Number of Technology Open Days organised:** 8
- **Number of awareness-raising and capacity building webinars organised:** 16  
(Including 8 webinars specifically focused on the needs of SMEs)

#### Work Package 3: Financial Support for Strengthening Cybersecurity Capabilities

This WP directly addresses the Call's objective of facilitating the uptake of cybersecurity solutions, particularly by SMEs. By distributing approximately 50% of the project's funding via Financial Support to Third Parties (FSTP), this WP empowers entities to adopt and implement advanced cybersecurity measures. It also aligns with the Call's focus on providing technical assistance and enabling stakeholders to participate in national and cross-border projects.

#### Expected outcomes

- Strengthened cybersecurity capabilities among SMEs and other stakeholders through targeted financial support.
- Adoption of innovative cybersecurity solutions and best practices aligned with EU strategic priorities.
- Enhanced resilience and compliance with EU cybersecurity regulations (e.g., NIS2, CRA).
- Efficient and transparent management of FSTP.

#### Deliverables

- **D3.1 Strategy Document for FSTP Priorities (M8):** Defines priority areas for FSTP support, updated for each call wave if needed.
- **D3.2 Monitoring and Impact Evaluation Report (M48):** Evaluates outcomes of FSTP-supported projects and recommends mechanism improvements.

#### KPIs

- **Number of supported projects aligned with EU and Czech cybersecurity priorities:** 25
- **Number of entities benefiting from FSTP cascade financing:** 25
- **Number of entities provided with information and technical support related to funding opportunities:** 50  
(out of this number, at least 30 SMEs)
- **Number of webinars focused on FSTP calls and project development:** 8  
(Including 6 webinars specifically aimed at the target group of SMEs)

#### Work Package 4: Cybersecurity Community Building and Engagement

This WP contributes to the strengthened cybersecurity community by expanding membership, fostering collaboration, and promoting synergies between national and EU-level initiatives. The WP supports the Call's objective of acting as a national contact point, enabling collaboration with the ECCC and other NCCs. Activities such as working group meetings, idea-pitching sessions, and knowledge-sharing events facilitate deeper collaboration and innovation.

#### Expected outcomes

- Expanded and more resilient cybersecurity community, engaging diverse stakeholders across sectors.
- Improved collaboration within the national cybersecurity ecosystem and with the broader NCC Network.
- Increased knowledge sharing and capacity building through targeted activities.
- Promotion and dissemination of community-developed resources and achievements.
- Increased participation of Czech entities in the EU Cybersecurity Competence Community.

#### Deliverables

- **D4.1 Community Membership Management Report (M24):** Summarizes membership recruitment and management efforts.
- **D4.2 Knowledge Sharing and Engagement Report (M36):** Documents all knowledge-sharing and capacity-building activities, including collaboration initiatives.



- **D4.3 Final Community Impact Report (M48)** Comprehensive evaluation of community growth, collaborations, and sustainability.

**KPIs**

- **Number of community members engaged:** 270
- **Number of actions to foster expertise and synergies within the community:** 50
- **Number of collaborative actions with NCCs and ECCC:** 30
- **Number of reusable resources shared in the public repository:** 30
- **Number of organised community meetings:** 8
- **Number of activities aimed at the promotion of membership in EU Cybersecurity Competence Community:** 5

**Total number of organised events among all of the WPs:**

Type of event	KPIs (numbers)
Technology open days	8
Awareness-raising and capacity building webinars	16
Webinars focused on FSTP calls and project drafting	8
Community meetings	8


**Overall Impact:** By fostering a robust cybersecurity community, supporting the adoption of cybersecurity solutions, and strengthening the NCC's role within the EU framework, this project will contribute significantly to the EU's strategic autonomy in cybersecurity. Deliverables such as updated strategy documents, FSTP call publications, and impact reports will document progress and ensure accountability, directly supporting the goals of the Call document.

**Dissemination and communication of the project and its results**

*If relevant, describe the communication and dissemination activities, activities (target groups, main messages, tools, and channels ) which are planned in order to promote the activities/results and maximise the impact. The aim is to inform and reach out to society and show the activities performed, and the use and the benefits the project will have for citizens*

*Clarify how you will reach the target groups, relevant stakeholders, policymakers and the general public and explain the choice of the dissemination channels.*

*Describe how the visibility of EU funding will be ensured.*

 *In case your proposal is selected for funding, you will have to provide a more detailed plan for these activities (dissemination and communication plan), within 6 months after grant signature. This plan will have to be periodically updated; in line with the project progress.*

To effectively **communicate and disseminate the NCC-CZ 2.0 project's activities and outcomes**, NCC-CZ consortium will employ a robust set of strategies and tools tailored to reach its target audiences, including research and academic organizations, SMEs and public organizations, in coordination with partners on the national level (for example the NCPs for Horizon Europe and Digital Europe programmes, EDIHs) and EU level (NCC Network, ECCC). The objective is to maximize visibility, engagement, and impact across these groups by emphasizing the project's benefits and its value.

**Main target audiences:**

- SMEs including start-ups, industrial stakeholders



- research and academic organizations
- NGOs, relevant civil society associations
- standardization and certification organizations
- public sector
- general public

#### Primary communication channels:

- **Website:**
  - A dedicated NCC-CZ website will serve as the project's central information platform, showcasing activities, news, and events. Also, both consortium partner's will utilise their own websites to amplify NCC-CZ's content and expand reach.
- **Social Media:**
  - Selected social media platforms of both consortium partners will be used to disseminate updates and engage target audiences effectively. Posts will provide regular insights into NCC-CZ activities, events, and outcomes, fostering a broader online community.
- **Media:**
  - NCC-CZ will collaborate with specialized media in cybersecurity through PR articles and press releases. NCC-CZ consortium representatives might provide interviews at key project milestones to maintain public interest and engagement. Regular press releases will also ensure consistent visibility of project achievements.
- **Direct Stakeholder Communication:**
  - NCC-CZ will maintain regular contact with partners and stakeholders through newsletters, direct emails, and updates on new activities or outputs. This approach will enable continuous engagement and build strong stakeholder relations.

#### Communication tools:

- **Events and awareness campaigns:**
  - A series of events - including international and national conferences, regional seminars, and tailored workshops/webinars - will promote awareness and knowledge sharing.
- **PR campaigns:**
  - Traditional tools like press releases, interviews, and expert media articles will be supported by modern communication formats such as podcasts and social media posts to capture audience interest effectively.
- **Direct mailing campaigns:**
  - Through newsletters and targeted mailing, NCC-CZ will reach out to stakeholders and inform them about relevant project updates.

#### Communication and dissemination strategy:

- NCC-CZ consortium will follow a sophisticated **Communication and Dissemination Strategy** developed at the start of the project, utilising the *Communication and Dissemination Strategy* developed in the NCC-CZ project with adjustments if needed. This strategy will align with the strategic objectives of the NCC-CZ and encompass an overall dissemination and communication strategy tailored to the needs of target groups, specifying responsibilities, cooperation frameworks, and detailed approaches.

#### Ensuring EU funding visibility:

- It will be ensured that all project and communication activities will adhere to the EU visibility requirements, acknowledging EU support and displaying the European flag (emblem) and funding statement including the quality of information disclaimer.

#### Supporting materials:

- The project will produce a comprehensive set of marketing materials illustrating NCC-CZ services to attract target group attention.

By leveraging these channels, tools, and structured documentation, NCC-CZ will ensure effective communication, maximize project impact, and emphasize the added value EU funding brings to cybersecurity efforts.

The inclusion of CSH, which also coordinates the **Cybersecurity Innovation Hub (CIH)**, enhances the project's capacity to disseminate its outcomes and engage stakeholders effectively. As part of the EDIH network, CIH contributes additional outreach channels, enabling the project to access a broader audience across Europe. This partnership ensures that knowledge-sharing activities, workshops, and training sessions take into account the latest innovations in cybersecurity and are aligned with the EDIH network's goals. By leveraging CIH's established connections and expertise, the project maximizes the impact of its dissemination and communication efforts, directly benefiting stakeholders and strengthening the



European cybersecurity ecosystem. CIH has built a Central-European EDIH network collaborating in the field of best practices and experiences exchange with relevance for the region.

#§COM-DIS-VIS-CDV§#

3.2 Competitiveness and benefits for society

**Competitiveness and benefits for the society**

*Describe the extent to which the project will strengthen competitiveness and bring important benefits for society*

The NCC-CZ 2.0 project aims to enhance **cybersecurity competitiveness and provide significant societal benefits** across the Czech Republic and the EU. Through its targeted initiatives, NCC-CZ will boost the capacity of SMEs, start-ups, and academic and research institutions to participate in cross-border projects and cybersecurity actions funded by EU programs. By providing stakeholders with technical assistance in applying for DEP funds in cooperation with other national partners, NCC-CZ will strengthen their competitive positioning in the evolving cybersecurity landscape.

**Strengthening competitiveness**

- The provided support from the NCC-CZ will enhance stakeholders' ability to effectively compete on both national and international levels for funding, empowering them to implement best practices and innovative cybersecurity solutions that increase resilience and market readiness.
- NCC-CZ's role in supporting and promoting the Cybersecurity Competence Community will foster knowledge exchange and serve as a platform for dialogue on the European level.
- The project will foster cross-border cooperation, both with other NCCs within the Network and by connecting national communities. This exchange will strengthen competitiveness by drawing on diverse insights and facilitating access to new business opportunities.

**Societal benefits**

- The NCC-CZ will work closely with other partners to raise cybersecurity educational awareness, fostering a more informed and resilient society. By building public awareness of cybersecurity challenges and best practices, the project will contribute to a safer cyberspace and bolster societal resilience against current and emerging threats.

Through targeted project activities, NCC-CZ will contribute to a well-informed, cybersecurity-conscious society, providing businesses with the secure environment needed to leverage modern technologies. Additionally, NCC-CZ's focus on developing cybersecurity skills and supporting innovation will further drive the Czech Republic's and EU's progress toward a safer and more resilient future.

3.3 Environmental sustainability and contribution to European Green Deal goals

**Environmental sustainability and contribution to European Green Deal goals**

*Describe the extent to which the project will contribute to environmental sustainability and in particular to European Green Deal goals*

 This might not be applicable to all topics — for details refer to the Call document.

Not applicable as stated in the call document.

#§IMP-ACT-IA§#

#@WRK-PLA-WP@#

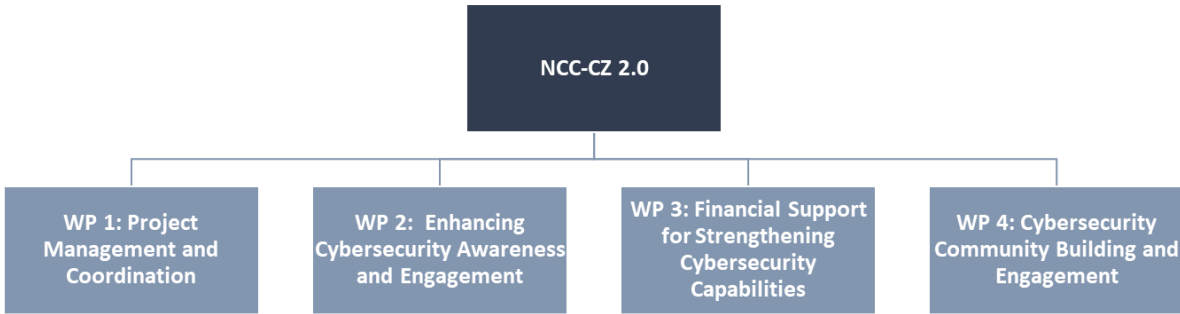
## 4. WORK PLAN, WORK PACKAGES, ACTIVITIES, RESOURCES AND TIMING

### 4.1 Work plan

#### Work plan

*Provide a brief description of the overall structure of the work plan (list of work packages or graphical presentation (Pert chart or similar)).*

In the figure below, the overall structure of the planned WPs of the NCC-CZ 2.0 project is presented. The work plan will consist of fulfilling the objectives and scope as described above in section 1.1 and 1.2. All of the WPs are scheduled for the entire duration of the project (i.e., 48 months).



The main objectives of the NCC-CZ 2.0 WPs are:

- **WP 1: Project Management and Coordination** aims to ensure effective project coordination, monitoring, and financial management while maintaining high-quality deliverables and mitigating risks.
- **WP 2: Enhancing Cybersecurity Awareness and Engagement** focuses on identifying and addressing gaps in cybersecurity awareness, targeting outreach activities, promoting EU funding opportunities, and enhancing visibility and collaboration.
- **WP 3: Financial Support for Strengthening Cybersecurity Capabilities** seeks to refine and implement the FSTP mechanism through strategic calls for proposals, addressing critical cybersecurity needs and enhancing capabilities of relevant stakeholders.
- **WP 4: Cybersecurity Community Building and Engagement** aims to expand and manage the cybersecurity community, promote collaboration, align national and EU initiatives, and amplify community achievements while fostering cross-border cooperation.

Details about the individual WPs including the planned objectives, tasks, milestones, and deliverables as well as budgetary information are available in section 4.2 below.

## 4.2 Work packages, activities, resources and timing

### Work Package 1

Estimated budget — Resources												
Participant	Costs <i>(n/a for Lump Sum Grants)</i>											
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		D.2 Internally invoiced goods and services	D.3 PAC procurement costs <i>(for PAC Grants for Procurement)</i>	E. Indirect costs	Total costs
NUKIB	70 person months	240 000 EUR	0 EUR	0 EUR	0 EUR	0 EUR	0 grants 0 prizes	0 EUR	0 EUR	0 EUR	16 800 EUR	256 800 EUR
CSH	14 person months	72 700 EUR	0 EUR	0 EUR	2 000 EUR	10 000 EUR	0 grants 0 prizes	0 EUR	0 EUR	0 EUR	5 929 EUR	90 629 EUR
Total	84 person months	312 700 EUR	0 EUR	0 EUR	2 000 EUR	10 000 EUR	0 grants 0 prizes	0 EUR	0 EUR	0 EUR	22 729 EUR	347 429 EUR
For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see <a href="#">Portal Reference Documents</a> ).												



**Work Package 2**

Estimated budget — Resources												
Participant	Costs <i>(n/a for Lump Sum Grants)</i>											
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		D.2 Internally invoiced goods and services	D.3 PAC procurement costs <i>(for PAC Grants for Procurement)</i>	E. Indirect costs	Total costs
NUKIB	40 person months	137 143 EUR	0 EUR	10 000 EUR	15 000 EUR	50 000 EUR	0 grants 0 prizes	0 EUR	0 EUR	0 EUR	14 850,01 EUR	226 993,01 EUR
CSH	60 person months	327 200 EUR	0 EUR	5 000 EUR	2 000 EUR	8 300 EUR	0 grants 0 prizes	0 EUR	0 EUR	0 EUR	23 975 EUR	366 475 EUR
Total	100 person months	464 343 EUR	0 EUR	15 000 EUR	17 000 EUR	58 300 EUR	0 grants 0 prizes	0 EUR	0 EUR	0 EUR	38 825,01 EUR	593 468,01 EUR
For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see <a href="#">Portal Reference Documents</a> ).												

**Work Package 3**

Estimated budget — Resources												
Participant	Costs <i>(n/a for Lump Sum Grants)</i>											
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		D.2 Internally invoiced goods and services	D.3 PAC procurement costs <i>(for PAC Grants for Procurement)</i>	E. Indirect costs	Total costs
NUKIB	100 person months	342 857 EUR	0 EUR	0 EUR	0 EUR	80 000 EUR	25 grants 0 prizes	2 500 000 EUR	0 EUR	0 EUR	204 599,99 EUR	3 127 456,99 EUR
CSH	34 person months	181 750 EUR	0 EUR	0 EUR	0 EUR	0 EUR	0 grants 0 prizes	0 EUR	0 EUR	0 EUR	12 722,5 EUR	194 472,5 EUR
Total	134 person months	524 607 EUR	0 EUR	0 EUR	0 EUR	80 000 EUR	25 grants 0 prizes	2 500 000 EUR	0 EUR	0 EUR	217 322,49 EUR	3 321 929,49 EUR
For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see <a href="#">Portal Reference Documents</a> ).												

**Work Package 4**

Estimated budget — Resources												
Participant	Costs <i>(n/a for Lump Sum Grants)</i>											
	A. Personnel		B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		D.2 Internally invoiced goods and services	D.3 PAC procurement costs <i>(for PAC Grants for Procurement)</i>	E. Indirect costs	Total costs
NUKIB	70 person months	240 000 EUR	0 EUR	60 000 EUR	50 000 EUR	180 000 EUR	0 grants 0 prizes	0 EUR	0 EUR	0 EUR	37 100 EUR	567 100 EUR
CSH	27 person months	145 400 EUR	0 EUR	10 000 EUR	2 000 EUR	0 EUR	0 grants 0 prizes	0 EUR	0 EUR	0 EUR	11 018 EUR	168 418 EUR
Total	97 person months	385 400 EUR	0 EUR	70 000 EUR	52 000 EUR	180 000 EUR	0 grants 0 prizes	0 EUR	0 EUR	0 EUR	48 118 EUR	735 518 EUR
For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see <a href="#">Portal Reference Documents</a> ).												

**Purchases and equipment**

<b>Purchase costs (travel and subsistence, equipment and other goods works and services)</b>				
<i>Details for major cost items (needed if costs declared under 'purchase costs' are higher than 15% of the claimed personnel costs). Start with the most expensive cost items, down to the 15% threshold.</i>				
Participant 1:	NUKIB			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
Purchase costs related to ensuring planned activities in the field of community building, awareness activities and FSTP	Other goods, works and services	WP2, WP3, WP4	Costs associated with the implementation of planned awareness raising activities (e.g. renting space, equipment, organising and delivering workshops, providing communication activities), cascade funding activities (e.g. providing external evaluators), activities related to broadening and deepening cooperation within the cybersecurity community and building capacity and inter-operability in this area (e.g. conferences, webinars, workshops, training materials and tools).	310 000 EUR
Total				310 000 EUR
Participant 2:	CSH			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
N/A				
Total				N/A
Total purchase costs > 15% (all participants)				310 000 EUR
Remaining purchase costs < 15% (all participants)				174 300 EUR

Total purchase costs (all participants)	484 300 EUR
---	-------------

**Other cost categories**

Other cost categories (financial support to third parties, internally invoiced goods and services, etc)		
Complete the table below for each participant that would like to declare costs under other costs categories (e.g. financial support and internally invoiced goods and services), irrespective of the percentage of personnel costs.		
Participant 1:	NUKIB	
Cost category	Explanations	Costs (EUR)
Financial support to third parties	<p>The implementation of WP3 will involve three strategic calls for proposals over the project's duration, with each call tailored to address priority areas identified through ongoing analysis. These calls will aim to strengthen cybersecurity capabilities among small and medium-sized enterprises (SMEs) and other eligible entities.</p> <p>Maximum amount per third party: 100 000 EUR (mandatory co-financing of 50% by the supported third party).</p> <p>Criteria for calculating the exact amounts: budget categories and cost eligibility rules will be in line with the Call document and DEP rules.</p> <p>Types of activity that qualify (closed list): innovation, concept development and experimentation, proof-of-concept delivery, demonstration, analysis, organisation of events and courses, networking, awareness raising activities, capacity building, methodology, software, guidelines and best practices, technical documentation and user's manuals, data repositories, evaluation frameworks, feasibility studies, audits and implementation of compliance measures.</p> <p>Person/categories of persons to be supported: SMEs, start-ups, academic and research organizations, NGOs.</p> <p>Criteria for giving support and evaluation process: To ensure effective selection and impactful outcomes, all submitted projects will be evaluated based on a set of transparent criteria focused on quality, feasibility, and impact. The evaluation process will align with the established processes of NCC-CZ FSTP Mechanism and the NCC-CZ Council, building on the framework of the first NCC-CZ project, with necessary adjustments based on current needs and lessons</p>	2 500 000 EUR

	<p>learned. The evaluation process is structured as a round-based call, ensuring that the exact time of submission within the call's time-frame does not influence the outcome of the evaluation.</p> <p>Each project is thoroughly assessed by at least two independent experts: a designated reviewer, who conducts a detailed evaluation, and a NCC-CZ Council Rapporteur, who provides additional insight and context for the evaluation. After these individual evaluations are completed, the NCC-CZ Council convenes to discuss the project in depth. This process ensures that a wide range of perspectives is considered, including the alignment of the project with strategic goals and its potential impact. Based on this discussion, the NCC-CZ Council formulates a recommendation, either supporting or rejecting the project for funding. This recommendation is then forwarded to the Director of NUKIB, who makes the final decision regarding project approval or rejection, ensuring a balanced and transparent decision-making process.</p>	
Internally invoiced goods and services	N/A	-
Participant 2:	CSH	
Cost category	Explanations	Costs (EUR)
Financial support to third parties	N/A	-
Internally invoiced goods and services	N/A	-

**Timetable**

<b>Timetable (projects of more than 2 years)</b> <i>Fill in cells in beige to show the duration of activities. Repeat lines/columns as necessary.</i> <b>Note:</b> Use actual calendar years and quarters. In the timeline you should indicate the timing of each activity per WP. You may add additional columns if your project is longer than 6 years.																
ACTIVITY	YEAR 1				YEAR 2				YEAR 3				YEAR 4			
	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4
<b>Task 1.1</b> - Project team and consortium coordination																
<b>Task 1.2</b> - Project monitoring and reporting																
<b>Task 1.3</b> - Financial management																
<b>Task 1.4</b> - Risk management and mitigation																
<b>Task 2.1</b> - Identifying and planning awareness raising activities																
<b>Task 2.2</b> - Amplifying project visibility and stakeholder reach																
<b>Task 2.3</b> - Strengthening collaboration across the NCC Network																
<b>Task 2.4</b> - Skills development and engagement																
<b>Task 2.5</b> - Project development and support																
<b>Task 3.1</b> - Needs assessment and strategy development																

<b>Task 3.2</b> - Implementation of FSTP calls and project selection																
<b>Task 3.3</b> - Monitoring, impact evaluation, and reporting																
<b>Task 3.4</b> - Enhancement of FSTP mechanism																
<b>Task 4.1</b> - Community growth and engagement																
<b>Task 4.2</b> - Membership management and technical support																
<b>Task 4.3</b> - Knowledge sharing and networking activities																
<b>Task 4.4</b> - ECCC support and active involvement																

#\$WRK-PLA-WP\$#



#@ETH-ICS-EI@#

5. OTHER

5.1 Ethics

<b>Ethics</b> <i>If the Call document contains a section on ethics, the ethics issues and measures you intend to take to solve/avoid them must be described in Part A.</i>
<b>Ethical dimension of the objectives, methodology and likely impact</b> The project does not involve any ethics issues that would invoke the need for ethics self-assessment. Therefore, no ethical issues have been entered into the section 9 of this form. However, we note that all work carried out under the project will respect fundamental ethics principles, including those reflected in the Charter of Fundamental Rights of the European Union, the relevant ethics rules of European Commission projects, and national and European laws.
<b>Compliance with ethical principles and relevant legislation</b> The project ethics requires all partners contributing to the project to comply with the letter and spirit of any laws, legislation and guidelines that apply and to implement all tasks to the highest ethical behaviour and standards. Each partner shall implement their project tasks with total respect and highest regard for their organisational colleagues, fellow partners and project participants. The project will be implemented in a professional manner without any form of prejudices whatsoever, irrespective of gender, race, ethnic background, religion, nationality, geography, colour or creed.  The project coordinator, National Cyber And Information Security Agency (NUKIB), will be monitoring ethics that the project will leverage. Good ethical governance and review of research and innovation is a core value and priority at NUKIB. It is the responsibility of the NUKIB and CSH to ensure compliance with statutory requirements and execution to the highest ethical principles, which emphasise the rights and welfare of subjects, treating all with dignity and ensuring that those who participate in research, whether subjects, researchers, other stakeholders are not put at risk project will leverage. Additionally, all activities will be carried out ensuring ethical principles in accordance with Directive 95/46/EC of the European Parliament and also in accordance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). All national data protection and privacy laws will also be followed.

#§ETH-ICS-EI\$# #@SEC-URI-SU@#


5.2 Security

<b>Security</b> <i>The security issues and the measures you intend to take to solve/avoid them must be described in Part A.</i> <b>Note:</b> Beneficiaries must ensure that their projects are not subject to national/third country security requirements that could affect the implementation or put into question the award of the grant (e.g. technology restrictions, national security classification, etc).
The project does not involve any security aspects that would invoke the need for Security self-assessment. EUCI will not be used during the project preparation or implementation. It is not aimed at producing results that could have potential to be misused.

#§SEC-URI-SU\$# #@DEC-LAR-DL@#

6. DECLARATIONS

<b>Double funding</b>	
<b>Information concerning other EU grants</b>	<b>YES/NO</b>

 Please note that there is a strict prohibition of double funding from the EU budget (except under EU Synergies actions).	
We confirm that to our best knowledge none of the projects under the action plan as a whole or in parts have benefited from any other EU grant (including EU funding managed by authorities in EU Member States or other funding bodies, e.g. EU Regional Funds, EU Agricultural Funds, etc). If NO, explain and provide details.	YES
We confirm that to our best knowledge none of the projects under the action plan as a whole or in parts are (nor will be) submitted for any other EU grant (including EU funding managed by authorities in EU Member States or other funding bodies, e.g. EU Regional Funds, EU Agricultural Funds, etc). If NO, explain and provide details.	YES

<b>Financial support to third parties (if applicable)</b>
<i>If in your project the maximum amount per third party will be more than the threshold amount set in the Call document, justify and explain why the higher amount is necessary in order to fulfil your project's objectives.</i>
The maximum amount per third party will not be more than the threshold amount set in the Call document.

#\$DEC-LAR-DL\$#

ANNEX 2

ESTIMATED BUDGET FOR THE ACTION

	Estimated eligible <sup>1</sup> costs (per budget category)										Estimated EU contribution <sup>2</sup>				
	Direct costs								Indirect costs	Total costs	EU contribution to eligible costs			Maximum grant amount <sup>6</sup>	
	A. Personnel costs		B. Subcontracting costs	C. Purchase costs			D. Other cost categories		E. Indirect costs <sup>3</sup>		Funding rate % <sup>4</sup>	Maximum EU contribution <sup>5</sup>	Requested EU contribution		
	A.1 Employees (or equivalent)		A.4 SME owners and natural person beneficiaries	B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties	D.2 Internally invoiced goods and services	E. Indirect costs					
	A.2 Natural persons under direct contract														
A.3 Seconded persons															
Forms of funding	Actual costs	Unit costs (usual accounting practices)	Unit costs <sup>7</sup>	Actual costs	Actual costs	Actual costs	Actual costs	Actual costs	Unit costs (usual accounting practices)	Flat-rate costs <sup>8</sup>					
	a1	a2	a3	b	c1	c2	c3	d1	d2	e = flat-rate * (a1 + a2 + a3 + b + c1 + c2 + c3 + d1 + d2)	f = a + b + c + d + e	U	g = f * U%	h	m
1 - NUKIB	960 000.00	0.00	0.00	0.00	70 000.00	65 000.00	310 000.00	2 500 000.00	0.00	273 350.00	4 178 350.00	50	2 089 175.00	2 089 175.00	2 089 175.00
1.1 - CSH	727 050.00	0.00	0.00	0.00	15 000.00	6 000.00	18 300.00	0.00	0.00	53 644.50	819 994.50	50	409 997.25	409 997.25	409 997.25
Σ consortium	1 687 050.00	0.00	0.00	0.00	85 000.00	71 000.00	328 300.00	2 500 000.00	0.00	326 994.50	4 998 344.50		2 499 172.25	2 499 172.25	2 499 172.25

<sup>1</sup> See Article 6 for the eligibility conditions. All amounts must be expressed in EUR (see Article 21 for the conversion rules).

<sup>2</sup> The consortium remains free to decide on a different internal distribution of the EU funding (via the consortium agreement; see Article 7).

<sup>3</sup> Indirect costs already covered by an operating grant (received under any EU funding programme) are ineligible (see Article 6.3). Therefore, a beneficiary/affiliated entity that receives an operating grant during the action duration cannot declare indirect costs for the year(s)/reporting period(s) covered by the operating grant, unless they can demonstrate that the operating grant does not cover any costs of the action. This requires specific accounting tools. Please immediately contact us via the EU Funding & Tenders Portal for details.

<sup>4</sup> See Data Sheet for the funding rate(s).

<sup>5</sup> This is the theoretical amount of the EU contribution to costs, if the reimbursement rate is applied to all the budgeted costs. This theoretical amount is then capped by the 'maximum grant amount'.

<sup>6</sup> The 'maximum grant amount' is the maximum grant amount decided by the EU. It normally corresponds to the requested grant, but may be lower.

<sup>7</sup> See Annex 2a 'Additional information on the estimated budget' for the details (units, cost per unit).

<sup>8</sup> See Data Sheet for the flat-rate.

## **ANNEX 2a**

### **ADDITIONAL INFORMATION ON UNIT COSTS AND CONTRIBUTIONS**

#### **SME owners/natural person beneficiaries without salary**

See [\*Additional information on unit costs and contributions \(Annex 2a and 2b\)\*](#)

ANNEX 4 DIGITAL EUROPE MGA — MULTI + MONO

FINANCIAL STATEMENT FOR [PARTICIPANT NAME] FOR REPORTING PERIOD [NUMBER]

Eligible <sup>1</sup> costs (per budget category)												EU contribution <sup>2</sup>					Revenues
Direct costs										Indirect costs	Total costs	EU contribution to eligible costs			Total requested EU contribution	Income generated by the action	
A. Personnel costs		B. Subcontracting costs	C. Purchase costs			D. Other cost categories			E. Indirect costs <sup>2</sup>	Funding rate % <sup>3</sup>		Maximum EU contribution <sup>4</sup>	Requested EU contribution				
A.1 Employees (or equivalent)		A.4 SME owners and natural person beneficiaries	B. Subcontracting	C.1 Travel and subsistence	C.2 Equipment	C.3 Other goods, works and services	D.X Financial support to third parties	D.2 Internally invoiced goods and services	[OPTION for PAC Grants for Procurement: D.3 PAC procurement costs]	E. Indirect costs							
A.2 Natural persons under direct contract																	
A.3 Seconded persons																	
Forms of funding	Actual costs	Unit costs (usual accounting practices)	Unit costs <sup>5</sup>	Actual costs	Actual costs	Actual costs	Actual costs	Actual costs	Unit costs (usual accounting practices)	[ Actual costs]	Flat-rate costs <sup>6</sup>						
	a1	a2	a3	b	c1	c2	c3	d1a	d2	[ d3]	e = flat-rate * (a1 + a2 + a3 + b + c1 + c2 + c3 + d1a + d2 (+ d3))	f = a+b+c+d+e	U	g = f*U%	h	m	n
XX – [short name beneficiary/affiliated entity]																	

The beneficiary/affiliated entity hereby confirms that:

The information provided is complete, reliable and true.

The costs and contributions declared are eligible (see Article 6).

The costs and contributions can be substantiated by adequate records and supporting documentation that will be produced upon request or in the context of checks, reviews, audits and investigations (see Articles 19, 20 and 25).

For the last reporting period: that all the revenues have been declared (see Article 22).

① Please declare all eligible costs and contributions, even if they exceed the amounts indicated in the estimated budget (see Annex 2). Only amounts that were declared in your individual financial statements can be taken into account lateron, in order to replace costs/contributions that are found to be ineligible.

<sup>1</sup> See Article 6 for the eligibility conditions. All amounts must be expressed in EUR (see Article 21 for the conversion rules).

<sup>2</sup> If you have also received an EU operating grant during this reporting period, you cannot claim indirect costs - unless you can demonstrate that the operating grant does not cover any costs of the action. This requires specific accounting tools. Please contact us immediately via the Funding & Tenders Portal for details.

<sup>3</sup> See Data Sheet for the reimbursement rate(s).

<sup>4</sup> This is the *theoretical* amount of EU contribution to costs that the system calculates automatically (by multiplying the reimbursement rates by the costs declared). The amount you request (in the column 'requested EU contribution') may be less.

<sup>5</sup> See Annex 2a 'Additional information on the estimated budget' for the details (units, cost per unit).

<sup>6</sup> See Data Sheet for the flat-rate.

## **ANNEX 5**

### **SPECIFIC RULES**

#### **CONFIDENTIALITY AND SECURITY (— ARTICLE 13)**

##### **Sensitive information with security recommendation**

Sensitive information with a security recommendation must comply with the additional requirements imposed by the granting authority.

Before starting the action tasks concerned, the beneficiaries must have obtained all approvals or other mandatory documents needed for implementing the task. The documents must be kept on file and be submitted upon request by the coordinator to the granting authority. If they are not in English, they must be submitted together with an English summary.

For requirements restricting disclosure or dissemination, the information must be handled in accordance with the recommendation and may be disclosed or disseminated only after written approval from the granting authority.

##### **EU classified information**

If EU classified information is used or generated by the action, it must be treated in accordance with the security classification guide (SCG) and security aspect letter (SAL) set out in Annex 1 and Decision 2015/444<sup>1</sup> and its implementing rules — until it is declassified.

Deliverables which contain EU classified information must be submitted according to special procedures agreed with the granting authority.

Action tasks involving EU classified information may be subcontracted only with prior explicit 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).

EU classified information may not be disclosed to any third party (including participants involved in the action implementation) without prior explicit written approval from the granting authority.

#### **ETHICS (— ARTICLE 14)**

##### **Ethics**

Actions involving activities raising ethics issues must be carried out in compliance with:

- ethical principles

---

<sup>1</sup> Commission Decision 2015/444/EC, Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

and

- applicable EU, international and national law, including the EU Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Supplementary Protocols.

The beneficiaries must pay particular attention to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of persons, the right to non-discrimination, the need to ensure protection of the environment and high levels of human health protection.

Before the beginning of an action task raising an ethical issue, the beneficiaries must have obtained all approvals or other mandatory documents needed for implementing the task, notably from any (national or local) ethics committee or other bodies such as data protection authorities.

The documents must be kept on file and be submitted upon request by the coordinator to the granting authority. If they are not in English, they must be submitted together with an English summary, which shows that the documents cover the action tasks in question and includes the conclusions of the committee or authority concerned (if any).

## **INTELLECTUAL PROPERTY RIGHTS (IPR) — BACKGROUND AND RESULTS — ACCESS RIGHTS AND RIGHTS OF USE (— ARTICLE 16)**

### **Definitions**

Access rights — Rights to use results or background.

Dissemination — The public disclosure of the results by appropriate means, other than resulting from protecting or exploiting the results, including by scientific or professional publications in any medium.

Exploit(ation) — The use of results in further innovation and deployment activities other than those covered by the action concerned, including among other things, commercial exploitation such as developing, creating, manufacturing and marketing a product or process, creating and providing a service, or in standardisation activities.

Fair and reasonable conditions — Appropriate conditions, including possible financial terms or royalty-free conditions, taking into account the specific circumstances of the request for access, for example the actual or potential value of the results or background to which access is requested and/or the scope, duration or other characteristics of the exploitation envisaged.

### **List of background — Background free from restrictions**

The beneficiaries must, where industrial and intellectual property rights (including rights of third parties) exist prior to the Agreement, establish a list of these pre-existing industrial and intellectual property rights, specifying the rights owners.

The coordinator must — before starting the action — submit this list to the granting authority.

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons, background that is subject to control or other restrictions by a country (or entity from a country) which is not one of the eligible countries or target countries set out in the call conditions and that impact the results (i.e. would make the results subject to control or restrictions) must not be used and must be explicitly excluded in the list of background — unless otherwise agreed with the granting authority.

### **Results free from restrictions**

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons, the beneficiaries must ensure that the results of the action are not subject to control or other restrictions by a country (or entity from a country) which is not one of the eligible countries or target countries set out in the call conditions — unless otherwise agreed with the granting authority.

### **Ownership of results**

Results are owned by the beneficiaries that generate them (unless the consortium agreement specifies another ownership regime).

### **Protection of results**

The beneficiaries must adequately protect their results — for an appropriate period and with appropriate territorial coverage — if protection is possible and justified, taking into account all relevant considerations, including the prospects for commercial exploitation, legitimate interests of the other beneficiaries and any other legitimate interests.

### **Exploitation of results**

Beneficiaries must — up to four years after the end of the action (see Data Sheet, Point 1) — use their best efforts to exploit their results directly or to have them exploited indirectly by another entity, in particular through transfer or licensing.

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons (and unless otherwise agreed with the granting authority), the beneficiaries must produce a significant amount of products, services or processes that incorporate results of the action or that are produced through the use of results of the action in the eligible countries or target countries set out in the call conditions.

Where the call conditions impose moreover a first exploitation obligation, the first exploitation must also take place in the eligible countries or target countries set out in the call conditions.

The beneficiaries must ensure that these obligations also apply to their affiliated entities, associated partners, subcontractors and recipients of financial support to third parties.

### **Transfers and licensing of results**

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons, the beneficiaries may not transfer ownership of their results or grant licences to third parties which are established in countries which are not eligible countries or target countries set out in the call conditions (or are controlled by such countries or entities



from such countries) — unless they have requested and received prior approval by the granting authority.

The request must:

- identify the specific results concerned
- describe in detail the new owner or licensee and the planned or potential exploitation of the results and
- include a reasoned assessment of the likely impact of the transfer or license on the security interests or EU strategic autonomy.

The granting authority may request additional information.

The beneficiaries must ensure that their obligations under the Agreement are passed on to the new owner or licensee and that this new owner or licensee has the obligation to pass them on in any subsequent transfer.

### **Access rights — Additional rights of use**

#### *Rights of use of the granting authority on results for information, communication, publicity and dissemination purposes*

The granting authority also has the right to exploit non-sensitive results of the action for information, communication, dissemination and publicity purposes, using any of the following modes:

- **use for its own purposes** (in particular, making them available to persons working for the granting authority or any other EU service (including institutions, bodies, offices, agencies, etc.) or EU Member State institution or body; copying or reproducing them in whole or in part, in unlimited numbers; and communication through press information services)
- **distribution to the public** in hard copies, in electronic or digital format, on the internet including social networks, as a downloadable or non-downloadable file
- **editing** or **redrafting** (including shortening, summarising, changing, correcting, cutting, inserting elements (e.g. meta-data, legends or other graphic, visual, audio or text elements), extracting parts (e.g. audio or video files), dividing into parts or use in a compilation)
- **translation**(including inserting subtitles/dubbing)in all official languages of EU
- **storage** in paper, electronic or other form
- **archiving** in line with applicable document-management rules
- the right to authorise **third parties** to act on its behalf or sub-license to third parties, including if there is licensed background, any of the rights or modes of exploitation set out in this provision
- **processing**, analysing, aggregating the results and **producing derivative works**

- **disseminating** the results in widely accessible databases or indexes (such as through ‘open access’ or ‘open data’ portals or similar repositories, whether free of charge or not).

The beneficiaries must ensure these rights of use for the whole duration they are protected by industrial or intellectual property rights.

If results are subject to moral rights or third party rights (including intellectual property rights or rights of natural persons on their image and voice), the beneficiaries must ensure that they comply with their obligations under this Agreement (in particular, by obtaining the necessary licences and authorisations from the rights holders concerned).

*Access rights for the granting authority and EU institutions, bodies, offices or agencies to results for policy purposes*

The beneficiaries must grant access to their results — on a royalty-free basis — to the granting authority, other EU institutions, bodies, offices or agencies, for developing, implementing and monitoring EU policies or programmes.

Such access rights are limited to non-commercial and non-competitive use.

*Access rights for the granting authority to results in case of a public emergency*

If requested by the granting authority in case of a public emergency, the beneficiaries must grant non-exclusive, world-wide licences to third parties — under fair and reasonable conditions — to use the results to address the public emergency.

*Access rights for third parties to ensure continuity and interoperability*

Where the call conditions impose continuity or interoperability obligations, the beneficiaries must make the results produced in the framework of the action available to the public (freely accessible on the Internet under open source licences).

**COMMUNICATION, DISSEMINATION AND VISIBILITY (— ARTICLE 17)**

**Communication and dissemination plan**

The beneficiaries must provide a detailed communication and dissemination plan, setting out the objectives, key messaging, target audiences, communication channels, social media plan, planned budget and relevant indicators for monitoring and evaluation.

**Dissemination of results**

The beneficiaries must disseminate their results as soon as feasible, in a publicly available format, subject to any restrictions due to the protection of intellectual property, security rules or legitimate interests.

They must upload the public **project results** to the Digital Europe Project Results platform, available through the Funding & Tenders Portal.

In addition, where the call conditions impose additional dissemination obligations, they must also comply with those.

**Additional communication activities**

The beneficiaries must engage in the following additional communication activities:

- **present the project** (including project summary, coordinator contact details, list of participants, European flag and funding statement and special logo and project results) on the beneficiaries' **websites** or **social media accounts**

## **SPECIFIC RULES FOR CARRYING OUT THE ACTION (— ARTICLE 18)**

### **Implementation in case of restrictions due to security or EU strategic autonomy**

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons, the beneficiaries must ensure that none of the entities that participate as affiliated entities, associated partners, subcontractors or recipients of financial support to third parties are established in countries which are not eligible countries or target countries set out in the call conditions (or are controlled by such countries or entities from such countries) — unless otherwise agreed with the granting authority.

The beneficiaries must moreover ensure that any cooperation with entities established in countries which are not eligible countries or target countries set out in the call conditions (or are controlled by such countries or entities from such countries) does not affect the security interests or EU strategic autonomy and avoids potential negative effects over security of supply of inputs critical to the action.

### **Specific rules for PAC Grants for Procurement**

When implementing innovative procurements in PAC Grants for Procurement, the beneficiaries must respect the following conditions:

- avoid any conflict of interest and comply with the principles of transparency, non-discrimination, equal treatment, sound financial management, proportionality and competition rules
- assign the ownership of the intellectual property rights under the contracts to the contractors (unless there are exceptional overriding public interests which are duly justified in Annex 1), with the right of the buyers to access results — on a royalty-free basis — for their own use and to grant (or to require the contractors to grant) non-exclusive licences to third parties to exploit the results for them — under fair and reasonable conditions — without any right to sub-license
- allow for all communications to be made in English (and any additional languages chosen by the beneficiaries)
- ensure that prior information notices, contract notices and contract award notices contain information on the EU funding and a disclaimer that the EU is not participating as contracting authority in the procurement
- allow for the award of multiple procurement contracts within the same procedure (multiple sourcing)
- for procurements involving classified information: apply the security rules set out in Annex 5 mutatis mutandis to the contractors and the background and results of the contracts

- where the call conditions restrict participation or control due to security or EU strategic autonomy reasons: apply the restrictions set out in Annex 5 mutatis mutandis to the contractors and the results under the contracts
- where the call conditions impose a place of performance obligation: ensure that the part of the activities that is subject to the place of performance obligation is performed in the eligible countries or target countries set out in the call conditions
- to ensure reciprocal level of market access: where the WTO Government Procurement Agreement (GPA) does not apply, ensure that the participation in tendering procedures is open on equal terms to bidders from EU Member States and all countries with which the EU has an agreement in the field of public procurement under the conditions laid down in that agreement, including all Horizon Europe associated countries. Where the WTO GPA applies, ensure that tendering procedures are also open to bidders from states that have ratified this agreement, under the conditions laid down therein.

### **Specific rules for Grants for Financial Support**

When implementing financial support to third parties in Grants for Financial Support, the beneficiaries must respect the following conditions:

- avoid any conflict of interest and comply with the principles of transparency, non-discrimination and sound financial management
- for the selection procedure and criteria:
  - publish open calls widely (including on the Funding & Tenders Portal and the beneficiaries' websites)
  - keep open calls open for at least two months
  - inform recipients of call updates (if any) and the outcome of the call (list of selected projects, amounts and names of selected recipients)

### **Specific rules for JU actions**

JU actions must contribute to the long-term implementation of the JU partnership, including the JU Strategic Research and Innovation Agenda, the JU objectives and the exploitation of research and innovation results.

Moreover, when implementing JU actions, the members and contributing partners of the Joint Undertaking must fulfil their obligations regarding contributions to the Joint Undertaking:

- the description of the action in Annex 1 must include, for beneficiaries, affiliated entities, associated partners or other participants or third parties which are members or contributing partners, the estimated contributions to the action, i.e.:
  - in-kind contributions to operational activities ('IKOP'; if applicable)
  - in-kind contributions to additional activities linked to the action ('IKAA'; if applicable)
  - financial contributions ('FC'; if applicable)

- the contributions must be reported during the implementation of the action in the Portal Continuous Reporting tool
- at the end of the action, the members and contributing partners that have not received funding under the grant must ensure that financial and in-kind contributions of EUR 430 000 or more (see Article 21) are supported by statements of contributions (CS) and certificates on the statements of contributions (CCS) which fulfil the following conditions:
  - be provided by a qualified approved external auditor which is independent and complies with Directive 2006/43/EC (or for public bodies: by a competent independent public officer)
  - the verification must be carried out according to the highest professional standards to ensure that the statements of contributions comply with the provisions under the Agreement and the applicable JU Regulation, that the contributions cover activities that are part of the action and that they have not been reimbursed by the grant
- contributions must comply with the following conditions:
  - costs covered by financial contributions cannot be claimed for reimbursement under the JU grant.

The beneficiaries must comply with the additional IPR, dissemination and exploitation obligations set out in the call conditions (Article 16 and Annex 5), in particular:

- for all JU grants: the granting authority right to object to transfers or licensing also applies to results generated by beneficiaries not having received funding under the grant.

In addition to the obligations set out in Article 17, communication and dissemination activities as well as infrastructure, equipment or major results funded under JU actions must moreover display the Joint Undertaking's special logo:



**EuroHPC**  
Joint Undertaking



and the following text:

“The project is supported by the [insert JU name] and its members *[OPTION for actions with national contribution top-ups: (including top-up funding by [name of the national funding authority])]*.”

For EuroHPC and Chips JU grants, the beneficiaries must respect the following conditions when implementing actions with national contribution top-ups from Participating States:

- the beneficiaries must ensure visibility of the national contributions (see below)
- the payment deadlines for prefinancing, interim or final payments are automatically suspended if a national funding authority is late with its payments to the Joint Undertaking for the national contribution top-up
- the European Anti-Fraud Office (OLAF), European Public Prosecutor's Office (EPPO), European Court of Auditors (ECA), the National Court of Auditors and other national authorities can exercise their control rights on the project implementation and costs declared, including for the national contribution top-up.

### **Specific rules for blending operations**

When implementing blending operations, the beneficiaries acknowledge and accept that:

- the grant depends on the approved financing from the Implementing Partner and/or public or private investors for the project
- they must inform the granting authority both about the approval for financing and the financial close — within 15 days
- the payment deadline for the first prefinancing is automatically suspended until the granting authority is informed about the approval for financing
- both actions will be managed and monitored in parallel and in close coordination with the Implementing Partner, in particular:
  - all information, data and documents (including the due diligence by the Implementing Partner and the signed agreement) may be exchanged and may be relied on for the management of the other action (if needed)
  - issues in one action may impact the other (e.g. suspension or termination in one action may lead to suspension also of the other action; termination of the grant will normally suspend and exit from further financing and vice versa, etc.)
- the granting authority may disclose confidential information also to the Implementing Partner.



Digitally sealed by the European Commission  
Date: 2025.05.29 08:25:28 CEST

This electronic receipt is a digitally signed version of the document submitted by your organisation. Both the content of the document and a set of metadata have been digitally sealed.

This digital signature mechanism, using a public-private key pair mechanism, uniquely binds this eReceipt to the modules of the Funding & Tenders Portal of the European Commission, to the transaction for which it was generated and ensures its full integrity. Therefore a complete digitally signed trail of the transaction is available both for your organisation and for the issuer of the eReceipt.

Any attempt to modify the content will lead to a break of the integrity of the electronic signature, which can be verified at any time by clicking on the eReceipt validation symbol.

More info about eReceipts can be found in the FAQ page of the Funding & Tenders Portal.

(<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq>)