



GRANT AGREEMENT

Project 101226928 — NCCEE2

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':

RIIGI INFOSUSTEEMI AMET (RIA), PIC 953382834, established in PARNU MNT 139 A, Tallinn 15169, Estonia,

and the following other beneficiaries, if they sign their 'accession form' (see Annex 3 and Article 40):

2. **ETTEVOTLUSE JA INNOVATSIOONI SIHTASUTUS (EBIA)**, PIC 971995291, established in SEPISE 7, TALLINN 11415, Estonia,

3. **SIHTASUTUS TALLINNA TEADUSPARK TEHNOPOL (TEHNOPOL)**, PIC 999764257, established in TEADUSPARAGI 6/1, TALLINN 12618, Estonia,

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 action¹

Annex 2 Estimated budget for the action

Annex 2a Additional information on unit costs and contributions (if applicable)

Annex 3 Accession forms (if applicable)²

Annex 3a Declaration on joint and several liability of affiliated entities (if applicable)³

Annex 4 Model for the financial statements

Annex 5 Specific rules (if applicable)

¹ Template published on [Portal Reference Documents](#).

² Template published on [Portal Reference Documents](#).

³ 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.....23

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.....25

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.....	26
10.3 Pillar-assessed participants.....	27
SECTION 2 RULES FOR CARRYING OUT THE ACTION.....	28
ARTICLE 11 — PROPER IMPLEMENTATION OF THE ACTION.....	29
11.1 Obligation to properly implement the action.....	29
11.2 Consequences of non-compliance.....	29
ARTICLE 12 — CONFLICT OF INTERESTS.....	29
12.1 Conflict of interests.....	29
12.2 Consequences of non-compliance.....	29
ARTICLE 13 — CONFIDENTIALITY AND SECURITY.....	29
13.1 Sensitive information.....	29
13.2 Classified information.....	30
13.3 Consequences of non-compliance.....	30
ARTICLE 14 — ETHICS AND VALUES.....	30
14.1 Ethics.....	31
14.2 Values.....	31
14.3 Consequences of non-compliance.....	31
ARTICLE 15 — DATA PROTECTION.....	31
15.1 Data processing by the granting authority.....	31
15.2 Data processing by the beneficiaries.....	31
15.3 Consequences of non-compliance.....	32
ARTICLE 16 — INTELLECTUAL PROPERTY RIGHTS (IPR) — BACKGROUND AND RESULTS — ACCESS RIGHTS AND RIGHTS OF USE.....	32
16.1 Background and access rights to background.....	32
16.2 Ownership of results.....	32
16.3 Rights of use of the granting authority on materials, documents and information received for policy, information, communication, dissemination and publicity purposes.....	32
16.4 Specific rules on IPR, results and background.....	33
16.5 Consequences of non-compliance.....	34
ARTICLE 17 — COMMUNICATION, DISSEMINATION AND VISIBILITY.....	34
17.1 Communication — Dissemination — Promoting the action.....	34
17.2 Visibility — European flag and funding statement.....	34
17.3 Quality of information — Disclaimer.....	35

17.4	Specific communication, dissemination and visibility rules.....	35
17.5	Consequences of non-compliance.....	35
ARTICLE 18 — SPECIFIC RULES FOR CARRYING OUT THE ACTION.....		35
18.1	Specific rules for carrying out the action.....	35
18.2	Consequences of non-compliance.....	35
SECTION 3 GRANT ADMINISTRATION.....		35
ARTICLE 19 — GENERAL INFORMATION OBLIGATIONS.....		35
19.1	Information requests.....	35
19.2	Participant Register data updates.....	36
19.3	Information about events and circumstances which impact the action.....	36
19.4	Consequences of non-compliance.....	36
ARTICLE 20 — RECORD-KEEPING.....		36
20.1	Keeping records and supporting documents.....	36
20.2	Consequences of non-compliance.....	37
ARTICLE 21 — REPORTING.....		38
21.1	Continuous reporting.....	38
21.2	Periodic reporting: Technical reports and financial statements.....	38
21.3	Currency for financial statements and conversion into euros.....	39
21.4	Reporting language.....	39
21.5	Consequences of non-compliance.....	39
ARTICLE 22 — PAYMENTS AND RECOVERIES — CALCULATION OF AMOUNTS DUE.....		39
22.1	Payments and payment arrangements.....	39
22.2	Recoveries.....	40
22.3	Amounts due.....	40
22.4	Enforced recovery.....	45
22.5	Consequences of non-compliance.....	46
ARTICLE 23 — GUARANTEES.....		46
23.1	Prefinancing guarantee.....	46
23.2	Consequences of non-compliance.....	47
ARTICLE 24 — CERTIFICATES.....		47
24.1	Operational verification report (OVR).....	47
24.2	Certificate on the financial statements (CFS).....	47
24.3	Certificate on the compliance of usual cost accounting practices (CoMUC).....	47
24.4	Systems and process audit (SPA).....	48
24.5	Consequences of non-compliance.....	48

ARTICLE 25 — CHECKS, REVIEWS, AUDITS AND INVESTIGATIONS — EXTENSION OF FINDINGS.....	48
25.1 Granting authority checks, reviews and audits.....	48
25.2 European Commission checks, reviews and audits in grants of other granting authorities.....	50
25.3 Access to records for assessing simplified forms of funding.....	50
25.4 OLAF, EPPO and ECA audits and investigations.....	50
25.5 Consequences of checks, reviews, audits and investigations — Extension of results of reviews, audits or investigations.....	50
25.6 Consequences of non-compliance.....	52
ARTICLE 26 — IMPACT EVALUATIONS.....	52
26.1 Impact evaluation.....	52
26.2 Consequences of non-compliance.....	52
CHAPTER 5 CONSEQUENCES OF NON-COMPLIANCE.....	52
SECTION 1 REJECTIONS AND GRANT REDUCTION.....	52
ARTICLE 27 — REJECTION OF COSTS AND CONTRIBUTIONS.....	52
27.1 Conditions.....	52
27.2 Procedure.....	53
27.3 Effects.....	53
ARTICLE 28 — GRANT REDUCTION.....	53
28.1 Conditions.....	53
28.2 Procedure.....	53
28.3 Effects.....	54
SECTION 2 SUSPENSION AND TERMINATION.....	54
ARTICLE 29 — PAYMENT DEADLINE SUSPENSION.....	54
29.1 Conditions.....	54
29.2 Procedure.....	54
ARTICLE 30 — PAYMENT SUSPENSION.....	54
30.1 Conditions.....	54
30.2 Procedure.....	55
ARTICLE 31 — GRANT AGREEMENT SUSPENSION.....	55
31.1 Consortium-requested GA suspension.....	56
31.2 EU-initiated GA suspension.....	56
ARTICLE 32 — GRANT AGREEMENT OR BENEFICIARY TERMINATION.....	57
32.1 Consortium-requested GA termination.....	57
32.2 Consortium-requested beneficiary termination.....	58
32.3 EU-initiated GA or beneficiary termination.....	59

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

DATA SHEET

1. General data

Project summary:

Project summary
<p>NCCEE2 is the next step of NCCEE project, moving towards a more capable cybersecurity community, a more sustainable impact in building those capabilities in Estonia and contributing to development of the cybersecurity sector. Building on the success of the activities of the previous, deployment oriented NCCEE project, it is paramount to continue on the path of advancing capabilities across the cybersecurity sector in Estonia. Moving from individual projects to a culture of innovation and capacity building to keep Estonia and Europe safe, NCCEE2 has the following objectives: 1. Creating sustained impact in capacity building in cybersecurity industry, research and technology alongside the cybersecurity community through events, knowledge sharing, sustainable innovation programs and facilitation of collaboration; 2. Promoting and encouraging a culture of innovation in cybersecurity, including increasing practical implementation of research outcomes, facilitating the participation in cross-border projects and entrepreneurship; 3. Increasing the number of specialists and youth acquiring knowledge and training in the field of cybersecurity, with a special focus on women and girls, while taking into account the needs of the cybersecurity community; 4. Promoting and supporting the uptake and dissemination of state-of-the-art cybersecurity solutions by all actors in society, with special attention paid to small and medium sized enterprises. NCCEE2 aims to enhance the existing capabilities of the Estonian and European cybersecurity community, guiding them towards market opportunities and future-proof solutions. The NCCEE2 consortium will leverage the experience from the NCCEE deployment project to expand the scope and focus on the long-term viability of the local National Coordination Centre, supporting the mission and strategic goals of the European Cybersecurity Competence Centre and Network of NCCs.</p>

Keywords:

- Cybersecurity
- Community, skills, technology, research, national and international cooperation, business development

Project number: 101226928

Project name: Cybersecurity Community Building and Continuation of the Estonian Coordination Centre Activities

Project acronym: NCCEE2

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 April 2025

Project end date: 31 March 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	RIA	RIIGI INFOSUSTEEMI AMET	EE	953382834	2 282 438.40	1 141 219.20
2	BEN	EBIA	ETTEVOTLUSE JA INNOVATSIOONI SIHTASUTUS	EE	971995291	1 605 000.00	802 500.00
3	BEN	TEHNOPOL	SIHTASUTUS TALLINNA TEADUSPARK TEHNOPOL	EE	999764257	1 476 600.00	738 300.00

N°	Role	Short name	Legal name	Ctry	PIC	Total eligible costs (BEN and AE)	Max grant amount
Total						5 364 038.40	2 682 019.20

Coordinator:

- RIIGI INFOSUSTEEMI AMET (RIA)

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)
5 364 038.40	50	2 682 019.20	2 682 019.20

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)	2 145 615.36	n/a	1 - RIA	n/a
			2 - EBIA	n/a
			3 - TEHNOPOL	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:

EE221010220027690221 EEUHEE2XXXX

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 190 of EU Financial Regulation 2024/2509⁴ 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(38) of EU Financial Regulation 2024/2509, i.e. non-financial resources made available free of charge by third parties.

⁴ For the definition, see Article 190 Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast) ('EU Financial Regulation') (OJ L, 2024/2509, 26.9.2024): "**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 138(1) and 143(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".

Fraud — Fraud within the meaning of Article 3 of EU Directive 2017/1371⁵ and Article 1 of the Convention on the protection of the European Communities' financial interests, drawn up by the Council Act of 26 July 1995⁶, 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 2988/95⁷.

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 138(1)(c) of EU Financial Regulation 2024/2509⁸.

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 **101226928 — NCCEE2** ('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

⁵ 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).

⁶ OJ C 316, 27.11.1995, p. 48.

⁷ 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).

⁸ 'Professional misconduct' includes, in particular, the following: violation of ethical standards of the profession; wrongful conduct with impact on professional credibility; breach of generally accepted professional ethical standards; false declarations/misrepresentation of information; participation in a cartel or other agreement distorting competition; violation of IPR; attempting to influence decision-making processes by taking advantage, through misrepresentation, of a conflict of interests, or to obtain confidential information from public authorities to gain an advantage; incitement to discrimination, hatred or violence or similar activities contrary to the EU values where negatively affecting or risking to affect the performance of a legal commitment.

The grant is an action grant⁹ which takes the form of a budget-based mixed actual cost grant (i.e. a 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)¹⁰ 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

⁹ 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”.

¹⁰ See Article 125 EU Financial Regulation 2024/2509.



- other changes require an amendment or simplified approval, if specifically provided for in Article 6.2
- flexibility caps: not applicable.

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 enterprises¹¹ 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).

¹¹ 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.

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.

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 grant¹² 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.

¹² 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".

6.4 Consequences of non-compliance

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’¹³ (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:

¹³ For the definition, see Article 190(2) EU Financial Regulation 2024/2509: “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 internal organisation of the consortium
- 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

Not applicable

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/EC¹⁴
- 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/EC¹⁵
- for the controls under Article 25: to allow for the checks, reviews, audits and investigations

¹⁴ 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 (OJ L 157, 9.6.2006, p. 87).

¹⁵ 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 (OJ L 157, 9.6.2006, p. 87).

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 157 EU Financial Regulation 2024/2509).

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 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 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 2015/444¹⁶ 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

¹⁶ 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).

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

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 2018/1725¹⁷.

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 2016/679¹⁸).

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

¹⁷ 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).

¹⁸ 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).

- 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.

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 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:

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

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:

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

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 2024/2509.

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 2015/2366¹⁹ applies.

¹⁹ 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).

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 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/EC²⁰ (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

²⁰ 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 (OJ L 157, 9.6.2006, p. 87).

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:

- (a) be provided by a qualified approved external auditor which is independent and complies with Directive 2006/43/EC²¹ (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.

²¹ 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 (OJ L 157, 9.6.2006, p. 87).

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 (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 883/2013²² and No 2185/96²³
- 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 263 of EU Financial Regulation 2024/2509.

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

²² 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).

²³ 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 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).

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), failure to cooperate with checks, reviews, audits and investigations, 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), failure to cooperate with checks, reviews, audits and investigations, 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), failure to cooperate with checks, reviews, audits and investigations, 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), failure to cooperate with checks, reviews, audits and investigations, 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 137 to 148 EU Financial Regulation 2024/2509 and Articles 4 and 7 of Regulation 2988/95²⁴).

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

²⁴ 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).

- 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.

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 1182/71²⁵, 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).

²⁵ 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).

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.

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:	101226928
Project name:	Cybersecurity Community Building and Continuation of the Estonian Coordination Centre Activities
Project acronym:	NCCEE2
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 April 2025
Project duration:	48 months

TABLE OF CONTENTS

Project summary3

List of participants 3

List of work packages4

Staff effort 15

List of deliverables16

List of milestones (outputs/outcomes) 29

List of critical risks 30

Project reviews 32

PROJECT SUMMARY

Project summary

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.

Use the project summary from your proposal.

NCCEE2 is the next step of NCCEE project, moving towards a more capable cybersecurity community, a more sustainable impact in building those capabilities in Estonia and contributing to development of the cybersecurity sector. Building on the success of the activities of the previous, deployment oriented NCCEE project, it is paramount to continue on the path of advancing capabilities across the cybersecurity sector in Estonia. Moving from individual projects to a culture of innovation and capacity building to keep Estonia and Europe safe, NCCEE2 has the following objectives:

1. Creating sustained impact in capacity building in cybersecurity industry, research and technology alongside the cybersecurity community through events, knowledge sharing, sustainable innovation programs and facilitation of collaboration;
2. Promoting and encouraging a culture of innovation in cybersecurity, including increasing practical implementation of research outcomes, facilitating the participation in cross-border projects and entrepreneurship;
3. Increasing the number of specialists and youth acquiring knowledge and training in the field of cybersecurity, with a special focus on women and girls, while taking into account the needs of the cybersecurity community;
4. Promoting and supporting the uptake and dissemination of state-of-the-art cybersecurity solutions by all actors in society, with special attention paid to small and medium sized enterprises.

NCCEE2 aims to enhance the existing capabilities of the Estonian and European cybersecurity community, guiding them towards market opportunities and future-proof solutions. The NCCEE2 consortium will leverage the experience from the NCCEE deployment project to expand the scope and focus on the long-term viability of the local National Coordination Centre, supporting the mission and strategic goals of the European Cybersecurity Competence Centre and Network of NCCs.

LIST OF PARTICIPANTS

PARTICIPANTS

Grant Preparation (Beneficiaries screen) — Enter the info.

Number	Role	Short name	Legal name	Country	PIC
1	COO	RIA	RIIGI INFOSUSTEEMI AMET	EE	953382834
2	BEN	EBIA	ETTEVOTLUSE JA INNOVATSIOONI SIHTASUTUS	EE	971995291
3	BEN	TEHNOPOL	SIHTASUTUS TALLINNA TEADUSPARK TEHNOPOL	EE	999764257

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	Management	1 - RIA	96.00	1	48	D1.1 – Revised Gender Action Plan (GAP) D1.2 – Quality Plan D1.3 – Data Management Plan D1.4 – Risk Management Plan D1.5 – Annual Report based on KPIs I D1.6 – Annual Report based on KPIs II D1.7 – Annual Report based on KPIs III D1.8 – Annual Report based on KPIs IV
WP2	Boosting Cybersecurity Entrepreneurship	1 - RIA	75.00	1	48	D2.1 – CyberAccelerator program design D2.2 – Updated Methodology for CyberTransformation I D2.3 – Updated Methodology for CyberTransformation II D2.4 – Implemented Acceleration Program I D2.5 – Implemented Acceleration Program II D2.6 – Implemented Acceleration Program III
WP3	Research, Development and Innovation in Cybersecurity	1 - RIA	24.00	1	48	D3.1 – Grant System Design D3.2 – Grant Coordination and Management Plan D3.3 – Cyber Innovation diplomacy & pathway to crossborder projects strategy D3.4 – Digital Innovation and Diplomacy Report

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
						D3.5 – Compendium of results of CyberInnovation Grants I D3.6 – Compendium of results of CyberInnovation Grants II
WP4	Next Generation of Cybersecurity Professionals	1 - RIA	48.00	1	48	D4.1 – Internships and Scholarship Programs Design D4.2 – A set of Policy Papers I D4.3 – A set of Policy Papers II D4.4 – A set of Policy Papers III D4.5 – A set of Policy Papers IV D4.6 – CyberWizards I D4.7 – CyberWizards II D4.8 – Internships and Scholarship Programs Implementations I D4.9 – Internships and Scholarship Programs Implementations II
WP5	Exploitation, Dissemination and Communication	1 - RIA	57.00	1	48	D5.1 – Dissemination and Communication Plan D5.2 – Community engagement overview I D5.3 – Community engagement overview II D5.4 – Exploitation Report D5.5 – Final Report on Dissemination and Communications activities and Events compendium

Work package WP1 – Management

Work Package Number	WP1	Lead Beneficiary	1 - RIA
Work Package Name	Management		
Start Month	1	End Month	48

Objectives

The Management work package aims to:

- Ensure optimal use of resources including time, budget, and personnel.
- Identify potential risks early and establish mitigation strategies.
- Maintain high standards in deliverables to meet stakeholder expectations.
- Adhere to project timelines and milestones to ensure timely completion.
- Maintain clear and ongoing communication with all stakeholders.

Description**T1.1 Management of Project NCCEE2****Sub-Task (ST)1.1.1 Overall Management:**

A practical and efficient management structure will be established to ensure the successful implementation of the project, taking into account the processes that worked well during the previous project.

The Project Coordinator (PC) will oversee the management and upkeep of the web-based management system which is already in place, as part of the pilot NCCEE project. The PC utilizes webbased project platforms to manage project activities. The PC ensures that project tasks are completed on schedule in accordance with agreements with other parties, that deliverable documents are prepared and submitted according to plan and that any necessary modifications are communicated in advance, allowing for adequate time to respond appropriately.

The project will be overseen by a Project Steering Committee (SC), composed of team members from RIA, EIS, and Tehnopol. These will be experienced team members who have worked on the pilot NCCEE project.

The SC will manage key decisions regarding project execution, monitor progress, address challenges, and promote effective communication and knowledge sharing among stakeholders.

As part of the overall management, a Gender Action Plan which was already created for the pilot NCCEE project will be reviewed, and put forth for approval by the SC to implement the project's gender strategy. A designated Gender Action Officer will be appointed to manage and coordinate these efforts, reporting to both the PC and the SC.

Sub-Task 1.1.2 Collaboration and Coordination within Consortium:

The SC will generally meet every month, but meetings will be scheduled as needed. The meeting topics and decisions will be compiled into a memo, which is accessible to all participants of the meeting.

A cooperation agreement will be established with RIA and 2 consortium partners in order to outline the obligations and the framework for collaboration.

If necessary, additional members from Tehnopol, EIS, or RIA, such as Work Package Leaders, will be invited to participate in Project Steering Committee meetings to deliberate or formulate more precise plans or reviews on specific topics.

Sub-Task (ST) 1.1.3 Communication with Granting Authority:

The PC will handle communication and information exchange with the Granting Authority (ECCC).

Responsibilities include: 1) submitting regular, timely reports on administrative and financial progress, 2) ensuring all partners contribute to ongoing financial and final reports for the ECCC, and 3) informing ECCC of any significant changes and communicating with ECCC to ensure that project activities are carried out according to the requirements.

T1.2 Financial Management

PC will share information and guidelines with the partners in order to comply with the necessary financial administration and procurement practices required by Digital Europe, maintaining accurate records for all expenditures.

The PC will provide assistance to partners related to fund eligibility and EC reporting guidelines, such as contractual, legal, and technical reporting.

To address any questions related to fund eligibility and ECCC reporting guidelines, such as contractual, legal, and technical reporting, PC will communicate directly with partners. Furthermore, PC will thoroughly review the costs reported by partners, request clarifications when needed, and validate the eligibility of these costs according to ECCC regulations, including the relevant audit certificates. If any irregularities are detected, PC will promptly notify partners and provide guidance on the required corrective actions.

T1.3 Risk and Data Management

Sub-Task 1.3.1 Risk Management:

The PC will be assisted by SC in managing risks by reviewing the risk profile biannually. A risk management plan will be created, which will outline the process for identifying, assessing, and managing risks associated with the project, as well as defining appropriate measures for risk prevention.

During Project Steering Committee meetings, risks will be reviewed and decisions will be made based on the situation, ensuring that the project remains on schedule and avoids delays.

Sub-Task 1.3.2 Data Management:

Secure Data management will be carried out, ensuring compliance with data protection requirements during data sharing and storage.

Throughout the project, we will ensure compliance with all relevant legal frameworks to manage personal and health data in accordance with privacy and ethical standards. We will obtain ethical approval and informed consent from participants, ensuring they understand how their data will be used and their rights to access, withdraw, or delete it. We plan to anonymize and pseudonymize the data, store it securely on encrypted servers, and restrict access to authorized personnel only. Data will be used exclusively for the project's purposes, with any secondary use requiring explicit consent. The data will be retained for the necessary duration and securely deleted once the retention period expires. The data protection officer will oversee ongoing compliance and ensure that all processes align with data protection standards.

PC will develop a data management plan outlining the necessary data storage facilities for safe handling and storage.

Work package WP2 – Boosting Cybersecurity Entrepreneurship

Work Package Number	WP2	Lead Beneficiary	1 - RIA
Work Package Name	Boosting Cybersecurity Entrepreneurship		
Start Month	1	End Month	48

Objectives

- To foster the creation and development of new state-of-the-art cybersecurity solutions in the cybersecurity market sector.
- To increase the competition among existing cybersecurity service providers in the Estonian market and as such foster the development of new and innovative tools.
- To provide financial support for the adoption and widespread use of the state-of-the-art cybersecurity solutions.

Description

T2.1 Cybersecurity Acceleration Program

As the regulation establishing the ECCC states, the EU “suffers from insufficient investment and limited access to cybersecurity knowhow, skills and facilities, and few Union cybersecurity research and innovation outcomes are translated into marketable solutions or widely deployed across the economy”. Therefore this task will provide a continuation and a development of the accelerator project from the initial NCCEE project which contributed to the development of 15 early-stage cybersecurity start-up companies between 2023 and 2024.

The 7-month accelerator program will continue from the initial NCCEE pilot program and will sharpen the focus on cybersecurity innovation. The program will continue to be designed for the creation and development of new start-up companies who would provide state-of-the-art cybersecurity solutions for the market uptake. The accelerator program

will focus heavily on research and innovation in cybersecurity, but the goal is to transform research-intensive solutions (TRL level 5+) to market. The accelerator program will be open to students, researchers, start-up entrepreneurs and spin-offs from existing companies. The criteria for the applicants will be based on trends, research and market needs and will focus heavily on innovation.

One acceleration program per year will be implemented once a year for three cycles (3 years of the 4-year project) to ensure that the teams participating can complete their proposed projects and to make sure the community is continuously aware of the program and the attention paid to the innovation side of cybersecurity. Compared to the initial accelerator program, the next three cohorts will be smaller to ensure more attention to individual teams. A total of 18 startup companies will be supported during the 3-year period to bring new cybersecurity products and services to the market. The tentative starting dates for each batch will be 10/2025, 10/2026 and 10/2027 and will run until April of the successive year.

The accelerator program is built and implemented on the principle of sprints, where group activities alternate with individual activities. A dedicated program manager will ensure the participants will complete their individual projects and keep them on track throughout the program period. Lead mentors, business mentors and cybersecurity mentors will guide the teams based on individual needs.

Companies participating in the accelerator program will go through the following development cycles:

1. Defining the client's problem and designing a value proposition based on the need (product-market-customer-fit);
2. Business model and team building;
3. Product development and prototyping (build-measure-learn);
4. Intellectual property;
5. Investor readiness and other financing opportunities;
6. Go-to-market strategies and pilot preparations.

The task relies also heavily on the overall community driven mission of the NCCEE2 project, especially through the creation of the Cybersecurity Mentor Pool proposed in Task 2.3. As start-ups grow, the business side is needed throughout, but the possibility of the existing community members to contribute in mentoring new and upcoming colleagues (or future competitors) creates a community mission not seen in the Estonian start-up ecosystem.

T2.2 Development Grants for start-ups in the Acceleration Program

Development Grants in the value of 60 000€ per startup can be acquired by the start-ups participating in the acceleration program. This funding is provided through a competitive process and the funding is aimed to create, develop and disseminate innovative and state-of-the-art cybersecurity solutions.

These grants aim to strengthen cybersecurity capabilities of stakeholders and lead to uptake of novel cybersecurity solutions, strengthening Estonian Cybersecurity Community and potentially contributing to the strategic autonomy of the European Union.

The grants are provided to the participants of the Cybersecurity Accelerator Program described in Task 2.1 and will be used for various elements of business and product development to build, validate, and test the products or services and to develop the business model and implement go-to-market strategies. The Accelerator will be hosting periodic events to showcase project prototypes, invite feedback, and motivate start-ups to progress with their activities.

CyberAccelerator will be a helpful tool to encourage entrepreneurship within the cybersecurity field, leading also to increased capacity of future cross-border projects.

T2.3 CyberSecurity Mentor Pool

To provide expertise to start-ups in Estonia and abroad, NCCEE2 will establish a network of experts to mentor SMEs, start-ups, and researchers, enhancing cybersecurity skills and fostering collaboration.

The mentors will come from the community members in Estonia and will provide expertise and contribute actively to the strategic tasks related to relevant national and regional challenges for cybersecurity in different sectors. They can also facilitate interdisciplinary and cross-border collaboration on EU-funded projects, helping to establish synergies with relevant activities at national, regional and local levels. Also when other accelerator programs or cybersecurity skills programs ask for Estonian expertise, the network can provide access.

Mentors can also help in promoting and disseminating relevant outcomes of various NCCEE funded projects to third parties at national and international level.

T2.4 Cyber Transformation methodology development and maintenance

This task will continue the development of a simple, commercially logical, and commercially accepted methodology for providing cybersecurity posture assessment. The methodology was initially created during the NCCEE deployment project and has since had an impact of increasing competition in Estonia (bringing down the cost of the service and allowing for more actors to come to the market) and raising awareness among the Estonian companies who otherwise would struggle to procure these services.

The goal of this Methodology is to provide harmonization of service providers' approach to Cybersecurity services provision. According to the methodology an evaluation must be given to networks, firewalls, servers, risk analyses and awareness of the employees and the management board about cyber hygiene and security. The service providers conducting the evaluation and mapping will follow the methodology drawn up by RIA. They will do the preliminary work of assessing the organization's footprint from outside, visit the organization on site, conduct interviews, perform scans of the organisation's networks, and present the final results to the management board.

As the cybersecurity landscape is constantly changing, this task will ensure that two new versions will be developed over a 4 year period, taking into account the feedback received from the community members who are providing those services and the specialists from the field. The methodology versions will include instruction manuals, examples and templates for the service providers, the customers and third party evaluators. The new versions will be translated into English for dissemination and uptake from other NCCs and competent authorities.

Work package WP3 – Research, Development and Innovation in Cybersecurity

Work Package Number	WP3	Lead Beneficiary	1 - RIA
Work Package Name	Research, Development and Innovation in Cybersecurity		
Start Month	1	End Month	48

Objectives

- To provide financial support for cybersecurity innovation, state-of-the-art tools, products and services
- To promote, encourage and facilitate the participation of Estonian community members in cross-border projects and cybersecurity actions funded through EU programs
- To provide technical assistance to stakeholders in their application phase for projects managed by the ECCC
- To foster collaboration between the private sector and research institutions in Estonia and Europe
- To enhance the involvement of Estonian companies and foster international partnerships, strengthening Estonia's position as a cybersecurity hub and developing local skills and expertise in the field.
- Collaborating with the European network of NCCs to share knowledge and experience, between NCCs and the Estonian cybersecurity community.

Description

T3.1 Cybersecurity Research Grants and Partnerships

NCCEE2 will design and operate a program to distribute innovation and development grants in order to promote the creation or development of state-of-the-art cybersecurity solutions. These grants will work in synergy with the overall goal of the NCCEE2: to increase cooperation between the private sector, the researchers and the possible end-users of cybersecurity solutions. This grant program will also steer the Estonian cybersecurity community towards the Digital Europe Programme Cybersecurity goals as the topics for the calls will be aligned with the DEP work programme 2025-2027.

The program will provide competitive grants from 60 000 € to 100 000 € for new scientific discovery, product and service development in cybersecurity over 12-24 months with at least three cut-off dates. This task will rely on industry-academia cooperation, as every consortium applying for grants should include both businesses as well as academic entities.

We foresee at least three general topics for grants, aligned with the DEP WP 2025-2027 and distributed between the cut-off dates in 2025 and 2026 for the projects to be completed by 2027 and 2028. We have planned for at least 3 cut-off dates for these projects, each time selecting 5-6 projects to be funded and will initially propose the following topics:

- 10/2025 for the topic “Cybersecurity automation”
- 3/2026 for the topic “AI use in cybersecurity”
- 6/2026 for the topic “Tools and strategies for the transition to quantum-safe cryptographic algorithms”

These topics and cut-off dates are subject to change based on feedback from the community members or developments in the design phase of the grants.

We initially envision that the grants could be used for

- Creating and testing prototypes
- The technological development, testing and demonstration of components necessary for the products
- Product testing and industrial experiments, feasibility studies
- Consultations and registering a patent, utility model or an industrial design solution
- Accreditation, certification, standardization, metrology etc.
- Hiring cybersecurity doctoral students at private companies and supporting their research goals.

Over the 48 months of the project we foresee at least 18 projects being funded. As the projects will require a consortium to be formed, we anticipate the Estonian research entities (universities and research-heavy organizations) contributing to multiple consortia.

Grant conditions will require R&D beneficiaries to produce public case studies or demonstration videos to make research outcomes accessible and understandable to the broader cybersecurity community to stimulate further innovation. The collaboration between industry and academia will provide for research papers that could benefit the research community and facilitate further discovery.

The application process for the grants will be designed in a similar manner to the process required for European grants, but on a lower level of bureaucracy to facilitate higher participation rates. This will encourage the beneficiaries to “practice” the application process to participate in pan-European project calls.

Sub-Task 3.1.1: Designing of Grant System:

Designing the grant system - includes designing of a comprehensive grant system that includes the structural, legal, and procedural framework necessary to ensure the grants effectively support research and partnership within cybersecurity ecosystem.

Sub-Task 3.1.2: Grant Coordination and Management:

To ensure effective grant coordination and management, grants will be distributed in collaboration with external partners, such as EIS, emphasising seamless communication, thorough reporting and rigorous quality control. Clear communication channels will be established with partners to align on responsibilities, expectations, and goals. A tracking system will oversee the distribution process, enabling prompt resolution of issues and adjustments as needed. Regular, standardised reporting and documentation practices will be implemented to capture key data, including financial transactions, project milestones, and impact assessments, ensuring accountability and transparency throughout the grant lifecycle.

T3.2 Cyber Innovation Diplomacy and Pathway to Cross-Border Projects

This task will create a strategy focused on promoting cybersecurity innovation by increasing Estonian community participation in international and regional projects.

This task includes three sub-tasks: sharing information and raising awareness on cybersecurity projects and opportunities, creating a platform and spaces for companies to find potential collaboration and consortium partners and providing technical assistance to stakeholders by supporting the stakeholders in their application phase for projects managed by the ECCC and others.

Sub-task 3.2.1: Awareness raising on potential projects:

The sub-task will focus on disseminating information on various platforms to the Estonian Cybersecurity Community about project calls from Digital Europe, Horizon Europe, European Defense Fund and other relevant funds. The sub-task will rely on the communication and dissemination plan in Work Package 5. RIA will organise at least 8 Call Introduction events in Estonia (2 every year) to support dissemination of information about DIGITAL calls and Horizon Europe calls when possible.

Sub-task 3.2.2: Supporting partnerships:

The sub-task facilitates the participation of the Estonian Cybersecurity Community at various brokerage events on the European level. As European cross-border projects usually require consortium partners from various Member States, the Community members may need extra encouragement and assistance in the participation in such events. The task relies on sub-task 3.2.1 for awareness raising and a robust Community membership.

As the project calls are published in Digital Europe, Horizon Europe, European Defense Fund and other relevant calls, we will collaborate with the regional NCCs (NCC-FI, NCC-SE, NCC-LV, NCC-LT, NCC-DK, NCC-NO, NCC-IS and others) to organize a regional Information Day about those calls. The Info Day will be held in different locations and Tallinn, Estonia will be one of those. We will organize at least 3 such events in Tallinn and regional partners will be invited to those Info Days to meet and network, while colleagues from the ECCC and other NCCs will be invited to present and discuss calls. RIA will send delegations including members of businesses and academia to events organized by other NCCs to facilitate networking.

Part of the sub-task is to visit other NCCs in the region with the members of the Estonian Cybersecurity Community.

Sub-task 3.2.3: Consultation services for Members of the Community:

As providing technical assistance to stakeholders by supporting the stakeholders in their application phase for projects managed by the ECCC is one of the key tasks for the NCCs, this sub-task will create a process by which Members of the Estonian Cybersecurity Community can get consultation services for such projects. The goal is to decrease the bureaucratic burden for companies who may not have the resources to put into project writing. Ideally Members of the Community could get access to consultation services in the project preparation phase.

The task will consist of three parts:

1. Market research into which technical consultation services are needed
2. Centralized procurement of technical consultation services
3. Criteria and processes by which Members of the Community can access those consultation services

We target that 10 SME community members will be able to use centrally procured consultation services yearly. Consultation services will be available from the 2nd year of the NCCEE2 project.

Work package WP4 – Next Generation of Cybersecurity Professionals

Work Package Number	WP4	Lead Beneficiary	1 - RIA
Work Package Name	Next Generation of Cybersecurity Professionals		
Start Month	1	End Month	48

Objectives

- To reinforce cybersecurity and technology skills and competence in industry, technology and research and at all relevant educational levels, supporting gender balance
- To tackle the gender gap by increasing the number of women and girls gaining cybersecurity skills across various educational formats
- To promote cybersecurity as a core component of the digital society through interdisciplinary training and education
- To engage with national actors regarding possible contributions to promoting and disseminating cybersecurity educational programmes

Description

T4.1 CyberWizards

This task will provide a continuation of a popular task initiated in the NCCEE deployment project through training young women and girls in the field of Cybersecurity.

Since women are under-represented in the workforce of cybersecurity, the NCCEE project initiated two versions of training camps for teenagers who are on the verge of deciding their career paths - one-day camps in collaboration with the girls organization of the Estonian Defense League and 6-day summer camps for the international community. The goal of the

camps is to show hands on the challenges that cybersecurity experts are facing daily and how to solve them while introducing them to the community.

The six-day summer camps will be organized in concert with the community members from Estonia and other NCCs who are interested that their own youth participate in these events.

Through the 4 year project we will organize a total of 4 larger summer camps, each of them lasting 6-days. Camps will be every year, each for 80-100 young people. The goal is for at least half of those participants to be from other countries and organizing this will need close collaboration with the Network of NCCs and competent authorities from our partner countries.

In addition to international summer camps, we will continue organizing 1-day hands-on training for girls and to people who are working with youth. This will be done in cooperation with Estonian Defence League and other youth organizations, aiming at increasing interest of girls in Cybersecurity career-paths. Over the 4 year project we will organize 8 one-day trainings.

T4.2 Entry level work experience

As cybersecurity skills shortage is becoming a bigger problem in a more digital society, the market still makes it difficult to find entry-level work experience, such as internships or junior positions. In order to support young adults and fresh graduates finding their first professional position we will work together with existing internships programs and other projects to support the growth of internship opportunities for cybersecurity positions and junior research positions where they are encouraged to write their thesis in cybersecurity related topics.

The task includes mapping existing internship programs (e.g the IT internship program for the public sector in Estonia), working together with the program owners to expand it and encouraging private cybersecurity companies to join the program.

We aim to focus on mapping opportunities during the first year and to work with the Estonian cybersecurity community to promote the idea of entry-level work programs.

Starting from 2nd year we intend to facilitate at least 10 internship positions per year.

T4.3 Scholarships and Incentives

The main goal of this task is to introduce cybersecurity as a career path (or a field that is an important part of any other career path, regardless of their future field of work) for youth aged 15-25. The task includes mapping of existing programs, competitions, and events that young people who are attending and working towards integrating cybersecurity topics into those events.

For example:

1. A special prize for a cybersecurity related paper at the National Contest of Young Scientists where students at middle schools and high schools can submit their school research papers
2. A special hacking prize at a robotics competition
3. Special cybersecurity or CTF themed courses/trainings on popular online programs for talented middle and high-schoolers provided by universities
4. Continuing working towards integrated Cybersecurity courses and lectures in universities

NCCEE2 will support third party activities with small but relevant financial incentives such as prizes, scholarships or incentives to procure professional trainers for local youth. These will range from 1000€ to 3000€ and can be used for example to fund activities of cybersecurity clubs in schools, facilitate participation of professionals and students in internship programs or fund preparation of cybersecurity-related educational materials. We intend to support 4 activities per year, totalling 16 initiatives.

T4.4 Stakeholder engagement and coordination

Aim of this task is to create synergies between stakeholders by gathering and disseminating information about the skills gap and the initiatives, projects, and programs focusing on Cybersecurity skills in Europe and globally. Stakeholder engagement would primarily consist of information sharing through various platforms such conferences where our target groups are attending, various working groups, info seminars, trainings, video calls, 1:1 meetings etc with the following target groups:

- organizations offering services, products and trainings
- organizations looking for talented cybersecurity specialists
- people who lack the knowledge where to find information about the field of cybersecurity and/or where and how to

learn it on their own or in formal educational system (this includes cooperation with European partners such as ENISA, the European Cybersecurity Skills Academy and other relevant entities)

- people working or within close contact with youth (teachers, trainers, youth workers, parents etc)

Outcome of stakeholder engagement activities would be a set of policy papers, which would be disseminated to Estonian policy makers and the ECCC working groups on cyberskills, stakeholders at ENISA and to European Cybersecurity Skills Academy. This will help 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.

Work package WP5 – Exploitation, Dissemination and Communication

Work Package Number	WP5	Lead Beneficiary	1 - RIA
Work Package Name	Exploitation, Dissemination and Communication		
Start Month	1	End Month	48

Objectives

- To increase awareness and visibility of project achievements, promote and disseminate the relevant outcomes of the work of the NCCEE2, the ECCC and the other NCCs in the Network of NCCs
- To encourage community membership and assess the requests to become part of the European Cybersecurity Competence Community
- To act as a contact points at the national level for the Cybersecurity Competence Community
- To maximize impact and ensure sustainability of project results across Estonia and EU
- To share knowledge through various channels and engage stakeholders, youth, women, girls, and others towards the cybersecurity ecosystem.
- To enhance project profile and engage diverse audiences.
- To strengthen partnerships and encourage collaboration.

Description

T5.1 Dissemination, communication, and media outreach

Creation and execution of a dissemination and communication plan for NCCEE2, which covers:

- 1) Planned impacts and communication messages,
- 2) Channels of communication (such as website, social networks, events, conferences, and media),
- 3) Allocation of responsibilities and targets. Key Performance Indicators (KPIs) established to evaluate effectiveness.

The dedicated NCCEE section on RIA's main website, created during the pilot project, will continue to serve as a key resource for project updates. This section will be regularly updated with the latest developments, ensuring timely and relevant information is accessible. In the next phase, the website will incorporate additional sub-topics in both Estonian and English to maximize its utility. Furthermore, a strategic framework for communicating EU funding opportunities will be developed and integrated into the website, enhancing its value for stakeholders.

The CyberMeetUp community mailing list, established during the NCCEE deployment project, will be continued, maintained and updated regularly. This mailing list will be instrumental in notifying Community members about relevant events, including local and international brokerage sessions, monthly CyberMeetUps, and other pertinent activities.

RIA's social media platforms, such as LinkedIn, YouTube and Facebook, will continue to be leveraged to inform and engage the Community about upcoming events and project updates.

NCCEE2 activities will also be promoted through the newsletters of affiliated ministries, the NCC Mattermost platform, and the ECCC newsletter.

T5.2 Community engagement in Estonia and abroad

Sub-task 5.2.1 Community membership maintenance and encouragement:

To foster a thriving and engaged cyber community, a strategy for ongoing membership maintenance and encouragement will be implemented. This will include regular communication to keep members informed, engaged, and motivated to participate actively. Personalised outreach, such as welcoming new members, acknowledging achievements, and encouraging involvement in community events, will strengthen member connections and loyalty. Feedback loops will

be established to understand member needs and enhance their experience. By creating a supportive, responsive, and inclusive environment, this approach aims to boost retention, increase participation, and cultivate a sense of belonging within the cyber community.

Sub-task 5.2.2 Cybersecurity Competence Community:

The NCCEE2 project will focus on facilitating community engagement and registration to the European Cybersecurity Atlas, which provides international opportunities for collaboration between cybersecurity experts. We foresee ATLAS registration as a prerequisite for participating in some of the NCCEE2 events.

Sub-task 5.2.3 International Community Events:

As the first Baltic Cyber Innovation Forum CyberBazaar (a joint undertaking between NCC-EE, NCC-LV, and NCC-LT) was a successful example of collaboration (initiated through the NCCEE deployment project and the respective deployment projects in Latvia and Lithuania), we will ensure exploring new collaboration forms to ensure collaboration between Estonia, Latvia and Lithuania. In NCCEE2 project we will focus on activities stimulating participation of the Estonian Cybersecurity Community, the consortium partners and other relevant actors in various external conferences and workshops. Suitable events will be selected on a regular basis and chosen with sufficient flexibility to react to ad hoc, cost-effective dissemination opportunities.

T5.3 CyberMeetUps

As the CyberMeetUp events, which stem from the NCCEE pilot project, are well rooted and successful, we will continue organizing these monthly community events, where various cybersecurity challenges and possibilities will be introduced, achievements celebrated and research results disseminated. This includes information about NCC-EE services and knowledge provided by the Community Members, updates about the threat landscape and threat intelligence and awareness raising about project calls from Digital Europe, Horizon Europe, European Defense Fund, and other relevant funds (as laid out in sub-task 3.2.1).

We foresee 9 CyberMeetUps per year, meaning a total of 36 fascinating and practical events for cybersecurity members in Estonia during the NCCEE2 project.

We will encourage collaboration with the network of NCCs to disseminate knowledge from other communities and the relevant project results from other NCC projects.


T5.4. Exploitation Plan

The goal of this task is to create an actionable plan for the legacy of cybersecurity research, development, and education, along with strategies for continued coordination and networking. This includes the implementation of ideas, concepts, and educational resources created in WPs 2, 3, and 4. A consultation will be aligned with the actions outlined in these work packages, and will also focus on engaging youth, as well as women and girls, in these initiatives. Focus will be on the exploitation and legacy with a target of being self-sustainable. We will be looking for collaboration and synergies between public and private sector entities and international cooperation. The outcome of this task will be a document with a proposal for policy makers in Estonia about the way forward.

STAFF EFFORT

Staff effort per participant						
Grant Preparation (Work packages - Effort screen) — Enter the info.						
Participant	WP1	WP2	WP3	WP4	WP5	Total Person-Months
1 - RIA	96.00	48.00	24.00	48.00	48.00	264.00
3 - TEHNOPOL		27.00			9.00	36.00
Total Person-Months	96.00	75.00	24.00	48.00	57.00	300.00

LIST OF DELIVERABLES

<div>Deliverables</div> <div>Grant Preparation (Deliverables screen) — Enter the info.</div> <div>The labels used mean:</div> <div>Public — fully open ( automatically posted online)</div> <div>Sensitive — limited under the conditions of the Grant Agreement</div> <div>EU classified —RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444</div>						
Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D1.1	Revised Gender Action Plan (GAP)	WP1	1 - RIA	R — Document, report	PU - Public	3
D1.2	Quality Plan	WP1	1 - RIA	R — Document, report	PU - Public	6
D1.3	Data Management Plan	WP1	1 - RIA	DMP — Data Management Plan	PU - Public	6
D1.4	Risk Management Plan	WP1	1 - RIA	R — Document, report	SEN - Sensitive	6
D1.5	Annual Report based on KPIs I	WP1	1 - RIA	R — Document, report	SEN - Sensitive	14
D1.6	Annual Report based on KPIs II	WP1	1 - RIA	R — Document, report	SEN - Sensitive	26
D1.7	Annual Report based on KPIs III	WP1	1 - RIA	R — Document, report	SEN - Sensitive	36
D1.8	Annual Report based on KPIs IV	WP1	1 - RIA	R — Document, report	SEN - Sensitive	48
D2.1	CyberAccelerator program design	WP2	3 - TEHNOPOL	R — Document, report	PU - Public	4
D2.2	Updated Methodology for CyberTransformation I	WP2	1 - RIA	R — Document, report	PU - Public	12
D2.3	Updated Methodology for CyberTransformation II	WP2	1 - RIA	R — Document, report	PU - Public	36
D2.4	Implemented Acceleration Program I	WP2	3 - TEHNOPOL	R — Document, report	PU - Public	15
D2.5	Implemented Acceleration Program II	WP2	3 - TEHNOPOL	R — Document, report	PU - Public	27

Deliverables

Grant Preparation (Deliverables screen) — Enter the info.

The labels used mean:

Public — fully open (🚩 automatically posted online)

Sensitive — limited under the conditions of the Grant Agreement

EU classified — RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision [2015/444](#)

Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D2.6	Implemented Acceleration Program III	WP2	3 - TEHNOPOL	R — Document, report	PU - Public	39
D3.1	Grant System Design	WP3	1 - RIA	R — Document, report	PU - Public	6
D3.2	Grant Coordination and Management Plan	WP3	1 - RIA	R — Document, report	PU - Public	7
D3.3	Cyber Innovation diplomacy & pathway to crossborder projects strategy	WP3	1 - RIA	R — Document, report	PU - Public	8
D3.4	Digital Innovation and Diplomacy Report	WP3	1 - RIA	R — Document, report	PU - Public	48
D3.5	Compendium of results of CyberInnovation Grants I	WP3	1 - RIA	R — Document, report	PU - Public	30
D3.6	Compendium of results of CyberInnovation Grants II	WP3	1 - RIA	R — Document, report	PU - Public	42
D4.1	Internships and Scholarship Programs Design	WP4	1 - RIA	R — Document, report	PU - Public	6
D4.2	A set of Policy Papers I	WP4	1 - RIA	R — Document, report	PU - Public	10
D4.3	A set of Policy Papers II	WP4	1 - RIA	R — Document, report	PU - Public	22
D4.4	A set of Policy Papers III	WP4	1 - RIA	R — Document, report	PU - Public	34
D4.5	A set of Policy Papers IV	WP4	1 - RIA	R — Document, report	PU - Public	46
D4.6	CyberWizards I	WP4	1 - RIA	R — Document, report	PU - Public	24
D4.7	CyberWizards II	WP4	1 - RIA	R — Document, report	PU - Public	47

Deliverables

Grant Preparation (Deliverables screen) — Enter the info.

The labels used mean:

Public — fully open (🚩 automatically posted online)

Sensitive — limited under the conditions of the Grant Agreement

EU classified — RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision [2015/444](#)

Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D4.8	Internships and Scholarship Programs Implementations I	WP4	1 - RIA	R — Document, report	PU - Public	24
D4.9	Internships and Scholarship Programs Implementations II	WP4	1 - RIA	R — Document, report	PU - Public	47
D5.1	Dissemination and Communication Plan	WP5	1 - RIA	R — Document, report	PU - Public	3
D5.2	Community engagement overview I	WP5	1 - RIA	R — Document, report	PU - Public	24
D5.3	Community engagement overview II	WP5	1 - RIA	R — Document, report	PU - Public	48
D5.4	Exploitation Report	WP5	1 - RIA	R — Document, report	PU - Public	46
D5.5	Final Report on Dissemination and Communications activities and Events compendium	WP5	1 - RIA	R — Document, report	PU - Public	48

Deliverable D1.1 – Revised Gender Action Plan (GAP)

Deliverable Number	D1.1	Lead Beneficiary	1 - RIA
Deliverable Name	Revised Gender Action Plan (GAP)		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	3	Work Package No	WP1

Description
<p>The document which has already been created as part of pilot NCCEE will be revised to meet the standards of the NCCEE2 project. The report will be made available in English/ Estonian and Word/ PDF format will be used. Care will be taken to include gender sensitive language throughout the document, and it will include:</p> <ol style="list-style-type: none"> 1) gender equality strategies and measures 2) gender impact policies and assessments

Deliverable D1.2 – Quality Plan

Deliverable Number	D1.2	Lead Beneficiary	1 - RIA
Deliverable Name	Quality Plan		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	6	Work Package No	WP1

Description
<p>Quality Plan will be created, based on proven quality assurance frameworks, in Word/ PDF format in Estonian and English.</p>

Deliverable D1.3 – Data Management Plan

Deliverable Number	D1.3	Lead Beneficiary	1 - RIA
Deliverable Name	Data Management Plan		
Type	DMP — Data Management Plan	Dissemination Level	PU - Public
Due Date (month)	6	Work Package No	WP1

Description
<p>The plan will include steps and methods about safely and securely handling of the data and its storage. The plan will be made available in English and Estonian in Word/ PDF format.</p>

Deliverable D1.4 – Risk Management Plan

Deliverable Number	D1.4	Lead Beneficiary	1 - RIA
Deliverable Name	Risk Management Plan		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	6	Work Package No	WP1



Description
The document will be made available in English and Estonian using Word/ PDF format.

Deliverable D1.5 – Annual Report based on KPIs I

Deliverable Number	D1.5	Lead Beneficiary	1 - RIA
Deliverable Name	Annual Report based on KPIs I		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	14	Work Package No	WP1

Description
The Project Progress Report for the first year based on KPIs, in English, in Word/PDF format.

Deliverable D1.6 – Annual Report based on KPIs II

Deliverable Number	D1.6	Lead Beneficiary	1 - RIA
Deliverable Name	Annual Report based on KPIs II		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	26	Work Package No	WP1

Description
The Project Progress Report for the second year based on KPIs, in English, in Word/PDF format.

Deliverable D1.7 – Annual Report based on KPIs III

Deliverable Number	D1.7	Lead Beneficiary	1 - RIA
Deliverable Name	Annual Report based on KPIs III		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	36	Work Package No	WP1

Description
The Project Progress Report for the third year based on KPIs, in English, in Word/PDF format.

Deliverable D1.8 – Annual Report based on KPIs IV

Deliverable Number	D1.8	Lead Beneficiary	1 - RIA
Deliverable Name	Annual Report based on KPIs IV		
Type	R — Document, report	Dissemination Level	SEN - Sensitive
Due Date (month)	48	Work Package No	WP1

Description

The final Project Progress Report based on KPIs, in English, in Word/PDF format.

Deliverable D2.1 – CyberAccelerator program design

Deliverable Number	D2.1	Lead Beneficiary	3 - TEHNOPOL
Deliverable Name	CyberAccelerator program design		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	4	Work Package No	WP2

Description

A revised version of the acceleration program will be put forward based on current requirements. The Document will be in Estonian and English and in Word/ PDF format.

Deliverable D2.2 – Updated Methodology for CyberTransformation I

Deliverable Number	D2.2	Lead Beneficiary	1 - RIA
Deliverable Name	Updated Methodology for CyberTransformation I		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	12	Work Package No	WP2

Description

The document will include updated methodology for facilitating cyber transformation, based on the process and findings of CyberTransformation. Updated 2nd version of the methodology will be published later in the project. The document will be in Estonian and English, in Word/ PDF format.

Deliverable D2.3 – Updated Methodology for CyberTransformation II

Deliverable Number	D2.3	Lead Beneficiary	1 - RIA
Deliverable Name	Updated Methodology for CyberTransformation II		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	36	Work Package No	WP2

Description

The document will include updated methodology for facilitating cyber transformation, based on the process and findings of CyberTransformation. The document will be in Estonian and English, in Word/ PDF format.

Deliverable D2.4 – Implemented Acceleration Program I

Deliverable Number	D2.4	Lead Beneficiary	3 - TEHNOPOL
Deliverable Name	Implemented Acceleration Program I		
Type	R — Document, report	Dissemination Level	PU - Public

Due Date (month)	15	Work Package No	WP2
-------------------------	----	------------------------	-----

Description
The report will list all participants that participated during the acceleration program during the project period, organised in 7-month batches. It will also include an overview of all grants paid out to the participants. Each report will present results for each batch. The document will be available in English and Estonian, in Word and PDF formats.

Deliverable D2.5 – Implemented Acceleration Program II

Deliverable Number	D2.5	Lead Beneficiary	3 - TEHNOPOL
Deliverable Name	Implemented Acceleration Program II		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	27	Work Package No	WP2

Description
The report will list all participants that participated during the acceleration program during the project period, organised in 7-month batches. It will also include an overview of all grants paid out to the participants. Each report will present results for each batch. The document will be available in English and Estonian, in Word and PDF formats.

Deliverable D2.6 – Implemented Acceleration Program III

Deliverable Number	D2.6	Lead Beneficiary	3 - TEHNOPOL
Deliverable Name	Implemented Acceleration Program III		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	39	Work Package No	WP2

Description
The report will list all participants that participated during the acceleration program during the project period, organised in 7-month batches. It will also include an overview of all grants paid out to the participants. Each report will present results for each batch. The document will be available in English and Estonian, in Word and PDF formats.

Deliverable D3.1 – Grant System Design

Deliverable Number	D3.1	Lead Beneficiary	1 - RIA
Deliverable Name	Grant System Design		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	6	Work Package No	WP3

Description
This will include the grant programs that are structured and designed as part of Task 3.1 in order to be implemented. The report will be in Word/PDF and in English and Estonian.

Deliverable D3.2 – Grant Coordination and Management Plan

Deliverable Number	D3.2	Lead Beneficiary	1 - RIA
Deliverable Name	Grant Coordination and Management Plan		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	7	Work Package No	WP3

Description
This will include a plan to effectively coordinate and manage the Grants for Task 3.1 to achieve the targeted results. The plan will be in English and Estonian and in Word/ PDF format.

Deliverable D3.3 – Cyber Innovation diplomacy & pathway to crossborder projects strategy

Deliverable Number	D3.3	Lead Beneficiary	1 - RIA
Deliverable Name	Cyber Innovation diplomacy & pathway to crossborder projects strategy		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	8	Work Package No	WP3

Description
The document will include the strategy to achieve the cyber innovation diplomacy and cross-border pathways for the cyber community. The document will be in English and Estonian and in Word/ PDF format.

Deliverable D3.4 – Digital Innovation and Diplomacy Report

Deliverable Number	D3.4	Lead Beneficiary	1 - RIA
Deliverable Name	Digital Innovation and Diplomacy Report		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	48	Work Package No	WP3

Description
The document will include a summary of all the activities carried under T3.2. The document will be in Estonian and English and in Word/ PDF format.

Deliverable D3.5 – Compendium of results of CyberInnovation Grants I

Deliverable Number	D3.5	Lead Beneficiary	1 - RIA
Deliverable Name	Compendium of results of CyberInnovation Grants I		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	30	Work Package No	WP3

Description
This compendium will showcase results achieved with CyberInnovation Grants.

The document will be in Estonian and English and in Word/ PDF format.

Deliverable D3.6 – Compendium of results of CyberInnovation Grants II

Deliverable Number	D3.6	Lead Beneficiary	1 - RIA
Deliverable Name	Compendium of results of CyberInnovation Grants II		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	42	Work Package No	WP3

Description

This compendium will showcase results achieved with CyberInnovation Grants.
The document will be in Estonian and English and in Word/ PDF format.

Deliverable D4.1 – Internships and Scholarship Programs Design

Deliverable Number	D4.1	Lead Beneficiary	1 - RIA
Deliverable Name	Internships and Scholarship Programs Design		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	6	Work Package No	WP4

Description

This will include a report on programs that will be designed or cooperated with as part of Tasks 4.3 and 4.4.
The report will be in English and Estonian, in Word/PDF format.

Deliverable D4.2 – A set of Policy Papers I

Deliverable Number	D4.2	Lead Beneficiary	1 - RIA
Deliverable Name	A set of Policy Papers I		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	10	Work Package No	WP4

Description

A set of policy papers distributed yearly, including best practices and identifying what can be done differently to enhance cybersecurity.
The report will be in Word/PDF and in English and Estonian.

Deliverable D4.3 – A set of Policy Papers II

Deliverable Number	D4.3	Lead Beneficiary	1 - RIA
Deliverable Name	A set of Policy Papers II		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	22	Work Package No	WP4

Description
set of policy papers distributed yearly, including best practices and identifying what can be done differently to enhance cybersecurity. The report will be in Word/PDF and in English and Estonian.

Deliverable D4.4 – A set of Policy Papers III

Deliverable Number	D4.4	Lead Beneficiary	1 - RIA
Deliverable Name	A set of Policy Papers III		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	34	Work Package No	WP4

Description
A set of policy papers distributed yearly, including best practices and identifying what can be done differently to enhance cybersecurity. The report will be in Word/PDF and in English and Estonian.

Deliverable D4.5 – A set of Policy Papers IV

Deliverable Number	D4.5	Lead Beneficiary	1 - RIA
Deliverable Name	A set of Policy Papers IV		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	46	Work Package No	WP4

Description
A set of policy papers distributed yearly, including best practices and identifying what can be done differently to enhance cybersecurity. The report will be in Word/PDF and in English and Estonian.

Deliverable D4.6 – CyberWizards I

Deliverable Number	D4.6	Lead Beneficiary	1 - RIA
Deliverable Name	CyberWizards I		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	24	Work Package No	WP4

Description
This will consist of a video-report with summary of all the events, camps, educational activities that will be carried out as part of Task 4.2. Each report will show results for each period. The report will be in audiovisual format in English.

Deliverable D4.7 – CyberWizards II

Deliverable Number	D4.7	Lead Beneficiary	1 - RIA
Deliverable Name	CyberWizards II		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	47	Work Package No	WP4

Description
<p>This will consist of a video-report with summary of all the events, camps, educational activities that will be carried out as part of Task 4.2.</p> <p>Each report will show results for each period. The report will be in audiovisual format in English.</p>

Deliverable D4.8 – Internships and Scholarship Programs Implementations I

Deliverable Number	D4.8	Lead Beneficiary	1 - RIA
Deliverable Name	Internships and Scholarship Programs Implementations I		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	24	Work Package No	WP4

Description
<p>This will include a summary of programs and feedback from participants and interns who participated in the programs as part of Tasks 4.3 and 4.4. Each report will show results for each period.</p> <p>The report will be in Word/PDF format, and will be in English and Estonian.</p>

Deliverable D4.9 – Internships and Scholarship Programs Implementations II

Deliverable Number	D4.9	Lead Beneficiary	1 - RIA
Deliverable Name	Internships and Scholarship Programs Implementations II		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	47	Work Package No	WP4

Description
<p>This will include a summary of programs and feedback from participants and interns who participated in the programs as part of Tasks 4.3 and 4.4. Each report will show results for each period.</p> <p>The report will be in Word/PDF format, and will be in English and Estonian.</p>

Deliverable D5.1 – Dissemination and Communication Plan

Deliverable Number	D5.1	Lead Beneficiary	1 - RIA
Deliverable Name	Dissemination and Communication Plan		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	3	Work Package No	WP5

Description
Plan with details about dissemination activities and communication. The document will be in Word/PDF, in English/ Estonian.

Deliverable D5.2 – Community engagement overview I

Deliverable Number	D5.2	Lead Beneficiary	1 - RIA
Deliverable Name	Community engagement overview I		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	24	Work Package No	WP5

Description
This will include a summary of all the events and activities carried out under the Task 5.2. Each report will show the version as A, and B based on the update respectively. The document will be in Word/ PDF and in English and Estonian.

Deliverable D5.3 – Community engagement overview II

Deliverable Number	D5.3	Lead Beneficiary	1 - RIA
Deliverable Name	Community engagement overview II		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	48	Work Package No	WP5

Description
This will include a summary of all the events and activities carried out under the Task 5.2. Each report will show the version as A, and B based on the update respectively. The document will be in Word/PDF and in English and Estonian.

Deliverable D5.4 – Exploitation Report

Deliverable Number	D5.4	Lead Beneficiary	1 - RIA
Deliverable Name	Exploitation Report		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	46	Work Package No	WP5

Description
This will include a summary of all the activities to be carried out as part of the exploitation plan. The report will be in English and Estonian and in Word/PDF format.

Deliverable D5.5 – Final Report on Dissemination and Communications activities and Events compendium

Deliverable Number	D5.5	Lead Beneficiary	1 - RIA
--------------------	------	------------------	---------

Deliverable Name	Final Report on Dissemination and Communications activities and Events compendium		
Type	R — Document, report	Dissemination Level	PU - Public
Due Date (month)	48	Work Package No	WP5

Description
<p>This will include a compendium of videos, digital images and other resources created and used during various activities/events/ workshops, along with a summary of the events and activities carried out as part of dissemination and communication.</p> <p>The document will be in English and Estonian.</p>

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	Design of all grants programs	WP4, WP3, WP2	1 - RIA	Document with updated program D2.1 delivered. Document with the grant system structure D3.1 delivered. Deliverable 4.1 has been prepared.	7
2	Acceleration Program implementation	WP2	3 - TEHNOPOL	Document for D2.4 for first batch delivered.	15
3	Periodic Report I and Mid-term Review Meeting	WP1	1 - RIA	Project progress for Months 1–18 has been reported. The technical and financial reports have been submitted via the EU Funding & Tenders Portal.	18
4	MidTerm Progress Review	WP1	1 - RIA	Deliverables due before M24 have been delivered.	24
5	Acceleration Program 2 implementation	WP2	3 - TEHNOPOL	Document for D2.5 for second batch delivered.	27
6	Acceleration Program 3 implementation	WP2	3 - TEHNOPOL	Document for D2.6 or third batch delivered.	39
7	Periodic Report II and Mid-term Review Meeting	WP1	1 - RIA	Project progress for Month 19-36 has been reported. The technical and financial reports have been submitted via the EU Funding & Tenders Portal.	36
8	CyberInnovation Grants have been distributed and projects completed	WP3	1 - RIA	Compendium of results of CyberInnovation grants (D3.5) has been delivered.	42
9	CyberWizards	WP4	1 - RIA	Video-report of all CyberWizards events and camps (D4.6, D4.7) has been prepared.	47
10	Internships and Scholarship Programs Implementations	WP4	1 - RIA	Deliverable 4.9 has been submitted.	47

Milestones					
Grant Preparation (Milestones screen) — Enter the info.					
Milestone No	Milestone Name	Work Package No	Lead Beneficiary	Means of Verification	Due Date (month)
11	Community engagement	WP5	1 - RIA	Community Engagement Overview (D5.3) has been finalized.	48
12	Final Review	WP1, WP4, WP3, WP2, WP5	1 - RIA	All deliverables have been delivered.	48
13	Periodic Report III and Final Review Meeting	WP1	1 - RIA	Project progress for Months 37–48 has been reported. The technical and financial reports have been submitted via the EU Funding & Tenders Portal	48

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	Delay in implementation. Likelihood (Low), Severity (Medium)	WP1, WP4, WP3, WP2, WP5	SC will develop a comprehensive project timeline with well-defined milestones and regular progress check-ins to detect and address issues early. SC will also include extra buffer time into the project schedule for high-risk tasks to absorb minor delays without impacting the overall timeline. Additionally, SC will identify areas where resources can be quickly reallocated to handle hold-ups, ensuring flexibility to keep progress steady.
2	Delay in development. Likelihood (Low), Severity (Medium)	WP1, WP4, WP3, WP2, WP5	The project will be divided into smaller, manageable development phases with realistic deadlines, allowing for continuous progress assessment. SC will ensure the development

Critical risks & risk management strategy <i>Grant Preparation (Critical Risks screen) — Enter the info.</i>			
Risk number	Description	Work Package No(s)	Proposed Mitigation Measures
			<p>team remains dedicated to the project, minimising interruptions from other tasks and keeping focus on deliverables.</p> <p>The SC will adopt an agile approach with frequent progress reviews to allow rapid course corrections, keeping development on track and responsive to challenges.</p>
3	Dropout of Consortium partners. Likelihood (Low), Severity (Medium)	WP4, WP3, WP2	<p>To mitigate partner dropouts, all participating organisations will be required to sign formal commitment agreements. In the event of a partner dropout, the SC will assess the impact on project goals and find a replacement organization to fulfil the assigned tasks.</p> <p>SC will maintain thorough documentation of all work to facilitate continuity and ease the transition to new contractors if necessary.</p>
4	Lack of uptake of grants. Likelihood (Medium), Severity (Medium)	WP3	<p>The innovation grants envisioned in this project will require a level of maturity on the side of the cybersecurity private sector which is difficult to measure. The proposed mitigation measure is a continued pulse-taking of the possible participants, the consultation activities through which the consortium can guide potential participants to the grants.</p>
5	Lack of interest and delayed response. Likelihood (Low), Severity (Medium)	WP1, WP4, WP3, WP2, WP5	<p>By focusing on practical, impactful initiatives—such as training sessions, networking events, and support for adopting secure digital solutions— SC will demonstrate the tangible benefits of participation to its target groups. Through these tailored engagements, the project will build a supportive environment that encourages companies and individuals to join, thereby ensuring sustained interest and active involvement.</p> <p>The project's strategic approach, emphasising collaboration and real-world impact, will help to drive engagement across the Estonian digital and cybersecurity landscape.</p>

PROJECT REVIEWS

Project Reviews			
Grant Preparation (Reviews screen) — Enter the info.			
Review No	Timing (month)	Location	Comments
RV1	18	tbc	at end of reporting period1
RV2	36	tbc	at end of reporting period2
RV3	48	tbc	at end of reporting period3



ANNEX 1



Digital Europe Programme (DIGITAL)

Description of the action (DoA)

Part B



TECHNICAL DESCRIPTION (PART B)

COVER PAGE

Part B of the Application Form must be downloaded from the Portal Submission System, completed and then assembled and re-uploaded as PDF in the system. Page 1 with the grey IMPORTANT NOTICE box should be deleted before uploading.

Note: Please read carefully the conditions set out in the Call document (for open calls: published on the Portal). Pay particular attention to the award criteria; they explain how the application will be evaluated.

PROJECT	
Project name:	Cybersecurity Community Building and Sustainable Impact of the Estonian National Coordination Centre Activities
Project acronym:	NCCEE2
Coordinator contact:	Lauri Tankler, RIA

HISTORY OF CHANGES		
Date	Page/section	Nature of change and reason / justification of change proposed
11.06.25	<p>p. 3-8 – Relevance</p> <p>p. 21 - Impact</p> <p>p. 32, p. 37, p. 45 – Work plan, work packages, activities, resources and timing</p> <p>p. 51-52 - Other cost categories</p> <p>p. 52-53 – Timetable</p>	<p>The following subsections has been updated in accordance with suggestions from the Proposal Evaluation Support:</p> <p>The "Objectives and Activities" and "Contribution to long-term policy objectives, policies and strategies — synergies"</p> <p>The "Dissemination and communication of the project and its results"</p> <p>Work Package 2, Task 2.1 Description</p> <p>Work Package 3, Task 3.1 Description</p> <p>Work Package 5, Sub-task 5.5.2 Description</p> <p>Other cost categories– Financial support to third parties "Explanation" updated for Participants 1-3</p> <p>Timetable</p>
02.07.25	<p>p. 47 - Staff effort per participant</p> <p>p. 49 - Purchases and equipment</p>	<p>Participant RIA Total Person-Month has been updated</p> <p>Two cost items have been added for Participant Tehnopol</p>
11.07.25	p. 30 – Estimated budget — Resources	Total amount of WP1 has been updated

TABLE OF CONTENTS

TECHNICAL DESCRIPTION (PART B)	1
COVER PAGE	1
1. RELEVANCE	3
1.1 OBJECTIVES AND ACTIVITIES	3
1.2 CONTRIBUTION TO LONG-TERM POLICY OBJECTIVES, POLICIES AND STRATEGIES — SYNERGIES ...	6
1.3 DIGITAL TECHNOLOGY SUPPLY CHAIN	8
1.4 FINANCIAL OBSTACLES	8
2. IMPLEMENTATION	9
2.1 MATURITY	9
2.2 IMPLEMENTATION PLAN AND EFFICIENT USE OF RESOURCES	9
2.3 CAPACITY TO CARRY OUT THE PROPOSED WORK	14
3. IMPACT	17
3.1 EXPECTED OUTCOMES AND DELIVERABLES — DISSEMINATION AND COMMUNICATION	17
3.2 COMPETITIVENESS AND BENEFITS FOR SOCIETY	21
3.3 ENVIRONMENTAL SUSTAINABILITY AND CONTRIBUTION TO EUROPEAN GREEN DEAL GOALS	23
4. WORK PLAN, WORK PACKAGES, ACTIVITIES, RESOURCES AND TIMING	24
4.1 WORK PLAN	24
4.2 WORK PACKAGES, ACTIVITIES, RESOURCES AND TIMING	26
5. OTHER	55
5.1 ETHICS	55
5.2 SECURITY	55
6. DECLARATIONS	56
ANNEXES	56

##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?

In a constantly technologically advancing world, digitalization is the constant that we must take into account which will impact all aspects of the society. As digitalization itself moves into more mature territory with artificial intelligence solutions, autonomous technologies and ever-expanding computational power, the role of cybersecurity continues to increase in our world. As the technology keeps developing, so does the need for research, development, innovation and entrepreneurship in the ecosystem of cybersecurity.

According to Estonian State Information Authority's report of 2023, Estonia's cyber ecosystem saw a surge of cyber incidents to nearly 3,314, with 484 incidents of Distributed Denial-of-Service (DDoS) attacks. These figures are the highest recorded within the last 5 years. There were many incidents that targeted the personal data of clients trying to compromise their privacy. The Estonian Police and Border Guard Board recorded a loss of 53 million euros to cyber-incidents in 2023 and increasing levels of cyber frauds, with increase in level of sophistication of cyber-attacks and level of organisation of frauds.

While the Estonian authorities have taken a series of proactive actions to deter and deal with the cyber-attacks and frauds, the public sector cannot and has not ever been doing this alone. Thus it is becoming more crucial to strengthen the cybersecurity ecosystem and community with international knowledge, research, and tools to tackle cyber incidents. As tools to provide cybersecurity come from the private sector, research from academia and skills from the educational sector, the collaboration to provide security is a common effort. As we anticipate a rise in the use of AI and machine learning mechanisms to organise and set up cyber incidents and frauds, it is important to facilitate a change where cybersecurity is not just a nice-to-have, but there would be a culture of cybersecurity to keep our society safe.

With a vision of protecting the digital world and cyberspace of the Member States, the EU organised the European Cybersecurity Competence Centre (Regulation (EU) 2021/887), and encouraged the Member States to establish the National Coordination Centres (NCCs). At the same time, assigning the NCCs to support the Competence Centre and Network's mission in national liaison and coordination activities with local stakeholders (Article 7, Regulation (EU) 2021/887). NCCs should:

- Provide expertise, contribute to strategic planning, and address national and regional cybersecurity challenges.
- Facilitate participation of civil society, industry (especially start-ups and SMEs), academia, and research institutions in EU-funded cybersecurity initiatives.
- Support stakeholders in applying for and implementing Competence Centre projects, ensuring compliance with financial and conflict-of-interest regulations.
- Align with national and regional cybersecurity policies, promote educational programs, and disseminate the outcomes of the Network, Community, and Competence Centre activities.
- Implement funded actions, provide financial support to third parties, and assess and promote involvement in Competence Centre-related activities.

Considering this mission, the Estonian NCC (NCC-EE) will build on an initial deployment project called NCCEE (which ran from March 2023 - March 2025) with this proposed NCCEE2 project, starting from April 1st 2025, to nurture the seed that has been planted and is showing signs of sprouting. Building a strong, inclusive, collaborative and innovative community requires continuous fostering and support. It requires a culture of innovation and development.

One of the roles of the NCCs across the EU is to support the cybersecurity community, including SMEs, by promoting the use and spread of advanced cybersecurity solutions and enhancing cybersecurity capabilities. The NCCEE2 project is built on the pilot NCCEE project, which was funded by Digital Europe Programme. With implementation of the NCCEE2 we plan to continue on the same path, to expand on the same framework to strengthen the cybersecurity across Estonia and assist other NCCs across Europe via exchange of knowledge, expertise, and best practices. As such, the project supports the general call objectives of enhancing digital security and fostering innovation in cybersecurity technologies. It aims to

create a stronger and secure digital environment that encourages growth of economy and social development across Estonia.

Objectives:

1. **Creating sustained impact in capacity building in the cybersecurity industry, research and technology alongside the cybersecurity community through events, knowledge sharing, sustainable innovation programs and facilitation of collaboration.**

The NCCEE2 project, as its predecessor NCCEE, is built on community. A well-connected cybersecurity ecosystem that bridges industry, academia, public institutions, and private citizens is essential for resilience. This community should be resilient on its own and for this a culture of community engagement needs to be built not just among Estonian companies, but throughout Europe. For the local part of this **NCCEE2** will host events, workshops, and virtual forums that encourage collaboration and knowledge exchange among key stakeholders. It will facilitate knowledge exchange, sharing of resources and provide continuous support for all the stakeholders. This aligns with the OECD's recommendation for countries to foster "multi-stakeholder partnerships" that drive cybersecurity readiness and innovation across sectors (OECD, *Digital Security Risk Management for Economic and Social Prosperity*, 2015). By fostering cross-sector and cross-border collaborations, **NCCEE2** enhances Estonia's capacity to respond effectively to cybersecurity challenges, strengthening its position within the European cybersecurity framework and contributing to the strategic autonomy goal of the ECCC. Additionally, **NCCEE2** will initiate a special track for cybersecurity companies to engage with European partners to participate in innovation projects, which also means cross-border collaboration by expanding international community events and knowledge-sharing initiatives, including partnerships with other NCC-s in the region. This cross-border exchange will help create a culture of collaboration, to solidify the notion that innovation is key, and foster innovative cybersecurity solutions, further solidifying the digital security infrastructure across the EU.

This project objective will be primarily achieved through the activities described in Work Package 5, as well as Work Package 2. To support this objective, the following KPIs have been established: NCCEE2 aims to actively engage 40 entities in its community on a regular basis and provide targeted support to 10 entities through the Cyber Innovation Diplomacy and Pathway to Cross-Border Project program, organize a total of 36 CyberMeetUp community engagement events, and host 3 international DIGITAL information days or brokerage events in Tallinn, Estonia.

2. **Promoting and encouraging a culture of innovation in cybersecurity, including increasing practical implementation of research outcomes, facilitating the participation in cross-border projects and entrepreneurship;**

NCCEE2 will drive cybersecurity research and development by collaborating with academic and industry stakeholders. A notable collaboration with Estonia's AI and Robotics Digital Innovation Hub (AIRE) will facilitate the exploration of the cybersecurity of cutting-edge technologies such as artificial intelligence and machine learning to address security vulnerabilities in Internet of Things and other digital innovations. This effort reflects the findings of a European Commission report, which emphasises the need for comprehensive cybersecurity R&D strategies to tackle digital threats posed by advanced technologies (*The EU Cybersecurity Strategy for the Digital Decade*, 2021). Through this initiative, **NCCEE2** aims to integrate Estonia into the larger EU research network, thereby enhancing regional and international cybersecurity capabilities. Moreover, **NCCEE2** will promote participation of Estonian organisations in Digital Europe and Horizon Europe funding calls, fostering greater collaboration and development of advanced cybersecurity solutions at the EU level.

The described objective will be achieved through the activities outlined under Work Package 3. Within this Work Package, we will implement Cyber Innovation Grants, which aim to support at least 18 innovation projects over a 48-month period. In order to encourage participation in cross-border projects, we aim to support 10 entities in participating in international events. To encourage international collaboration, we will organize 8 Digital Europe/Horizon Europe Introduction Events and 3 international DIGITAL information days or brokerage events. NCCEE2 intends to provide consultations and technical assistance to a total of 30 SMEs, supporting stakeholders during the application phase for projects managed by the ECCC in order to ensure their success in cross-border collaboration.

3. **Increasing the number of specialists and youth acquiring knowledge and training in the field of cybersecurity, with a special focus on women and girls, while taking into account the needs of the cybersecurity community;**

Developing a cybersecurity-skilled workforce is essential for the long-term digital security in both Estonia and Europe in general. **NCCEE2** will continue its efforts to implement educational

programs that span from early schooling to adult training, with specific initiatives designed to engage underrepresented groups, including women. Research underscores the impact of cybersecurity education on reducing digital risks and fostering a more informed citizenry (Al-Rimy et al., 2020). According to a study published by the World Economic Forum, cybersecurity education should be designed to continually adapt to emerging threats and to build foundational skills that enhance cyber resilience (*The Global Risks Report*, 2021). By promoting cybersecurity as a career pathway and integrating cybersecurity principles into general education, **NCCEE2** supports Estonia's role in building a knowledgeable, proactive society equipped to manage digital threats.

This objective will be achieved through the activities carried out under Work Package 4. The following KPIs have been set: NCCEE2 will organize four summer camps aimed at girls, each expecting 80–100 participants. In addition, eight one-day hands-on training sessions for girls will be held. Additionally, the project aims to facilitate at least 30 internship opportunities and support third-party initiatives, such as prizes, scholarships, or incentives to engage professional trainers for local youth. A total of 16 such initiatives are planned.

4. Promoting and supporting the uptake and dissemination of state-of-the-art cybersecurity solutions by all actors in society, with special attention paid to small and medium sized enterprises

Small and medium-sized enterprises (SMEs), crucial to Estonia's and Europe's economies, are ill-equipped to counter cybersecurity threats due to limited resources. **NCCEE2** will approach the problem from the service provider side while tackling the awareness problem. The grants NCCEE2 will provide to cybersecurity companies and the service providers will create new and innovative tools to help SMEs take care of their cybersecurity better. The cybersecurity accelerator program will bring new tools and services from research to market. Building on the NCCEE pilot project, we will continue to make sure the Estonian cybersecurity service providers will be able to provide a standardized level of service through the methodology the consortium partners have created and developed.

This objective will be supported through the Accelerator Program described under Work Package 2, which will fund 18 start-ups to develop cybersecurity-related solutions. To ensure that Estonian cybersecurity service providers are able to offer a standardized level of service, based on the methodology developed during NCCEE project, two new versions of the Cyber Transformation Methodology will be created over the four-year period. Furthermore, the Cyber Innovation Grants described under Work Package 3 will contribute to achieving this objective, with plans to award between 15 and 20 grants.

As society becomes increasingly dependent on interconnected technologies, the necessity for robust cybersecurity infrastructure and awareness cannot be overstated. **NCCEE2's** initiatives align with EU and global cybersecurity goals by prioritising technological resilience, fostering innovation and investment into a skilled workforce, and promoting sustainable community engagement. According to a study by the International Institute for Strategic Studies (IISS), coordinated cybersecurity strategies and international cooperation are fundamental to building resilient digital systems capable of withstanding complex cyber threats (*Cybersecurity and National Defense*, 2020). Through **NCCEE2**, Estonia is not only strengthening its national cybersecurity infrastructure but also contributing to a more secure and resilient European digital landscape, reflecting the EU's dedication to cybersecurity as a fundamental pillar of modern society.

In this way, **NCCEE2** shows a commitment to advancing digital security, fostering economic stability, and creating a safe, connected community that can confidently navigate and contribute to a rapidly digitalising world.

The project addresses key themes such as:

1. Public-Private Collaboration: Encouraging collaboration between government agencies, private sector businesses, and community organisations to share knowledge and resources.
2. Innovation and Technology: Promoting the adoption of cutting-edge cybersecurity technologies and practices.
3. Capacity Building: Strengthening the cybersecurity capabilities of businesses and the community through continuous education and training. International cooperation is of paramount importance to develop cybersecure Estonia and Europe.

Further, in terms of contribution towards the Digital Europe Programme Objectives, the project aligns with:

1. **Digital Transformation:** The project contributes to the Digital Europe Programme by promoting digital transformation and enhancing digital skills across Estonia. It ensures that businesses and community can safely leverage digital technologies for growth and development.
2. **Cybersecurity:** By implementing robust cybersecurity measures, the project significantly improves the overall cybersecurity posture of Estonia. This includes protecting sensitive data, enhancing preventative measures against cyber-attacks, and ensuring the reliability of digital services.
3. **Economic and Social Impact:** The project has the potential to create jobs in the cybersecurity sector, foster innovation, and build trust in digital services. It also aims to reduce the economic impact of cyber incidents on businesses and the community.

#@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.

"Estonia 2035" is a vision set out in the Estonian Digital Agenda 2030. The agenda talks about a futuristic Estonia, which is digitally powered, safe, and secure. To set-off this vision of **"Estonia 2035"**, along with several other initiatives, the pilot NCCEE project was initiated in 2022, and is being successfully implemented. To further support the vision of **"Estonia 2035"**, and make it a reality, the Estonian National Coordination Centre is focused to continue and enhance our efforts with **NCCEE2**. The **NCCEE2 project** is strongly aligned with **Estonia's national cyber strategy 2024–2030**, aiming at Estonia being the most resilient digital society. This strategy, developed amidst a complex global security environment and built upon the previous cybersecurity strategy (2019-2022), emphasises strengthening national security, boosting the resilience of critical infrastructure, and fostering a secure digital society.

NCCEE2 will focus on the following key elements from the **EU Cybersecurity Strategy for the Digital Decade**:

- **A reinforced presence on the technology supply chain.** The Strategy outlines that there should be a special focus on the development and use of latest cybersecurity tools developed by SMEs – especially the companies not subject to the revised NIS directive or NIS2. The objective is to "trigger a similar amount of investments by the Member States, to be matched by industry". NCCEE2 program on cybersecurity innovation will encourage such investments by small and medium cybersecurity companies in Estonia.

- **A Cyber-skilled EU workforce.** NCCEE2 will heavily contribute to this part of the strategy to develop, attract and retain the best cybersecurity talent and to invest in world class research and innovation. As the strategy pays special attention to diversity, NCCEE2 will continue to encourage women's participation in the STEM education and ICT-Cyber fields. NCCEE2 program for girls – the Cyber Wizards camp – has already proven to be an important contribution in this area.

Estonian Research and Development, Innovation and Entrepreneurship Strategy 2021-2035, particularly its focus "Digital Solutions in Every Area of Life," highlights cybersecurity as a critical element for Estonia's development. It emphasises the need for skilled human resources (skills and training) and interdisciplinary collaboration between businesses and researchers. These priorities align with Estonia's national goals and address gaps in the cybersecurity workforce and innovation ecosystems.

Building on the successful pilot phase of the initial NCCEE project, **NCCEE2** aims to further enhance national cybersecurity infrastructure and foster broad-based preventative measures to mitigate cybersecurity threats that align with both national priorities and broader EU digital security agenda.

The NCCEE2 will be complementary to the NIS2 implementation in Estonia. The National Cybersecurity Centre at the Estonian Information System Authority is the competent authority to enforce NIS2 among the critical sectors. This is done by providing CSIRT services to the public and critical sectors, building a

national information security standard, enforcing this standard and providing guidance on improving the cyber security posture in the NIS2 sectors. NCCEE2 acknowledges that this work cannot be done by RIA alone and a competent cybersecurity ecosystem must accompany this effort. Thus the NCCEE2 will ensure that:

- There is a vibrant cybersecurity marketplace to provide tools and services to the NIS2 subjects (as well as everyone else)
- The ecosystem invests in innovation in cybersecurity to meet the demand for services and tools
- There is a supply of competent, skilled people working to ensure the NIS2 subjects (as well as the rest of society) can safely digitize their lives.

Given these ambitious plans, the **NCCEE2** aims to tackle several significant challenges within Estonia's cybersecurity landscape, as highlighted in Estonia's 2024-2030 Strategic Plan for Cybersecurity. This plan emphasises the importance of strengthening the nation's cybersecurity capabilities in response to the increasing complexity and prevalence of digital threats, particularly as Estonia embraces advanced technologies such as artificial intelligence, robotics, machine learning, the Internet of Things, etc. The strategic vision seeks to establish a robust cybersecurity framework that supports the nation's digital transformation while safeguarding its critical infrastructure and economic growth.

An evaluation of the NCCEE deployment project progress and outcomes highlighted the following **Key Challenges** for the Estonian Cybersecurity Ecosystem, which the **NCCEE2** will be tackling using the respective **Solutions**:

- 1. Insufficient Focus on Cybersecurity Among Companies: As Estonia advances its digital initiatives, many businesses are still not adequately addressing cybersecurity risks associated with new technologies. Furthermore, a lack of investment in R&D activities and innovation in cybersecurity within many companies prevents the development of robust security solutions tailored to emerging threats. Without sufficient R&D, companies may struggle to innovate or stay abreast of rapidly evolving cybersecurity challenges.**
To address this gap, NCCEE2 will continue efforts to commission in-depth analyses, reviews, and training activities focused on the security implications of AI and robotics. Collaborating with Estonian cybersecurity researchers and institutions such as AIRE, these resources aim to enhance awareness and preparedness among companies and the broader community regarding emerging cyber threats. This aligns with the strategic objective of fostering a culture of cybersecurity that permeates all sectors of the economy.
- 2. Low Participation in EU Funding Opportunities: A critical challenge is limited engagement of Estonian cybersecurity companies in European Union funding initiatives, especially the Digital Europe Calls.**
To address this, NCCEE2 will actively promote funding opportunities available, providing administrative and technical support for application processes and project design. By serving as a central hub for facilitating collaboration among potential project participants, the project aims to boost the number of Estonian entities involved in international projects. This initiative aligns with the focus on enhancing the competitiveness of Estonian cybersecurity businesses and fostering innovation through increased participation in European funding mechanisms.
- 3. Cybersecurity Education and Workforce Diversity: Estonia's cybersecurity workforce remains predominantly male, and cybersecurity education is heavily focused on IT disciplines, limiting broader understanding and engagement across various sectors. This narrow approach restricts students and professionals from diverse fields, such as healthcare, finance, and public administration, from gaining essential cybersecurity knowledge, leaving critical sectors more vulnerable to digital threats. Additionally, gender imbalance in cybersecurity highlights a missed opportunity to draw from a broader talent pool, which could bring valuable perspectives and solutions to emerging challenges.**
NCCEE2 aims to address these gaps by continuing to promote cybersecurity education beyond traditional IT disciplines and also among groups underrepresented in the IT-world (e.g. girls). This effort will broaden understanding of cybersecurity principles across the workforce, equipping professionals to better recognise and address cyber risks in their respective fields. To tackle gender imbalance, the project will continue organising cybersecurity camps specifically aimed at young women and girls, aiming to break down existing stereotypes and encourage more women to enter the field. This approach aligns with the strategic objective of building a diverse, well-rounded cybersecurity workforce prepared to support Estonia's digital security across all sectors of the economy.

4. Fragmented Networking Opportunities within the Cybersecurity Community: lack of collaboration and communication among Estonian cybersecurity stakeholders poses a challenge to the sector's growth, and places limitations on the sector.

The project seeks to create networking opportunities that facilitate collaboration among cybersecurity companies, academia and public institutions. By organising events such as the ongoing "CyberMeetUp" series, the initiative aims to foster relationships that can lead to knowledge transfer and collaborative projects. Also, the project creates a platform for knowledge sharing and support that will allow the sector to access relevant information and events happening in the field to encourage the stakeholders. This is consistent with the strategic objective of strengthening partnerships across the cybersecurity ecosystem to enhance collective defence capabilities.

NCCEE2 is designed to comprehensively address the multifaceted challenges within Estonia's cybersecurity landscape, as outlined in Estonia's 2024-2030 Strategic Plan for Cybersecurity. By enhancing awareness, fostering diversity, improving skills, and facilitating collaboration, the project aims to create a more resilient cybersecurity environment. This environment will not only protect Estonia's digital infrastructure but also support its economic growth and innovation, ensuring that the country remains at the forefront of the global digital economy. Through these targeted efforts, the project aligns closely with Estonia's strategic vision of a secure, innovative, and resilient digital society.

The obvious mechanism for this is the long-term sustainability of the Estonian National Coordination Centre (NCC-EE) which needs to operate long-term, after the **NCCEE2** project has run its course. The **NCCEE2** project is therefore aimed at the sustainable impact and long-term strategic objectives that stem from the Regulation and the NCC-EE mission and vision. The mission is aligned with the strategic goals of the ECCC: to promote the development of the Estonian and European cybersecurity industry, technology, and research. The vision is focused on the cybersecurity market sector, the viability and the contribution it should provide:

NCC-EE vision: In Estonia, cyber security services are offered by viable, forward-looking companies with sufficient workforce focusing on research-based activities, which visibly contribute to the development of the sector across Europe, and the services of which are in strong demand both in Estonia and in the rest of the world.


The **NCCEE2** project will aim to cement the role of the NCC-EE into the Estonian Cybersecurity ecosystem through the four objectives stated above.

#§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.

N/A as per 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.

N/A as per 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.

As **NCCEE2** is the logical continuation of the deployment or pilot project NCCEE, most of the work proposed in this project is an advancement from the previous work with the goal of creating a sustainable impact in the Estonian Cybersecurity community.

This means the **NCCEE2** is built upon what NCC-Estonia has seen that has worked, continues with a similar team, the systems and processes that are already familiar and discards the components from the NCCEE deployment project that may not have had a significant impact. In terms of maturity, the **NCCEE2** project is based on the following:

NCCEE: The pilot NCCEE project began to strengthen Estonia's cybersecurity sector by boosting workforce diversity, fostering research and innovation, supporting SME cybersecurity adoption and enhancing community collaboration.

RIA as a competence center in cybersecurity: RIA has an established reputation as the cybersecurity powerhouse and knowledge center. The organization is not only reputable in the view of the public sector but has implemented a national cyber hygiene initiative aimed at educating citizens and businesses about basic cybersecurity practices to reduce the risk of cyber incidents. The cybersecurity specialist community, the NIS-NIS2 community, the community of auditors and the digital innovation community knows RIA as their cornerstone. The last years of increased hostilities in cyberspace have only solidified RIA's leadership in the field.

Public-Private Partnerships: As a small country, providing cybersecurity for the whole of society requires a partnership between public and private entities. This is in addition to the innovation, research and procurement part of the cybersecurity tools and services.

Existing and ongoing collaboration with Estonian Business Innovation Agency (EIS) and the Tehnopol Science and Business Park: Extensive discussions have identified Tehnopol as having the capacity and experience needed to undertake start-up focused activities of NCCEE. Tehnopol is well-known in the Estonian start-up ecosystem for its accelerator programs, which are crucial for enhancing science and business cooperation.

Professional Team and Budget Preparation: The consortium has assembled a professional team to carry out **NCCEE2** project activities, compiled provisional budgets, and estimated costs for various activities. Mapping of potential stakeholders and cooperation activities with research organizations such as TalTech University and Tartu University have also been completed.

#\$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 **NCCEE2** project will be divided into five distinct work packages (WPs) to efficiently allocate tasks among partners. Each WP will have designated leaders responsible for carrying out specific tasks. To ensure effectiveness, visibility, and sustainability, separate WPs will be dedicated to project management, coordination and the activities related to exploitation, dissemination, and communication.

The list of WPs is as follows:

WP No.	Title	Lead P.No.	Lead	Start Month	End Month
1	Management	1	RIA	1	48
2	Boosting Cybersecurity Entrepreneurship	1	RIA	1	48
3	Research, Development and Innovation in Cybersecurity	1	RIA	1	48
4	Next Generation of Cybersecurity Professionals	1	RIA	1	48
5	Exploitation, Dissemination and Communication	1	RIA	1	48

WP1: Management

The Management work package is essential for orchestrating success of the project. Like a conductor guiding an orchestra, it will help to ensure every task is executed harmoniously and efficiently. This package oversees planning, resource allocation, and scheduling, maximising productivity and minimising waste. It will also help in identifying and mitigating risks, ensuring the project stays on track and within budget. Furthermore, it will help to facilitate effective communication among stakeholders, providing regular updates and addressing concerns promptly. In essence, the management work package is the backbone of a well-coordinated, successful project, ensuring all elements work seamlessly together to achieve the successful outcome.

This work package contributes to the overall objective of sustainable impact and creating a culture of innovation in cybersecurity.

WP2: Boosting Cybersecurity Entrepreneurship

WP2 more directly supports the objective of creating a culture of capacity building by fostering the development of cutting-edge cybersecurity solutions. This work package drives the evolution of cybersecurity strategies and solutions, acting as the engine of innovation for the project. It focuses on supporting start-ups, who are designing innovative tools, and implementing transformative practices to enhance digital resilience. By fostering collaboration among stakeholders and mentors and aligning with EU cybersecurity objectives, WP2 facilitates progress towards the forefront of cutting-edge cybersecurity developments. It also supports further development of cybersecurity assessment methodology to address real-world challenges effectively and sustainably.

WP3: Research, Development and Innovation in Cybersecurity

WP3 merges technological innovation with innovation diplomacy to promote digital resilience and cross-border collaboration. It focuses on advancing European partnerships, finding synergies and supports building bridges between stakeholders - governments, cybersecurity industry, and research institutions - aligning diverse goals toward shared digital transformation objectives. By promoting active engagement in the DIGITAL programme and Horizon Europe, this work package motivates stakeholders to develop advanced solutions and strengthen their operational capacities within a coordinated European framework. This work package's main focus is the objective of promotion and encouragement of the culture of research, development and innovation.

WP4: Next Generation of Cybersecurity Professionals

This work package addresses the critical shortage of cybersecurity professionals by developing targeted training programs and directing young people to exciting careers in the field of cybersecurity through internships and incentives and prizes. Navigating complexities of the digital future will be made easier by a set of policy papers aimed at policy makers echoing challenges and interests of members of the cybersecurity community in Estonia.

WP5: Exploitation, Dissemination and Communication

The Exploitation, Dissemination, and Communication work package is the lifeline of a project's visibility and impact.

Exploitation will help to ensure that the project's results are put to practical use across Estonia and the EU. This involves identifying potential users, stakeholders, and industries that can benefit from the project's outcomes, ensuring long-term sustainability and return on investment. Exploitation will also focus

on long-term capacity to work independently of EU funding and on creation of independent resilience of Estonia in cybersecurity activities.

Dissemination helps spread the word about the project's achievements and progress. This process involves sharing information through various channels such as publications, conferences, social media, and websites, making the project more transparent and accessible to a broader audience within Estonia and beyond.

Communication will act as the project's voice, engaging with stakeholders, partners and the public. This involves maintaining a consistent flow of information, addressing questions, and fostering a positive image of the project.

By effectively conducting exploitation, dissemination and communication, the **NCCEE2** project will be able to maximise its impact, ensure that its findings are utilised, and build a strong, supportive community around its objectives.

The **NCCEE2** is built on the previous pilot NCCEE project and other projects, below is a short overview of the projects that have formed the groundwork for the **NCCEE2** project

NCCEE or "Cybersecurity Community Building Activities and Deployment of the Estonian National Coordination Centre": The project commenced in March 2023, with a life-span of 24 months. The project sought to advance Estonia's cybersecurity sector by enhancing essential capacities and boosting overall capabilities. It had four main objectives:

- Increasing the number of specialists and young people trained in cybersecurity, with a special focus on women and girls.
- Enhancing the practical application of research, development, and innovation within the cybersecurity market and other sectors.
- Encouraging the adoption and dissemination of state-of-the-art cybersecurity solutions by SMEs.
- Strengthening the cybersecurity community and ecosystem through events and information-sharing activities among relevant stakeholders, including communication on cross-European cybersecurity projects.

The project consortium aimed to achieve these goals through dedicated Work Packages designed specifically to progress towards a Cybersecure Estonia.

EU Cyber Capacity Building Network: Initiated in 2019, EU CyberNet involved a four-year plan to accomplish four key objectives: creating a network of cybersecurity experts and stakeholders, establishing a technical platform, offering training and support, and evolving into a knowledge centre for the EU's external cyber activities. By leveraging expertise across the European Union, EU CyberNet sought to form a collaborative network and a practical learning platform to enhance global cybersecurity. The insights provided by contributing experts helped shape EU policies towards partner countries in the field of cybersecurity.

Cyber Resilience for development: Cyber Resilience for Development (Cyber4Dev), an initiative by the European Union, focused on enhancing cyber-resilience and cybersecurity to safeguard both public and private sectors worldwide. This multi-million Euro investment aimed to protect economic and social development, vital community infrastructure, and national security systems. It benefitted all citizens, public agencies, and private enterprises in the participating countries. The project aspired to ensure that everyone can enjoy an open, free, secure, and resilient cyberspace.

Regional policies for competitive cybersecurity SMEs: Interreg Europe CYBER sought to enhance the competitiveness of European cybersecurity SMEs by fostering synergies among European Cybersecurity Smart Regions. The European Regional Development Fund (ERDF) allocated EUR 1.53 million to this five-year interregional cooperation program to achieve this goal. By undertaking various interregional cooperation initiatives, CYBER aimed to facilitate the exchange of best practices, improve public policies, and strengthen cybersecurity ecosystems. The project includes seven European regional partners: Institute for Business Competitiveness of Castilla y León (Spain), Tuscan Region (Italy), Digital Wallonia (Belgium), Brittany Region (France), Kosice IT Valley (Slovakia), Chamber of Commerce and Industry of Slovenia (Slovenia), and Estonian Information System Authority (Estonia). The Bretagne Development Innovation agency served as the leading partner in this initiative.

Empowering a Pan-European Network to Counter Hybrid Threats: EU-HYBNET (Empowering a Pan-European Network to Counter Hybrid Threats) is funded through the European Union's Horizon 2020 research and innovation programme. The project aimed to strengthen existing European networks that

counter hybrid threats and ensure their long-term sustainability. To achieve this, the project identified the common requirements of European practitioners and other relevant actors in the field of hybrid threats. This initiative ultimately aimed to fill knowledge gaps, address performance needs, and enhance the capabilities of research, innovation, and training efforts related to hybrid threats.

The above project initiatives have helped to build a robust foundation across the cybersecurity environment. Using them, and facing escalating challenges in cyberspace, the **NCCEE2** project intends to develop, fortify and expand the cybersecurity sector across Estonia, also benefiting other European Member States.

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.

The coordinators and collaborators behind NCCEE2 understand that effective project management is essential for the effective completion of large-scale projects because it provides an organised approach to planning, execution, and monitoring operations. Project management keeps activities on track and coordinates team efforts towards shared goals by defining roles, providing defined targets, and creating schedules. Teams can make timely adjustments and avoid delays by identifying problems early with the use of ongoing monitoring and evaluation. Additionally, effective risk management and resource allocation guarantee that project deadlines are reached and budgets are followed. Finally, project management promotes efficiency through better collaboration, communication, and accountability, all of which help to produce excellent results on time. Over the years, RIA has accumulated a significant amount of experience in overseeing complex technology-focused and cybersecurity projects.

To guarantee that project implementation stays on schedule and achieves high standards, RIA will lead continuous project management. RIA will use project management tools, like Confluence and Jira to track timelines and important milestones.

RIA also has extensive experience in quality assurance for technology-driven projects. A comprehensive Quality Plan will be created, based on proven quality assurance frameworks, to routinely monitor and assess the project's activities, deliverables, and results. This systematic strategy will keep the project on track and meet the expectations of all stakeholders.

Other than tracking the key performance indicators set out in this project proposal and updated regularly with incoming data, RIA's project quality assurance approach will assess seven essential components of quality: performance, cooperation, resource utilisation, information management, output, service supply, and dissemination. Each area will be examined using focused questions and indicators to determine the project's alignment with objectives, partner engagement, resource efficiency, and information sharing efficiency. The effectiveness of joint activities will be measured by measuring partner contributions and stakeholder involvement, while resource management will concentrate on budgeting and the proper use of both monetary and non-monetary resources. A preliminary set of questions and indicators to utilise is following:

Project's Alignment with Objectives

Did activities meet intended objectives?

Do results align with target group needs?

Was each partner's contribution consistent with the project plan?

Indicators: Percentage of objectives achieved, degree of alignment with target group needs, and compliance rate of partner contributions.

Engagement with Partners

Was collaboration among partners satisfactory?

Did each partner contribute to project goals?

Were project meetings effective?

Indicators: Partner contribution effectiveness, satisfaction with collaboration, number and diversity of actively engaged stakeholders.

Efficient Use of Resources

Were resources utilised appropriately?
Were expenditures documented and compliant with regulations?

Indicators: Budget utilisation rate, compliance with regulations.

Effectiveness of Information Sharing

Was information shared in a timely manner?
Were documents organised and secure?
Was there a version control system for documentation?

Indicators: Timeliness of information sharing, document accessibility, and utilization rate of version control systems.

These targeted questions and indicators will provide a clear framework for ongoing monitoring, helping to ensure effective management and high-quality project outcomes.

To ensure information is managed effectively, RIA will use systems for secure document sharing and version control, guaranteeing timely access to updated project materials. Each deliverable will be assessed against technical standards to ensure quality. For service or product delivery, RIA will ensure that outputs meet the needs of the target audience, are user-friendly, and adaptable to feedback from stakeholders. Finally, RIA will monitor dissemination efforts to verify that project achievements are communicated effectively and that the project's impact reaches a broad audience. Quality assurance updates will be provided regularly and most important issues identified will be addressed by the Project Steering Committee (SC).

To monitor and verify project impact, RIA will employ both quantitative and qualitative evaluation methods. Quantitative metrics will track specific objectives against an expected results framework, with ongoing monitoring of progress throughout the project lifecycle. This approach will include assessing the number of stakeholders involved, participation in project events, workshops, research initiatives and other engagement activities.

Qualitative assessments will complement these metrics by evaluating the impact of project activities. Methods such as content analysis and self-reflective discussions with stakeholders will provide insight into the perceived quality and relevance of project outcomes. Evaluation will be used to measure both the progress and quality of each work package, and key indicators will be designed to be specific, measurable, achievable, relevant, and time-bound (SMART).


Evaluation criteria will include metrics such as the number of best practices identified for cybersecurity, the number of stakeholders engaged from various sectors (e.g., SMEs, startups, academia), and the number of innovation and R&D initiatives supported. Dissemination and communication activities will also be evaluated according to defined standards, ensuring both breadth of outreach and depth of engagement. These comprehensive evaluation strategies will enable RIA to maintain a high level of oversight, ensuring the project's alignment with goals and a meaningful impact on target groups.

Beyond the proposed quality assurance methods, the consortium partners in this project (RIA, EIS, Tehnopol) are subject to oversight by the governmental bodies overseeing the progress and processes. In this way the achievements and activities will be subjected to quality control and impact assessment through multiple ministries in Estonia. This level of bureaucracy may seem overburdening, but will ensure cost effectiveness and level of impact on a political level.

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.**

To ensure that project goals and objectives are completed in the most cost-effective manner, the consortium has been carefully built to include partners whose experience closely matches the project's essential skills. RIA is a government agency and it follows a fixed government procurement process and procedures to ensure cost effectiveness of services bought.

Each partner has been assigned duties related to their area of expertise, allowing for more efficient resource utilisation, and decreasing the need for external assistance. This strategy enhances efficiency because each partner provides specific knowledge and tools that aid in the seamless creation and

implementation of the project's outcomes. The project work plan strikes a balance between three critical areas: effective project management, quality assurance, and development and implementation activities. Furthermore, the work plan provides adequate resources for dissemination and exploitation efforts, ensuring that project products reach a large audience.

RIA will centrally handle the project's financial administration with a focus of streamlining operations and increasing accountability. Financial resources will be distributed in instalments to project partners, who submit expense reports regularly. RIA will provide a detailed explanation of reporting requirements and procedures. This centralised management strategy will allow for effective budget monitoring and ensure that funds are only spent for qualified expenses.

To support compliance and maintain transparency, the Project Coordinator (PC) will advise project partners, so that all financial records and procurement processes adhere to Digital Europe requirements. If any issues arise regarding fund eligibility or adherence to the Granting Authority (ECCC) reporting guidelines, the PC will consult with the concerned partners to provide clarification. The PC will review, validate, and seek clarification on reported costs as necessary, confirming their eligibility according to ECCC standards.

This comprehensive financial management strategy, with regular oversight and open communication, will ensure that resources are effectively allocated, eligible, and fully documented throughout the project lifecycle.

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 success of the NCCEE pilot project demonstrated the effectiveness of the consortium's collaborative approach. Building on this success, the consortium for Phase II of the NCCEE will again include the Estonian Information System Authority (RIA), the Estonian Business and Innovation Agency (EIS), and Tehnopol. Each partner brings essential expertise that complements the others, allowing for a comprehensive approach to achieving the project's goals. The division of roles, the unique strengths of each participant and familiarity of work practices, ensure that all required skills for the project's success are readily available within the consortium.

Project coordinator **RIA** will oversee the **NCCEE2** project, providing general coordination and leadership to achieve its goals. With its strategic role within Estonian digital ecosystem, RIA is responsible for administering and coordinating the state's information systems, ensuring security and interoperability, and protecting Estonia's critical digital infrastructure. As Estonia's primary authority on cybersecurity, RIA will lead all cybersecurity policy initiatives under the project. It will also coordinate academic partnerships to promote cybersecurity research and organise outreach efforts, including training and community events for public and private sector participants. RIA's active role in cybersecurity training and its connections with both national and international stakeholders position it as the central force behind the **NCCEE2** project's objectives.

EIS contributes to the project with its expertise in supporting business and economic development within Estonia. Formed through the merger of Enterprise Estonia and KredEx, EIS is a national foundation dedicated to fostering economic growth and innovation across the country. In the **NCCEE2** project, EIS will oversee most sub-granting activities, bringing its substantial experience in managing grant applications, awards, and verification procedures. With a history as an Implementing Agency for Structural Funds, EIS has the infrastructure, processes, and knowledge required to handle complex grant programs effectively. EIS will also leverage its experience in stimulating business development and innovation to support the **NCCEE2** project's focus on fostering a dynamic and competitive cybersecurity ecosystem within Estonia.

Tehnopol, as the largest science and business park in the Baltics, brings extensive expertise in supporting startups and fostering entrepreneurship. Founded by the Estonian Government, the city of Tallinn, and Tallinn University of Technology (TalTech), Tehnopol offers a comprehensive support structure for

companies, including office spaces, business advisory services, and real-life test environments. Within the **NCCEE2** project, Tehnopol will be responsible for activities related to startup engagement, leveraging its vast experience in business support, mentoring, and innovation testing. Tehnopol's proven track record in supporting over 500 startups and its connections with over 400 technology companies, including global leaders like Microsoft and Starship Technologies, makes it ideally suited to cultivate the growth of cybersecurity startups. Additionally, Tehnopol's expertise in managing various national and European projects ensures that it has the resources and project management skills needed to drive **NCCEE2** project's objectives for entrepreneurial development in cybersecurity.

Each consortium partner has a clearly defined role that leverages its core strengths, creating a balanced and well-resourced team. RIA, EIS, and Tehnopol will coordinate closely to ensure seamless implementation, with RIA leading coordination efforts, EIS handling sub-grant management, and Tehnopol focusing on startup support. Regular coordination meetings and open communication channels will enable efficient collaboration and decision-making across the consortium, ensuring that each partner's contributions are fully aligned with the project's objectives. This division of roles ensures that the consortium has all the necessary expertise, resources, and infrastructure to fulfil the project's requirements effectively.

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
Lauri Tankler, Head of Cybersecurity Research and Development Coordination, Project Lead	Estonian Information System Authority (RIA)	<p>A former journalist and teacher, he has been analysing cybersecurity threats, engaging in international cooperation at RIA, focusing on the cybersecurity of election technologies and raising public awareness on cyber threats for the last four years through training, media appearances and ad campaigns.</p> <p>Lauri is responsible for leading a project team that ensures the implementation of a project with high-quality and efficacy. He is in charge of operations, improving systems, mitigating risks, and delivering strategic solutions. He ensures the implementation of optimal methodologies to facilitate long-term planning, status reporting, and process enhancements, while closely monitoring key performance indicators.</p> <p>He is the first and current head of the Network of NCCs, serving a second term.</p>
Airi Aljas, Project Coordinator (PC)	Estonian Information System Authority (RIA)	<p>Airi has completed the "PRINCE2®" training in project management. She has over 10 years of experience managing domestic and international projects of various sizes, ensuring that project objectives are achieved according to the plan. The PC is in charge of the project's overall coordination. PC's responsibilities include ensuring the smooth operation of daily project activities, managing coordination between all project partners, coordinating administrative and financial reporting, and acting as the main communication link between the project and the ECCCs Project Officer.</p>
Hendrik Pillmann, Expert Coordinator, Work Package Leader	Estonian Information System Authority (RIA)	<p>Hendrik obtained a bachelor's degree in political science, majoring in international relations and master's degree in homeland security. In his master's thesis Hendrik focused on the security of Internet of Things technology. Hendrik has worked as a teacher of natural and social subjects in Estonian general education schools and has also</p>



Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

		been in the service of the Police and Border Guard Board, dealing with the prevention, pre-trial proceedings, and coordination of aspects of cybercrime. In NCCEE2 Hendrik oversees the activities under WP3 and ensures that the different parties involved in WP2 tasks fulfill their responsibilities efficiently.
Tiina Pau, Expert Coordinator, Work Package Leader	Estonian Information System Authority (RIA)	Tiina Pau has studied educational technology at the master's level and worked as a teacher of mathematics and computer education, an educational technologist and conducted various extracurricular activities in school (including robotics). In the Board of Education and Youth and the Ministry of Education and Research, she had to coordinate the development of the national mathematics curriculum for grades 1-12 and activities related to the development of digital competences, as well as international communication on this topic and the coordination of Erasmus+ projects on the Estonian side. In NCCEE2, she is responsible for the detailed coordination, planning, monitoring and reporting of Work Package4.
Birgit Buldas, Expert Coordinator, Work Package Leader	Estonian Information System Authority (RIA)	The previous NCCEE project gave Birgit valuable experience, leading the activities under Work Package 2. In the NCCEE2 project, she will continue to oversee the WP2 activities and collaborate closely with partners to guarantee that the objectives of WP2 are coordinated, planned, and executed in accordance with the initial plan.
Kaisa Lindenburg, Expert Coordinator	Estonian Information System Authority (RIA)	Kaisa primarily serves the role of Community Manager in the project and is responsible for building, engaging, and maintaining relationships within the community. She is also responsible for organizing activities and events to grow the community and attract new members.
Acceleration Program Coordinator	Tehnopol	The Program Coordinator is in charge of the accelerator program, which is designed for the creation and development of new start-up companies in the field of cyber security, built and implemented on the principle of sprints, where group activities alternate with individual activities. The Program Coordinator works closely with the WP leader to ensure effective planning, coordination, and execution of all activities regarding the Acceleration Program.

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.

Based on current experience from the pilot NCCEE project, the NCCEE2 project will not use subcontracting for any services.

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.*

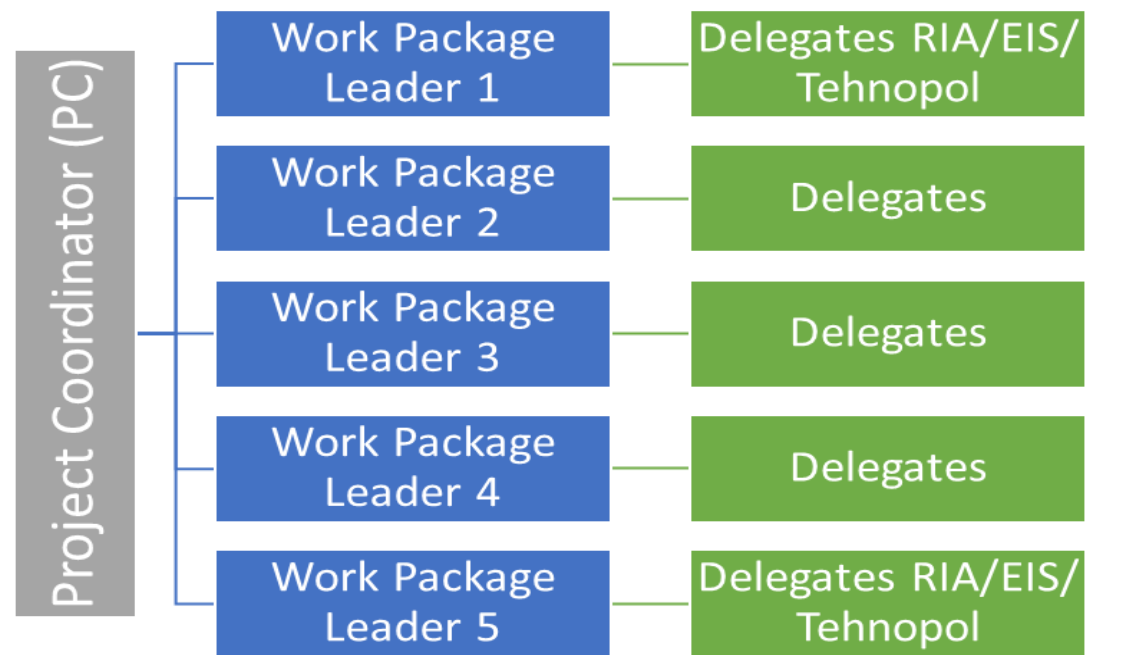
The project will be governed by a Project Steering Committee (SC), which will include representatives from RIA, EIS, Tehnopol, and if adequate, then also Work Package leaders (WPL), established at project inception. The SC will be led by the Project Coordinator (PC) from RIA, who is responsible for guiding the project. The inclusion of diverse members from the consortium ensures that each stage of the project is informed by relevant expertise.

The PC will define and implement operational, administrative, and technical protocols while establishing essential project management tools and infrastructure. Acting on behalf of the SC, the PC will oversee all project activities, including setting up task lists, deliverables, and milestones for each consortium member. The PC will also track progress to ensure that the project remains on schedule. Key responsibilities include implementing communication strategies, risk management procedures, progress reporting, and dispute resolution. Additionally, the PC will handle financial oversight, helping consortium members to maintain proper records and documentation of project expenses, adhering to regulatory requirements.

For each work package, the PC will determine and approve the resources and requirements needed for successful delivery. The PC will monitor the progress of activities across all work packages, ensuring that they align with project objectives and are integrated effectively.

To monitor progress and discuss future steps, the SC will hold regular meetings, either in person or virtually. During these sessions, any planning changes, project delays, or required adjustments will be reviewed and discussed. Decisions, including those affecting project scope or timelines, will be made collectively with the PC's approval to maintain alignment. Detailed meeting minutes will be documented to provide a record of decisions, project changes, and any schedule adjustments.

In compliance with funding regulations, the PC will compile and submit regular progress reports covering all consortium activities, which will help maintain project oversight and provide a clear record of progress for all consortium members. These mechanisms, together with progress checks and transparent communication, will ensure effective coordination and continuous alignment with project objectives throughout the project lifecycle.



#\$CON-SOR-CS\$# \$#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

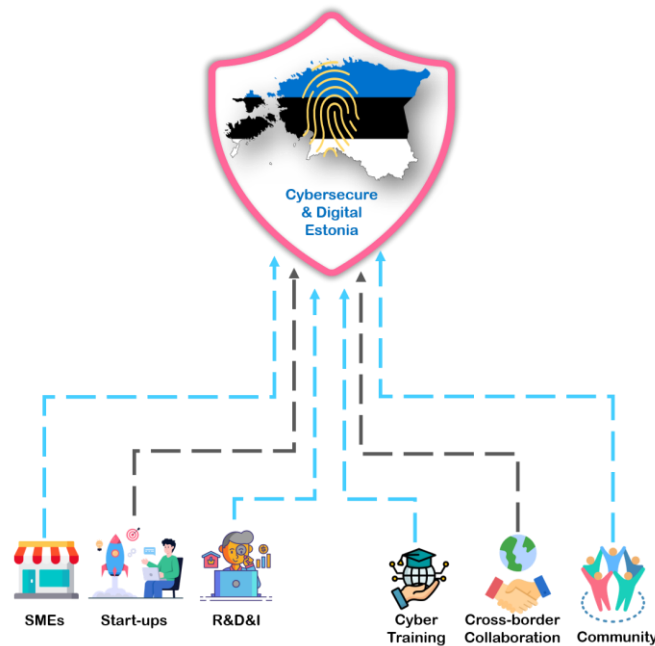
Define and explain the extent to which the project will achieve the expected impacts listed in Call document.

The **NCCEE2** project is designed to achieve a range of impactful outcomes that will contribute to the advancement of Estonia's cybersecurity landscape and strengthen the EU's broader digital security ecosystem. The expected impacts, as outlined in the Call document, will be realised through planned initiatives focused on fostering innovation, collaboration, talent development, and business growth. Below is an explanation of the expected outcomes and deliverables:

1. **Accelerator program - 18 start-ups funded** in total: As part of the project's commitment to nurturing innovation, the accelerator program will continue to provide funding to start-ups working on cybersecurity-related solutions. The expected outcome is the funding of 3 times 6 start-ups over the course of the project. By supporting these early-stage companies, NCCEE2 will help stimulate the development of innovative cybersecurity technologies, enhancing Estonia's role as a hub for cutting-edge cybersecurity solutions in Europe.
2. **Cyber Innovation Grants:** A key deliverable of NCCEE2 is the provision of Cyber Innovation Grants, with **15-20 grants** allocated across three critical areas which are aligned with the focus areas of the Digital Europe Cybersecurity Programme for 2025-2027 (and hopefully beyond): Automation of Cybersecurity, Artificial Intelligence (AI) for Cybersecurity and Transition to Quantum-Safe Cryptography. These grants will support a consortium of companies and academic institutions over 3 years, fostering collaboration between industry and academia. With involvement from **20 or more entities**, this initiative will advance research and development in cybersecurity technologies, contributing to the EU's global leadership in these emerging fields.
3. **Entities Engaged in the Community – 40 Entities Regularly Involved:** NCCEE2 aims to actively involve 40 entities in its community on a regular basis, promoting continuous engagement through networking events, knowledge-sharing platforms, and collaborative initiatives. This engagement will foster a consistent cybersecurity ecosystem where businesses, academia, public institutions, and individuals work together to address emerging cyber threats. The broader involvement of entities will also help build a more resilient digital infrastructure across the EU.
4. **Entities Supported in Cyber Business & Diplomacy Program – 10 Entities:** The project will provide targeted support to 10 entities through the Cyber Innovation Diplomacy and Pathway to Cross-Border Project program. This includes facilitating their participation in international events, offering individual advisory services, and fostering connections with key stakeholders in the global cybersecurity landscape. By enhancing the visibility and reach of Estonian cybersecurity companies and organisations, **NCCEE2** will contribute to Estonia's strategic positioning within the EU's cybersecurity framework and promote its international cybersecurity diplomacy efforts.
5. **Collaboration Actions – 8 Digital Europe/Horizon Europe Introduction Events:** NCCEE2 will host 8 call introduction events about Digital Europe Cybersecurity calls and/or Horizon Europe Cybersecurity related calls over the duration of the project, with two events held each year. These events will serve as platforms for introducing Digital Europe calls, fostering cross-border collaboration and facilitating partnerships between stakeholders from various sectors. By encouraging collaboration between companies, researchers and policymakers, these events will support the creation of innovative solutions and strengthen cybersecurity networks within the EU. The brokerage events will also promote knowledge exchange and the sharing of best practices, further enhancing the EU's collective cybersecurity capabilities.
6. **3 international DIGITAL information days** or brokerage events organized by RIA in Tallinn, Estonia to encourage international cooperation and establish collaboration between relevant entities at national, regional and local levels. These events will further facilitate participation of civil society, industry in particular start-ups and SMEs, academic and research communities and other actors in cross-border projects and cybersecurity actions funded through all relevant Union programmes. In addition to this NCC-EE will send participants to other events in the region, fostering collaboration with European cybersecurity partners.
7. **DIGITAL funding consultations** – at least **10 community member SMEs** yearly. NCCEE2 will provide consultations and technical assistance to a total of 30 SMEs in Estonia from the 2nd year of the project, by supporting the stakeholders in their application phase for projects managed by the ECCC.
8. **Summer Camps for Young People – 4 1-week summer camps and 8 1-day training camps:** As part of its commitment to fostering the next generation of cybersecurity talent, NCCEE2 will organise 4 summer camps aimed at young people, with a particular focus on encouraging girls to pursue careers in cybersecurity. These camps will provide hands-on learning experiences, mentorship, and exposure to the cybersecurity field, aiming to break down gender stereotypes and inspire a more diverse future workforce. Shorter camps will introduce cybersecurity to young people and motivate them to engage more actively with this lucrative and relevant field. By targeting young girls, the project will contribute to closing the gender gap in cybersecurity and ensure a more inclusive and resilient workforce for the future.

9. **CyberMeetUps – A total of 36 events**, 9 per year will foster community engagement in Estonia. CyberMeetUps will continue to be a great way to promote and disseminate the relevant outcomes of the work of the Network of NCCs and the ECCC at national, regional and local level. These events will also be helpful in 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.
10. **Internship programs – at least 30 cybersecurity interns** have been introduced by **NCCEE2** to different public and private internship positions. A well-coordinated internship program promotes peer-to-peer learning and helps to equip organisations with the latest and most effective tools and strategies available for cybersecurity, fortifying their overall cybersecurity capabilities, and helping them to become more resilient and better prepared to face the evolving challenges posed by cyber threats in the digital age.

Through these outcomes, **NCCEE2** is set to have a significant impact on the cybersecurity ecosystem in Estonia and the EU. By focusing on fostering innovation, supporting start-ups, providing funding opportunities for R&D&I and increasing the engagement of SMEs and other entities, the project will strengthen the EU's cybersecurity resilience. Additionally, by fostering collaboration, supporting international cyber-diplomacy efforts, and promoting education and diversity in the cybersecurity workforce, **NCCEE2** will contribute to the broader goals of digital security and economic growth across Europe. These actions align with EU priorities and will enhance the overall cybersecurity infrastructure, ensuring Estonia and the EU remain at the forefront of the global cybersecurity activities.



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.*

The dissemination and communication activities of the **NCCEE2** project are designed to ensure that the project's results and activities reach a wide audience, including relevant stakeholders, policymakers, and the general public. By strategically promoting the project's initiatives and outcomes, the project aims to maximise its impact and demonstrate the tangible benefits for society, particularly in terms of improving digital security and enhancing resilience in the face of evolving cyber threats. The communication activities will be led by RIA, who will bring in their experience from the pilot NCCEE project to the table. Communication plan from previous NCCEE project will be updated to include the needs and requirements of the **NCCEE2** project, and will be put forth during the first SC meeting, along with review, evaluation, and updates every twelve months. The revised plan will include to focus on three primary areas: (1) establishing the expected impacts and key messages, (2) detailing communication channels, and (3) clearly distributing roles and responsibilities among consortium partners, each with assigned Key Performance Indicators (KPIs) to measure the impact and effectiveness of outreach activities.

The plan will identify crucial impacts and objectives for the **NCCEE2** project, centring on strengthening cybersecurity resilience, fostering collaboration, and advancing Estonia's integration within the EU's cybersecurity initiatives. Key messages will emphasise **NCCEE2's** role in strengthening the national cybersecurity infrastructure, supporting proactive risk management, and showcasing international collaboration opportunities through European programs like Digital Europe and Horizon Europe.

Central to the communication strategy are different communication activities, which are led by Work Package Leaders, who will actively contribute to the implementation of the plan alongside the PC. Coordinated effort ensures that project outputs are accessible and clearly presented, event planning and organisation is coordinated, and consortium partners are supported, when delivering presentations at conferences, workshops, and other key gatherings.

To maintain alignment and consistency, the Work Package Leaders and partners will actively oversee all communication activities, ensuring that core messages are precise, relevant, and unified across all channels.

To ensure broad outreach and visibility, the project will utilise a variety of communication tools and channels. There are some events that are within the scope of our project:

- Local annual events: 2 different RIA annual conferences/symposiums, Cycon conference, Latitude59, STartuPDay, B-Sides, Tallinn Digital Summit, Estonian National Cybersecurity Conference, Cyber Battle for Baltics-Nordics, teachers conferences and other nationally important events.
- International visibility will be determined upon the interest of the local community but will definitely include brokerage events held by different NCCs all around Europe.

Key events for disseminating results and promoting knowledge exchange will be the ongoing "CyberMeetUp" series and brokerage events. CyberMeetUp's will be organized monthly and brokerage events twice a year, bringing together stakeholders from industry, academia, public institutions, and other relevant sectors to discuss the latest developments in cybersecurity, share best practices and foster collaboration. The events will also highlight the project's achievements and innovations, and promote opportunities for further engagement and funding, particularly through EU initiatives like Digital Europe. Each CyberMeetUp will be recorded and published on RIA's YouTube channel, resulting in at least **36 recordings** for the Estonian cybersecurity community. Additionally, an estimated **4 videos** from other events will be produced during the project.

In addition to traditional communication channels, a dedicated online platform will be developed to facilitate knowledge and resource sharing among stakeholders. This platform will serve as a central hub for cybersecurity-related resources, best practices, research findings, and event information. It will allow for easy access to key materials, enabling stakeholders and the general public to stay informed and collaborate on cybersecurity initiatives. The platform will also help cybersecurity community members to engage in national and international cooperation, promoting registration in ATLAS and mapping of competencies of various actors in Estonian cybersecurity landscape.

To reach the general public and create widespread awareness, the project will utilise popular social media channels (e.g., LinkedIn, Twitter, Facebook) of RIA and the website to share project updates, educational resources and event information. Information about NCCEE2 activities will be publicly available through RIA and other stakeholders, with an estimated **20 online media posts** per year.

NCCEE's dissemination activities will be closely coordinated with other National Competence Centres (NCCs) in the region, particularly those in Latvia, Lithuania, Finland, and Sweden. By organising joint events and sharing resources, the project will amplify its impact and create a more cohesive cybersecurity

network within the Baltic Sea region. This regional cooperation will facilitate cross-border knowledge-sharing and enhance the visibility of NCCEE2 results.

Regular articles in relevant newsletters will help a broad range of stakeholders, including SMEs, academia, and government bodies, to be informed about key project activities, funding opportunities and the latest developments in cybersecurity. In order to guarantee broad visibility and engagement with NCCEE2 initiatives, approximately **20 news pieces** will be published in Estonian media.

Major dissemination events, such as brokerage events, will be organised in collaboration with other NCCs and the European Cybersecurity Competence Centre (ECCC) to ensure broad participation and alignment with EU cybersecurity goals.

Indicative dissemination, communication, and promotion goals	Desired outcome over 48 months
News media articles <ul style="list-style-type: none"> - Cybersecurity Accelerator - Cybersecurity Innovation Grants - Skills initiatives - Community events - etc. 	20
Social media posts on beneficiaries' platforms <ul style="list-style-type: none"> - RIA - Tehnopol - EBIA 	80 (20 per year)
Dissemination, communication, promotion events <ul style="list-style-type: none"> - RIA CyberMeetUp - Info Days, Brokerage events on cross-border funding opportunities 	44
Dissemination, communication, promotion videos <ul style="list-style-type: none"> - RIA's YouTube Channel 	40+

Main goal of these dissemination efforts is to ensure that the results of **NCCEE2** reach those who stand to benefit the most. By involving a wide range of stakeholders and using a variety of communication channels, **NCCEE2** aims to increase awareness about the importance of cybersecurity and the resources available to businesses, researchers and individuals. RIA will also seek to inform and engage the broader public on how improved cybersecurity contributes to overall societal well-being, privacy and economic stability.

In short, the **NCCEE2** project will employ a comprehensive approach to dissemination, incorporating both traditional and digital communication tools to reach diverse audiences. By hosting targeted events, engaging in cross-border collaborations, developing a platform for knowledge sharing and providing informative resources **NCCEE2** will ensure that its results and impact are effectively communicated, fostering a safer and more resilient digital environment for all stakeholders involved.

#§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 **NCCEE2** project is designed in a way that proposes a longer term, sustainable impact for the cybersecurity private sector that has never been done before. The key parts of this project are grants to develop new, automated tools to provide cybersecurity, and the processes around these grants to help the community members reach a maturity to keep innovating even after the **NCCEE2** project has been completed.

The key here is the Financial Support to Third Parties schemes that have been designed to ensure sustainable impact over the 4 years of the project. The project consortium partners will ensure through the FTEs that the community members would be ready and willing to participate in both Estonian grants

projects and cross-border projects. The financing is well placed and the NCC-EE team will be able to guide the community to effectively utilize those grants.

Aside from the grants, through targeted support and partnerships, **NCCEE2** seeks to drive economic growth, improve public trust in digital systems and create a safer, more inclusive digital ecosystem.

NCCEE2 aims for the following societal benefits:

Enterprise Level

NCCEE continues the CyberAccelerator Program, funding a total of **18 start-ups** to encourage growth and innovation in the cybersecurity field. Through Cyber Innovation Grants, which focus on AI for cybersecurity, quantum-safety, and cybersecurity automation, **NCCEE2** will award **15-20 grants** across these priority areas, engaging at least **20 entities** in collaborative R&D efforts. By fostering partnerships between academia and industry, **NCCEE2** promotes the development of advanced solutions and enables enterprises to integrate cutting-edge cybersecurity innovations into their operations and product/service offerings.

NCCEE2 also supports **10 entities** within its Cyber Business & Diplomacy program, providing them with opportunities to participate in international events, connect with industry peers, and access tailored advisory services. Furthermore, to boost cross-border networking and collaboration, **NCCEE2** will host **8 DIGITAL call introduction events** over the project duration (two each year), facilitating knowledge-sharing and market expansion opportunities for Estonian businesses in the EU and beyond. These initiatives collectively empower SMEs and start-ups to enhance their cybersecurity positions, fostering innovation and helping European enterprises to compete effectively on the global stage.

Educational Level

A strong emphasis on cybersecurity education and workforce development lies at the heart of **NCCEE2**. The project aims to cultivate a skilled and diverse talent pool capable of supporting developing cybersecurity needs of Estonian and European economies. By fostering cybersecurity education across traditional IT fields as well as in sectors like healthcare, finance, manufacturing and other businesses **NCCEE2** ensures that professionals from various backgrounds gain critical cybersecurity skills. Furthermore, **NCCEE2** engages young people, especially girls, through initiatives like **4 cybersecurity summer camps**, cultivating early interest in cybersecurity and setting them on a path toward careers within the cybersecurity and technology fields. In addition, the project's communication and dissemination efforts help to promote cybersecurity literacy, empowering citizens to protect personal data, recognise digital threats, and confidently participate in digital society. This widespread educational focus is essential for building a resilient, digitally savvy society.

Although the impact from the youth camps can be seen only further in the future, the rest of the innovation activities (start-up grants and innovation grants) should be able to demonstrate the level of attention and awareness given to cybersecurity for people to see the long-term benefits of engaging with the field.

Community Level

NCCEE2's community-focused strategy aims to build a secure and digitally aware public environment. The project enhances the security of essential public services, including healthcare, education, and governance, contributing to public trust in Estonia's digital systems and supporting the nation's digital economy. In addition, it will ensure that **40 entities** are regularly engaged through community events and initiatives, fostering collaboration among cybersecurity stakeholders.

NCCEE2 actively promotes youth engagement in cybersecurity, with a strong focus on encouraging young people to consider careers in the field, aiming to bridge gender gaps and create pathways to jobs in cybersecurity and technology. Through community-level cybersecurity programs, **NCCEE2** equips citizens with the knowledge to safeguard personal data, recognise online threats and make informed decisions about data protection. To further facilitate international collaboration, **NCCEE2** will support stakeholder registration in the European Cybersecurity Atlas and provide access to the Cybersecurity Community Hub on the NCCEE website. This hub will feature an exchange platform for knowledge, mentors and contacts, offering a valuable resource for professionals, students, and educators. By creating an inclusive and well-connected community, **NCCEE2** ensures a secure digital environment that benefits both public and private sector organisations across Estonia.

Through a multi-level approach spanning education, enterprise support, and community outreach, the **NCCEE2** project is set to drive substantial gains in digital resilience and competitiveness across Estonia and the EU. By supporting cybersecurity R&D&I, empowering SMEs, and fostering cross-border collaboration, **NCCEE2** strengthens the digital infrastructure necessary for economic growth and technological advancement. Focus on fostering skills and research for helping critical infrastructure providers in Estonia will help to ensure capacity to fight potential cyber-attacks, which would seriously

disrupt our society. Attention to public education and awareness equips citizens and both public as well as private organisations with the knowledge and skills required to navigate the digital world securely.

Overall, **NCCEE2’s** comprehensive strategy creates a secure, resilient, and competitive digital ecosystem that benefits businesses, educators, and communities, setting the stage for a digitally robust future for all. We aim to ensure that Estonia reaches its vision of becoming an advanced and most resilient digital society.

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.*

N/A as per call document

#§IMP-ACT-IA§#

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

#@WRK-PLA-WP@#

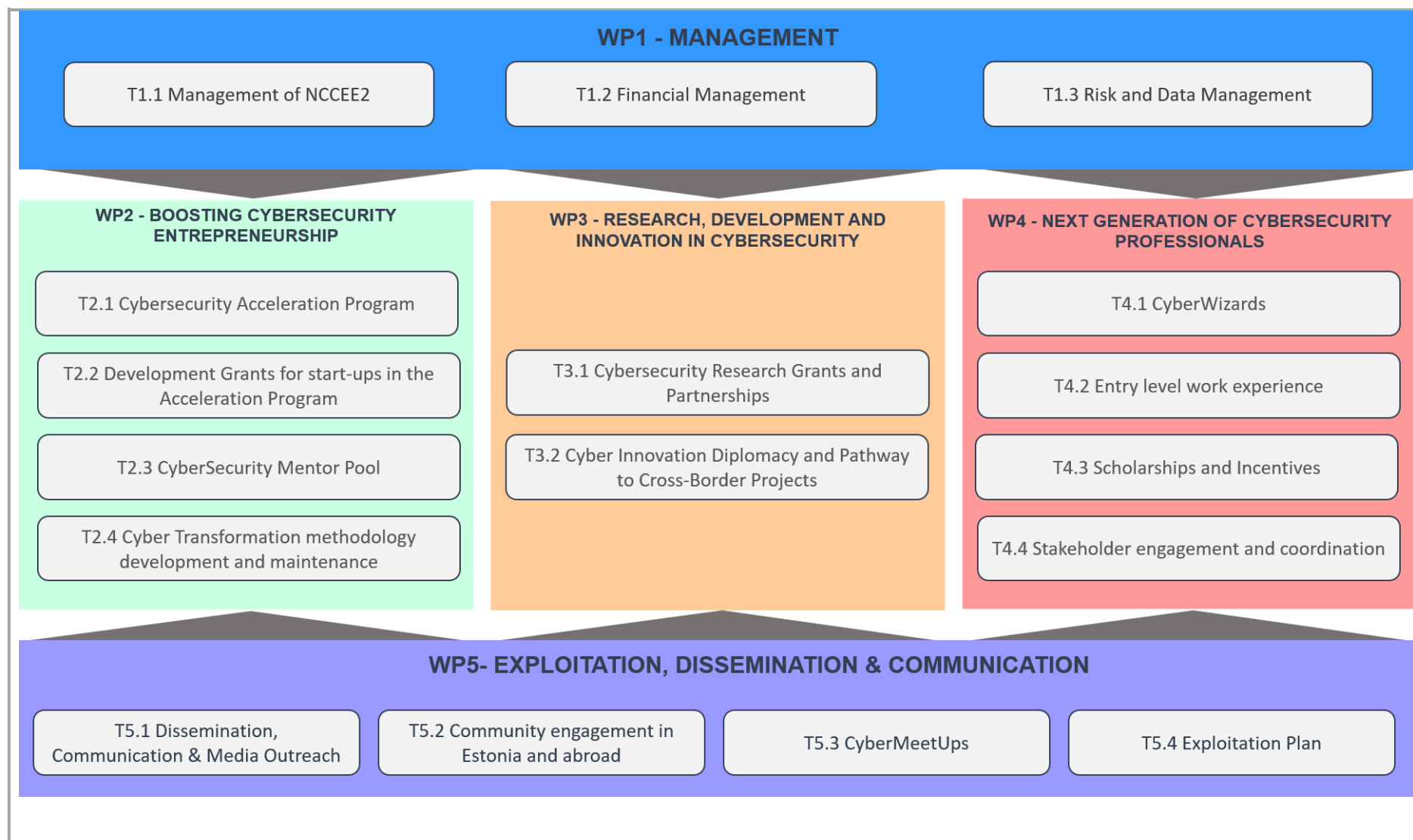
4. WORK PLAN, WORK PACKAGES, ACTIVITIES, RESOURCES AND TIMING

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)).

NCCEE2 Work Plan Graphical Representation:



4.2 WORK PACKAGES, ACTIVITIES, RESOURCES AND TIMING

WORK PACKAGE 1

Work Package 1: Management					
Duration:		M1 – M48	Lead Beneficiary:		RIA
Objectives					
<p>The Management work package aims to:</p> <ul style="list-style-type: none">• Ensure optimal use of resources including time, budget, and personnel.• Identify potential risks early and establish mitigation strategies.• Maintain high standards in deliverables to meet stakeholder expectations.• Adhere to project timelines and milestones to ensure timely completion.• Maintain clear and ongoing communication with all stakeholders.					
Activities and division of work (WP description)					
Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	
T1.1	Management of Project NCCEE2	<p><u>Sub-Task (ST)1.1.1 Overall Management:</u></p> <p>A practical and efficient management structure will be established to ensure the successful implementation of the project, taking into account the processes that worked well during the previous project.</p>	RIA EIS Tehnopol	COO BEN BEN	No

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

		<p>The Project Coordinator (PC) will oversee the management and upkeep of the web-based management system which is already in place, as part of the pilot NCCEE project. The PC utilizes web-based project platforms to manage project activities. The PC ensures that project tasks are completed on schedule in accordance with agreements with other parties, that deliverable documents are prepared and submitted according to plan and that any necessary modifications are communicated in advance, allowing for adequate time to respond appropriately.</p> <p>The project will be overseen by a Project Steering Committee (SC), composed of team members from RIA, EIS, and Tehnopol. These will be experienced team members who have worked on the pilot NCCEE project.</p> <p>The SC will manage key decisions regarding project execution, monitor progress, address challenges, and promote effective communication and knowledge sharing among stakeholders.</p> <p>As part of the overall management, a Gender Action Plan which was already created for the pilot NCCEE project will be reviewed, and put forth for approval by the SC to implement the project's gender strategy. A designated Gender Action Officer will be appointed to manage and coordinate these efforts, reporting to both the PC and the SC.</p> <p><u><i>Sub-Task 1.1.2 Collaboration and Coordination within Consortium:</i></u></p> <p>The SC will generally meet every month, but meetings will be scheduled as needed. The meeting topics and decisions will be compiled into a memo, which is accessible to all participants of the meeting.</p> <p>A cooperation agreement will be established with RIA and 2 consortium partners in order to outline the obligations and the framework for collaboration.</p> <p>If necessary, additional members from Tehnopol, EIS, or RIA, such as Work Package Leaders, will be invited to participate in Project</p>			
--	--	--	--	--	--

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

		<p>Steering Committee meetings to deliberate or formulate more precise plans or reviews on specific topics.</p> <p><u>Sub-Task (ST) 1.1.3 Communication with Granting Authority:</u></p> <p>The PC will handle communication and information exchange with the Granting Authority (ECCC)</p> <p>Responsibilities include: 1) submitting regular, timely reports on administrative and financial progress, 2) ensuring all partners contribute to ongoing financial and final reports for the ECCC, and 3) informing ECCC of any significant changes and communicating with ECCC to ensure that project activities are carried out according to the requirements.</p>			
T1.2	Financial Management	<p>PC will share information and guidelines with the partners in order to comply with the necessary financial administration and procurement practices required by Digital Europe, maintaining accurate records for all expenditures.</p> <p>The PC will provide assistance to partners related to fund eligibility and EC reporting guidelines, such as contractual, legal, and technical reporting.</p> <p>To address any questions related to fund eligibility and ECCC reporting guidelines, such as contractual, legal, and technical reporting, PC will communicate directly with partners. Furthermore, PC will thoroughly review the costs reported by partners, request clarifications when needed, and validate the eligibility of these costs according to ECCC regulations, including the relevant audit certificates. If any irregularities are detected, PC will promptly notify partners and provide guidance on the required corrective actions.</p>	RIA EIS Tehnopol	COO BEN BEN	No
T1.3	Risk and Data Management	<p><u>Sub-Task 1.3.1 Risk Management:</u></p> <p>The PC will be assisted by SC in managing risks by reviewing the risk profile biannually. A risk management plan will be created, which will outline the process for identifying, assessing, and managing risks associated with the project, as well as defining appropriate measures for risk prevention.</p>	RIA EIS Tehnopol	COO BEN BEN	No

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

		<p>During Project Steering Committee meetings, risks will be reviewed and decisions will be made based on the situation, ensuring that the project remains on schedule and avoids delays.</p> <p><u>Sub-Task 1.3.2 Data Management:</u></p> <p>Secure Data management will be carried out, ensuring compliance with data protection requirements during data sharing and storage.</p> <p>Throughout the project, we will ensure compliance with all relevant legal frameworks to manage personal and health data in accordance with privacy and ethical standards. We will obtain ethical approval and informed consent from participants, ensuring they understand how their data will be used and their rights to access, withdraw, or delete it. We plan to anonymize and pseudonymize the data, store it securely on encrypted servers, and restrict access to authorized personnel only. Data will be used exclusively for the project's purposes, with any secondary use requiring explicit consent. The data will be retained for the necessary duration and securely deleted once the retention period expires. The data protection officer will oversee ongoing compliance and ensure that all processes align with data protection standards.</p> <p>PC will develop a data management plan outlining the necessary data storage facilities for safe handling and storage.</p>			
--	--	--	--	--	--

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

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

RIA	96	611 359 EUR	0 EUR	44 000 EUR	0 EUR	36 000 EUR	0 grants	0 EUR	0 EUR	0 EUR	48 395 EUR	739 754 EUR
Total	96	611 359 EUR	0 EUR	44 000 EUR	0 EUR	36 000 EUR	0 grants	0 EUR	0 EUR	0 EUR	48 395 EUR	739 754 EUR

For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see [Portal Reference Documents](#)).

WORK PACKAGE 2

Work Package 2: Boosting Cybersecurity Entrepreneurship					
Duration:		M1 – M48	Lead Beneficiary:		
			RIA		
Objectives					
<ul style="list-style-type: none"> To foster the creation and development of new state-of-the-art cybersecurity solutions in the cybersecurity market sector. To increase the competition among existing cybersecurity service providers in the Estonian market and as such foster the development of new and innovative tools. To provide financial support for the adoption and widespread use of the state-of-the-art cybersecurity solutions. 					
Activities and division of work (WP description)					
Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontractin g (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

T2.1	Cybersecurity Acceleration Program	<p>As the regulation establishing the ECCC states, the EU “suffers from insufficient investment and limited access to cybersecurity knowhow, skills and facilities, and few Union cybersecurity research and innovation outcomes are translated into marketable solutions or widely deployed across the economy”. Therefore this task will provide a continuation and a development of the accelerator project from the initial NCCEE project which contributed to the development of 15 early-stage cybersecurity start-up companies between 2023 and 2024.</p> <p>The 7-month accelerator program will continue from the initial NCCEE pilot program and will sharpen the focus on cybersecurity innovation. The program will continue to be designed for the creation and development of new start-up companies who would provide state-of-the-art cybersecurity solutions for the market uptake. The accelerator program will focus heavily on research and innovation in cybersecurity, but the goal is to transform research-intensive solutions (TRL level 5+) to market. The accelerator program will be open to students, researchers, start-up entrepreneurs and spin-offs from existing companies. The criteria for the applicants will be based on trends, research and market needs and will focus heavily on innovation.</p> <p>One acceleration program per year will be implemented once a year for three cycles (3 years of the 4-year project) to ensure that the teams participating can complete their proposed projects and to make sure the community is continuously aware of the program and the attention paid to the innovation side of cybersecurity. Compared to the initial accelerator program, the next three cohorts will be smaller to ensure more attention to individual teams. A total of 18 startup companies will be supported during the 3-year period to bring new cybersecurity products and services to the market. The tentative starting dates for each batch will be 10/2025, 10/2026 and 10/2027 and will run until April of the successive year.</p> <p>The accelerator program is built and implemented on the principle of sprints, where group activities alternate with individual activities. A dedicated program manager will ensure the participants will complete their individual projects and keep them on track throughout the program period. Lead mentors, business mentors and cybersecurity mentors will guide the teams based on individual needs.</p> <p>Companies participating in the accelerator program will go through the following development cycles:</p> <ol style="list-style-type: none"> 1. Defining the client's problem and designing a value proposition based on the need (product-market-customer-fit); 2. Business model and team building; 	Tehnopol	COO	No
------	------------------------------------	---	----------	-----	----

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

		<ol style="list-style-type: none"> 3. Product development and prototyping (build-measure-learn); 4. Intellectual property 5. Investor readiness and other financing opportunities; 6. Go-to-market strategies and pilot preparations. <p>The task relies also heavily on the overall community driven mission of the NCCEE2 project, especially through the creation of the Cybersecurity Mentor Pool proposed in Task 2.3. As start-ups grow, the business side is needed throughout, but the possibility of the existing community members to contribute in mentoring new and upcoming colleagues (or future competitors) creates a community mission not seen in the Estonian start-up ecosystem.</p> <p>Selection and fund allocation process: the participants for the Accelerator will be selected through a competitive process. The consortium will put together a committee of experts in cybersecurity, digital innovation, business and start-up culture to ensure that a diverse pool of participants will be selected. The applicants will be selected based on their business proposal, project proposal, project maturity, value proposition and viability.</p> <p>As part of the selection process, the applicants will meet with the committee to present their case.</p> <p>Overall, the selection of the participants will be transparent, comprehensive and will focus on delivering the best, state-of-the-art projects to market.</p>			
T2.2	Development Grants for start-ups in the Acceleration Program	<p>Development Grants in the value of 60 000€ per startup can be acquired by the start-ups participating in the acceleration program. This funding is provided through a competitive process and the funding is aimed to create, develop and disseminate innovative and state-of-the-art cybersecurity solutions.</p> <p>These grants aim to strengthen cybersecurity capabilities of stakeholders and lead to uptake of novel cybersecurity solutions, strengthening Estonian Cybersecurity Community and potentially contributing to the strategic autonomy of the European Union.</p> <p>The grants are provided to the participants of the Cybersecurity Accelerator Program described in Task 2.1 and will be used for various elements of business and product development to build, validate, and test the products or services and to develop the business model and implement go-to-market strategies. The Accelerator will be hosting periodic events to showcase project prototypes, invite feedback, and motivate start-ups to progress with their activities.</p>	RIA Tehnopol	COO BEN	No

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

		CyberAccelerator will be a helpful tool to encourage entrepreneurship within the cybersecurity field, leading also to increased capacity of future cross-border projects.			
T2.3	CyberSecurity Mentor Pool	<p>To provide expertise to start-ups in Estonia and abroad, NCCEE2 will establish a network of experts to mentor SMEs, start-ups, and researchers, enhancing cybersecurity skills and fostering collaboration.</p> <p>The mentors will come from the community members in Estonia and will provide expertise and contribute actively to the strategic tasks related to relevant national and regional challenges for cybersecurity in different sectors. They can also facilitate interdisciplinary and cross-border collaboration on EU-funded projects, helping to establish synergies with relevant activities at national, regional and local levels. Also when other accelerator programs or cybersecurity skills programs ask for Estonian expertise, the network can provide access.</p> <p>Mentors can also help in promoting and disseminating relevant outcomes of various NCCEE funded projects to third parties at national and international level.</p>	RIA	COO	No
T2.4	Cyber Transformation methodology development and maintenance	<p>This task will continue the development of a simple, commercially logical, and commercially accepted methodology for providing cybersecurity posture assessment. The methodology was initially created during the NCCEE deployment project and has since had an impact of increasing competition in Estonia (bringing down the cost of the service and allowing for more actors to come to the market) and raising awareness among the Estonian companies who otherwise would struggle to procure these services.</p> <p>The goal of this Methodology is to provide harmonization of service providers' approach to Cybersecurity services provision. According to the methodology an evaluation must be given to networks, firewalls, servers, risk analyses and awareness of the employees and the management board about cyber hygiene and security. The service providers conducting the evaluation and mapping will follow the methodology drawn up by RIA. They will do the preliminary work of assessing the organization's footprint from outside, visit the organization on site, conduct interviews, perform scans of the organisation's networks, and present the final results to the management board.</p> <p>As the cybersecurity landscape is constantly changing, this task will ensure that two new versions will be developed over a 4 year period, taking into account the feedback received from the community members who are providing those services and the specialists from the field. The methodology versions will include instruction manuals, examples and templates for the service providers, the customers and third party evaluators. The new</p>	RIA	COO	No

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

		versions will be translated into English for dissemination and uptake from other NCCs and competent authorities.			
--	--	--	--	--	--

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
RIA	48	242 976 EUR	0 EUR	12 000 EUR	0 EUR	10 000 EUR	0	0 EUR	0 EUR	0 EUR	18 548 EUR	283 524 EUR
Tehnopol	27	135 000 EUR	0 EUR	0 EUR	0 EUR	90 000 EUR	18 grants	1 080 000 EUR	0 EUR	0 EUR	91 350 EUR	1 396 350 EUR
Total	75 person months	377 976 EUR	0 EUR	12 000 EUR	0 EUR	100 000 EUR	18 grants	1 080 000 EUR	0 EUR	0 EUR	109 898 EUR	1 679 874 EUR
For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see Portal Reference Documents).												

WORK PACKAGE 3

Work Package 3: Research, Development and Innovation in Cybersecurity

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

Duration:	M1 – M48	Lead Beneficiary:	RIA		
Objectives					
<ul style="list-style-type: none">To provide financial support for cybersecurity innovation, state-of-the-art tools, products and servicesTo promote, encourage and facilitate the participation of Estonian community members in cross-border projects and cybersecurity actions funded through EU programsTo provide technical assistance to stakeholders in their application phase for projects managed by the ECCCTo foster collaboration between the private sector and research institutions in Estonia and EuropeTo enhance the involvement of Estonian companies and foster international partnerships, strengthening Estonia's position as a cybersecurity hub and developing local skills and expertise in the field.Collaborating with the European network of NCCs to share knowledge and experience, between NCCs and the Estonian cybersecurity community.					
Activities and division of work (WP description)					
Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	
T3.1	Cybersecurity Research Grants and Partnerships	<p>NCCEE2 will design and operate a program to distribute innovation and development grants in order to promote the creation or development of state-of-the-art cybersecurity solutions. These grants will work in synergy with the overall goal of the NCCEE2: to increase cooperation between the private sector, the researchers and the possible end-users of cybersecurity solutions. This grant program will also steer the Estonian cybersecurity community towards the Digital Europe Programme Cybersecurity goals as the topics for the calls will be aligned with the DEP work programme 2025-2027.</p> <p>The program will provide competitive grants from 60 000 € to 100 000 € for new scientific discovery, product and service development in cybersecurity over 12-24 months with at least</p>	RIA EIS	COO AP	No

		<p>three cut-off dates. This task will rely on industry-academia cooperation, as every consortium applying for grants should include both businesses as well as academic entities.</p> <p>We foresee at least three general topics for grants, aligned with the DEP WP 2025-2027 and distributed between the cut-off dates in 2025 and 2026 for the projects to be completed by 2027 and 2028. We have planned for at least 3 cut-off dates for these projects, each time selecting 5-6 projects to be funded and will initially propose the following topics:</p> <ul style="list-style-type: none"> • 10/2025 for the topic “Cybersecurity automation” • 3/2026 for the topic “AI use in cybersecurity” • 6/2026 for the topic “Tools and strategies for the transition to quantum-safe cryptographic algorithms” <p>These topics and cut-off dates are subject to change based on feedback from the community members or developments in the design phase of the grants.</p> <p>We initially envision that the grants could be used for</p> <ul style="list-style-type: none"> - Creating and testing prototypes - The technological development, testing and demonstration of components necessary for the products - Product testing and industrial experiments, feasibility studies - Consultations and registering a patent, utility model or an industrial design solution - Accreditation, certification, standardization, metrology etc. - Hiring cybersecurity doctoral students at private companies and supporting their research goals. <p>Over the 48 months of the project we foresee at least 18 projects being funded. As the projects will require a consortium to be formed, we anticipate the Estonian research entities (universities and research-heavy organizations) contributing to multiple consortia.</p> <p>Grant conditions will require R&D beneficiaries to produce public case studies or demonstration videos to make research outcomes accessible and understandable to the broader cybersecurity community to stimulate further innovation. The collaboration between industry and academia will provide for research papers that could benefit the research community and facilitate further discovery.</p> <p>The application process for the grants will be designed in a similar manner to the process required for European grants, but on a lower level of bureaucracy to facilitate higher participation</p>			
--	--	--	--	--	--

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

		<p>rates. This will encourage the beneficiaries to “practice” the application process to participate in pan-European project calls.</p> <p>Selection and fund allocation process: EIS has a tried and tested process of project selection and fund allocation already in place for various innovation and R&D grants (through different EU and adjacent funds). This process includes a committee of experts (in our case in the fields of cybersecurity, ICT, research and development, automation, etc) who will evaluate a project proposal according to the design of the grant system. This evaluation only happens once the legal requirements are fulfilled by the beneficiary.</p> <p>The projects will be selected based on the project proposal, contribution to the overall goal of the current topic, viability of the project and project maturity.</p> <p>We envision a competitive grant allocation process where project proposals are submitted by the cut-off dates detailed above.</p> <p><u><i>Sub-Task 3.1.1: Designing of Grant System:</i></u></p> <p>Designing the grant system - includes designing of a comprehensive grant system that includes the structural, legal, and procedural framework necessary to ensure the grants effectively support research and partnership within cybersecurity ecosystem.</p> <p><u><i>Sub-Task 3.1.2: Grant Coordination and Management:</i></u></p> <p>To ensure effective grant coordination and management, grants will be distributed in collaboration with external partners, such as EIS, emphasising seamless communication, thorough reporting and rigorous quality control. Clear communication channels will be established with partners to align on responsibilities, expectations, and goals. A tracking system will oversee the distribution process, enabling prompt resolution of issues and adjustments as needed. Regular, standardised reporting and documentation practices will be implemented to capture key data, including financial transactions, project milestones, and impact assessments, ensuring accountability and transparency throughout the grant lifecycle.</p>			
T3.2	Cyber Innovation Diplomacy and Pathway to Cross-Border Projects	<p>This task will create a strategy focused on promoting cybersecurity innovation by increasing Estonian community participation in international and regional projects.</p> <p>This task includes three sub-tasks: sharing information and raising awareness on cybersecurity projects and opportunities, creating a platform and spaces for companies to find potential collaboration and consortium partners and providing technical assistance to stakeholders by</p>	RIA	COO	No

		<p>supporting the stakeholders in their application phase for projects managed by the ECCC and others.</p> <p><u><i>Sub-task 3.2.1 Awareness raising on potential projects</i></u></p> <p>The sub-task will focus on disseminating information on various platforms to the Estonian Cybersecurity Community about project calls from Digital Europe, Horizon Europe, European Defense Fund and other relevant funds. The sub-task will rely on the communication and dissemination plan in Work Package 5. RIA will organise at least 8 Call Introduction events in Estonia (2 every year) to support dissemination of information about DIGITAL calls and Horizon Europe calls when possible.</p> <p><u><i>Sub-task 3.2.2 Supporting partnerships</i></u></p> <p>The sub-task facilitates the participation of the Estonian Cybersecurity Community at various brokerage events on the European level. As European cross-border projects usually require consortium partners from various Member States, the Community members may need extra encouragement and assistance in the participation in such events. The task relies on sub-task 3.2.1 for awareness raising and a robust Community membership.</p> <p>As the project calls are published in Digital Europe, Horizon Europe, European Defense Fund and other relevant calls, we will collaborate with the regional NCCs (NCC-FI, NCC-SE, NCC-LV, NCC-LT, NCC-DK, NCC-NO, NCC-IS and others) to organize a regional Information Day about those calls. The Info Day will be held in different locations and Tallinn, Estonia will be one of those. We will organize at least 3 such events in Tallinn and regional partners will be invited to those Info Days to meet and network, while colleagues from the ECCC and other NCCs will be invited to present and discuss calls. RIA will send delegations including members of businesses and academia to events organized by other NCCs to facilitate networking.</p> <p>Part of the sub-task is to visit other NCCs in the region with the members of the Estonian Cybersecurity Community.</p> <p><u><i>Sub-task 3.2.3: Consultation services for Members of the Community</i></u></p> <p>As providing technical assistance to stakeholders by supporting the stakeholders in their application phase for projects managed by the ECCC is one of the key tasks for the NCCs, this sub-task will create a process by which Members of the Estonian Cybersecurity Community can get consultation services for such projects. The goal is to decrease the bureaucratic burden for companies who may not have the resources to put into project writing. Ideally Members of the Community could get access to consultation services in the project preparation phase.</p> <p>The task will consist of three parts:</p>		
--	--	--	--	--

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

		<ol style="list-style-type: none"> 1. Market research into which technical consultation services are needed 2. Centralized procurement of technical consultation services 3. Criteria and processes by which Members of the Community can access those consultation services <p>We target that 10 SME community members will be able to use centrally procured consultation services yearly. Consultation services will be available from the 2nd year of the NCCEE2 project.</p>			
--	--	--	--	--	--

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
RIA	24 person months	130 833 EUR	0 EUR	12 000 EUR	0 EUR	30 000 EUR	0	0 EUR	0 EUR	0 EUR	12 098 EUR	184 931 EUR
EIS	0 person months	0 EUR	0 EUR	0 EUR	0 EUR	0 EUR	18-20 grants	1 500 000 EUR	0 EUR	0 EUR	105 000 EUR	1 605 000 EUR
Total	24 person months	130 833 EUR	0 EUR	12 000 EUR	0 EUR	30 000 EUR	18-20 grants	1 500 000 EUR	0 EUR	0 EUR	117 098 EUR	1 789 931 EUR
For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see Portal Reference Documents).												

WORK PACKAGE 4

Work Package 4: Next Generation of Cybersecurity Professionals					
Duration:		M1 – M48	Lead Beneficiary:		RIA
Objectives					
<ul style="list-style-type: none">• To reinforce cybersecurity and technology skills and competence in industry, technology and research and at all relevant educational levels, supporting gender balance• To tackle the gender gap by increasing the number of women and girls gaining cybersecurity skills across various educational formats.• To promote cybersecurity as a core component of the digital society through interdisciplinary training and education.• To engage with national actors regarding possible contributions to promoting and disseminating cybersecurity educational programmes.					
Activities and division of work (WP description)					
Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	
T4.1	CyberWizards	<p>This task will provide a continuation of a popular task initiated in the NCCEE deployment project through training young women and girls in the field of Cybersecurity.</p> <p>Since women are under-represented in the workforce of cybersecurity, the NCCEE project initiated two versions of training camps for teenagers who are on the verge of deciding their career paths - one-day camps in collaboration with the girls organization of the Estonian Defense League and 6-day summer camps for the international community. The goal of the camps is to show hands on the challenges that cybersecurity experts are facing daily and how to solve them while introducing them to the community.</p>	RIA	COO	No

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

		<p>The six-day summer camps will be organized in concert with the community members from Estonia and other NCCs who are interested that their own youth participate in these events.</p> <p>Through the 4 year project we will organize a total of 4 larger summer camps, each of them lasting 6-days. Camps will be every year, each for 80-100 young people. The goal is for at least half of those participants to be from other countries and organizing this will need close collaboration with the Network of NCCs and competent authorities from our partner countries.</p> <p>In addition to international summer camps, we will continue organizing 1-day hands-on training for girls and to people who are working with youth. This will be done in cooperation with Estonian Defence League and other youth organizations, aiming at increasing interest of girls in Cybersecurity career-paths. Over the 4 year project we will organize 8 one-day trainings.</p>			
T4.2	Entry level work experience	<p>As cybersecurity skills shortage is becoming a bigger problem in a more digital society, the market still makes it difficult to find entry-level work experience, such as internships or junior positions. In order to support young adults and fresh graduates finding their first professional position we will work together with existing internships programs and other projects to support the growth of internship opportunities for cybersecurity positions and junior research positions where they are encouraged to write their thesis in cybersecurity related topics.</p> <p>The task includes mapping existing internship programs (e.g the IT internship program for the public sector in Estonia), working together with the program owners to expand it and encouraging private cybersecurity companies to join the program.</p> <p>We aim to focus on mapping opportunities during the first year and to work with the Estonian cybersecurity community to promote the idea of entry-level work programs. Starting from 2nd year we intend to facilitate at least 10 internship positions per year.</p>	RIA	COO	No
T4.3	Scholarships and Incentives	<p>The main goal of this task is to introduce cybersecurity as a career path (or a field that is an important part of any other career path, regardless of their future field of work) for youth aged 15-25. The task includes mapping of existing programs, competitions, and events that young people who are attending and working towards integrating cybersecurity topics into those events.</p> <p>For example:</p> <ol style="list-style-type: none"> 1. A special prize for a cybersecurity related paper at the National Contest of Young Scientists where students at middle schools and high schools can submit their school research papers 	RIA	COO	No

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

		<p>2. A special hacking prize at a robotics competition</p> <p>3. Special cybersecurity or CTF themed courses/trainings on popular online programs for talented middle and high-schoolers provided by universities</p> <p>4. Continuing working towards integrated Cybersecurity courses and lectures in universities</p> <p>NCCEE2 will support third party activities with small but relevant financial incentives such as prizes, scholarships or incentives to procure professional trainers for local youth. These will range from 1000€ to 3000€ and can be used for example to fund activities of cybersecurity clubs in schools, facilitate participation of professionals and students in internship programs or fund preparation of cybersecurity-related educational materials. We intend to support 4 activities per year, totalling 16 initiatives.</p>			
T4.4	Stakeholder engagement and coordination	<p>Aim of this task is to create synergies between stakeholders by gathering and disseminating information about the skills gap and the initiatives, projects, and programs focusing on Cybersecurity skills in Europe and globally. Stakeholder engagement would primarily consist of information sharing through various platforms such conferences where our target groups are attending, various working groups, info seminars, trainings, video calls, 1:1 meetings etc with the following target groups:</p> <ul style="list-style-type: none"> • organizations offering services, products and trainings • organizations looking for talented cybersecurity specialists • people who lack the knowledge where to find information about the field of cybersecurity and/or where and how to learn it on their own or in formal educational system (this includes cooperation with European partners such as ENISA, the European Cybersecurity Skills Academy and other relevant entities) • people working or within close contact with youth (teachers, trainers, youth workers, parents etc) <p>Outcome of stakeholder engagement activities would be a set of policy papers, which would be disseminated to Estonian policy makers and the ECCC working groups on cyberskills, stakeholders at ENISA and to European Cybersecurity Skills Academy. This will help 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.</p>	RIA	COO	No

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

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
RIA	48 person months	242 976 EUR	0 EUR	12 000 EUR	0 EUR	320 000 EUR	16 prizes	30 000 EUR	0 EUR	0 EUR	42 348 EUR	647 324 EUR
Total	48 person months	242 976 EUR	0 EUR	12 000 EUR	0 EUR	320 000 EUR	16 prizes	30 000 EUR	0 EUR	0 EUR	42 348 EUR	647 324 EUR
For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see Portal Reference Documents).												

WORK PACKAGE 5

Work Package 5: Exploitation, Dissemination and Communication			
Duration:	M1 – M48	Lead Beneficiary:	RIA
Objectives			
<ul style="list-style-type: none"> To increase awareness and visibility of project achievements, promote and disseminate the relevant outcomes of the work of the NCCEE2, the ECCC and the other NCCs in the Network of NCCs To encourage community membership and assess the requests to become part of the European Cybersecurity Competence Community 			

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

- To act as a contact points at the national level for the Cybersecurity Competence Community
- To maximize impact and ensure sustainability of project results across Estonia and EU.
- To share knowledge through various channels and engage stakeholders, youth, women, girls, and others towards the cybersecurity ecosystem.
- To enhance project profile and engage diverse audiences.
- To strengthen partnerships and encourage collaboration.

Activities and division of work (WP description)

Task No (continuous numbering linked to WP)	Task Name	Description	Participants		In-kind Contributions and Subcontracting (Yes/No and which)
			Name	Role (COO, BEN, AE, AP, OTHER)	
T5.1	Dissemination, communication, and media outreach	<p>Creation and execution of a dissemination and communication plan for NCCEE2, which covers:</p> <ol style="list-style-type: none"> 1) Planned impacts and communication messages, 2) Channels of communication (such as website, social networks, events, conferences, and media), 3) Allocation of responsibilities and targets. Key Performance Indicators (KPIs) established to evaluate effectiveness. <p>The dedicated NCCEE section on RIA's main website, created during the pilot project, will continue to serve as a key resource for project updates. This section will be regularly updated with the latest developments, ensuring timely and relevant information is accessible. In the next phase, the website will incorporate additional sub-topics in both Estonian and English to maximize its utility. Furthermore, a strategic framework for communicating EU funding opportunities will be developed and integrated into the website, enhancing its value for stakeholders.</p> <p>The CyberMeetUp community mailing list, established during the NCCEE deployment project, will be continued, maintained and updated regularly. This mailing list will be instrumental in notifying Community members about relevant events, including local and international brokerage sessions, monthly CyberMeetUps, and other pertinent activities.</p>	RIA EIS Tehnopol	COO BEN BEN	No

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

		RIA's social media platforms, such as LinkedIn, YouTube and Facebook, will continue to be leveraged to inform and engage the Community about upcoming events and project updates. NCCEE2 activities will also be promoted through the newsletters of affiliated ministries, the NCC Mattermost platform, and the ECCC newsletter.			
T5.2	Community engagement in Estonia and abroad	<p><u>Sub-task 5.2.1 Community membership maintenance and encouragement</u></p> <p>To foster a thriving and engaged cyber community, a strategy for ongoing membership maintenance and encouragement will be implemented. This will include regular communication to keep members informed, engaged, and motivated to participate actively. Personalised outreach, such as welcoming new members, acknowledging achievements, and encouraging involvement in community events, will strengthen member connections and loyalty. Feedback loops will be established to understand member needs and enhance their experience. By creating a supportive, responsive, and inclusive environment, this approach aims to boost retention, increase participation, and cultivate a sense of belonging within the cyber community.</p> <p><u>Sub-task 5.2.2 Cybersecurity Competence Community</u></p> <p>The NCCEE2 project will focus on facilitating community engagement and registration to the European Cybersecurity Atlas, which provides international opportunities for collaboration between cybersecurity experts. We foresee ATLAS registration as a prerequisite for participating in some of the NCCEE2 events. During the project timeline we will design, develop, test and deploy the API-based Atlas National Entity Registration Portal according to Regulation (EU) 2021/887.</p> <p><u>Sub-task 5.2.3 International Community Events:</u></p> <p>As the first Baltic Cyber Innovation Forum CyberBazaar (a joint undertaking between NCC-EE, NCC-LV, and NCC-LT) was a successful example of collaboration (initiated through the NCCEE deployment project and the respective deployment projects in Latvia and Lithuania), we will ensure exploring new collaboration forms to ensure collaboration between Estonia, Latvia and Lithuania. In NCCEE2 project we will focus on activities stimulating participation of the Estonian Cybersecurity Community, the consortium partners and other relevant actors in various external conferences and workshops. Suitable events will be selected on a regular basis and chosen with sufficient flexibility to react to ad hoc, cost-effective dissemination opportunities.</p>	RIA EIS Tehropol	COO BEN BEN	No
T5.3	CyberMeetUps	As the CyberMeetUp events, which stem from the NCCEE pilot project, are well rooted and successful, we will continue organizing these monthly community events, where various cybersecurity challenges and possibilities will be introduced, achievements celebrated and research results disseminated. This includes information about NCC-EE services and knowledge provided by the Community Members, updates about the threat landscape and	RIA EIS Tehropol	COO BEN BEN	No

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

		<p>threat intelligence and awareness raising about project calls from Digital Europe, Horizon Europe, European Defense Fund, and other relevant funds (as laid out in sub-task 3.2.1).</p> <p>We foresee 9 CyberMeetUps per year, meaning a total of 36 fascinating and practical events for cybersecurity members in Estonia during the NCCEE2 project.</p> <p>We will encourage collaboration with the network of NCCs to disseminate knowledge from other communities and the relevant project results from other NCC projects.</p>			
T5.4.	Exploitation Plan	<p>The goal of this task is to create an actionable plan for the legacy of cybersecurity research, development, and education, along with strategies for continued coordination and networking. This includes the implementation of ideas, concepts, and educational resources created in WPs 2, 3, and 4. A consultation will be aligned with the actions outlined in these work packages, and will also focus on engaging youth, as well as women and girls, in these initiatives. Focus will be on the exploitation and legacy with a target of being self-sustainable. We will be looking for collaboration and synergies between public and private sector entities and international cooperation. The outcome of this task will be a document with a proposal for policy makers in Estonia about the way forward.</p>	RIA	COO	No

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
RIA	48 person months	242 976 EUR	0 EUR	12 000 EUR	0 EUR	144 000 EUR	0 grants	0 EUR	0 EUR	0 EUR	27 928 EUR	426 904 EUR

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

Tehnopol	9 person months	45 000 EUR	0 EUR	0 EUR	0 EUR	30 000 EUR	0 prizes	0 EUR	0 EUR	0 EUR	5250 EUR	80 250 EUR
Total	57 person months	287 976 EUR	0 EUR	12 000 EUR	0 EUR	174 000 EUR	0 grants 0 prizes	0 EUR	0 EUR	0 EUR	33 178 EUR	507 154 EUR
For Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see Portal Reference Documents).												

Staff effort per participant

Fill in the effort per work package and Beneficiary/Affiliated Entity.

Please indicate the number of person/months over the whole duration of the planned work.

Identify the work-package leader for each work package by showing the relevant person/month figure in **bold**.

Participant	WP 1	WP 2	WP 3	WP 4	WP 5	Total Person-Months
RIA	96	48	24	48	48	264
Tehnopol	0	27	0	0	9	36
EIS	0	0	0	0	0	0
Total Person-Months	96	75	24	48	57	300

SUBCONTRACTING (N/A FOR PREFIXED LUMP SUM GRANTS)

Subcontracting

Give details on subcontracted project tasks (if any) and explain the reasons why (as opposed to direct implementation by the Beneficiaries/Affiliated Entities).

Subcontracting — Subcontracting means the implementation of 'action tasks', i.e. specific tasks which are part of the EU grant and are described in Annex 1 of the Grant Agreement.

Note: Subcontracting concerns the outsourcing of a part of the project to a party outside the consortium. It is not simply about purchasing goods or services. We normally expect that the participants have sufficient operational capacity to implement the project activities themselves. Subcontracting should therefore be exceptional.

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

Include only subcontracts that comply with the rules (i.e. best value for money and no conflict of interest; no subcontracting of coordinator tasks).						
Work Package No	Subcontract No (continuous numbering linked to WP)	Subcontract Name (subcontracted action tasks)	Description (including task number and BEN/AE to which it is linked)	Estimated Costs (EUR)	Justification (Why is subcontracting necessary?)	Best-Value-for-Money (How do you intend to ensure it?)
	S1.1					
Other issues: <i>If subcontracting for the entire project goes beyond 30% of the total eligible costs, give specific reasons.</i>			Insert text			

PURCHASES AND EQUIPMENT

Purchase costs (travel and subsistence, equipment and other goods works and services)				
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.				
Participant 1:	[RIA]			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
Training camps for youth	Other goods, works and services	WP4	This includes costs related to carrying out activities for 4 camps and 8 one-day camps	320 000 EUR
CyberMeetUp organization	Other goods, works and services	WP 5	The procurement of the venue, catering and technical assistance for the monthly flagship event called CyberMeetUp.	120 000 EUR
Travel	Travel and Subsistence	WP1-5	All transportation, accommodation and other logistical costs associated with travelling.	72 000 EUR

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

Certificate of Financial Statement	Other goods, works and services	WP 1	Procuring the auditing services to get a Certificate of our Financial Statement.	36 000 EUR
Total				548 000 EUR
Participant 2:	Tehnopol			
Cost item name	Category	WP(s)	Explanations	Costs (EUR)
Training modules	Other goods, works and services	WP 2	Procurement, logistics and trainer fees associated with providing a training program for the 18 start-ups in the CyberAccelerator program.	60 000 EUR
Communication services	Other goods, works and services	WP 5	Marketing and advertising costs associated with the CyberAccelerator program intended to find best possible candidates for the program.	30 000 EUR
Training modules	Other goods, works and services	WP 2	Preparation of training materials and providing technical support services during CyberAccelerator program training days.	2 000 EUR
Evaluation process	Other goods, works and services	WP 2	Tools, licenses, and services to help the CyberAccelerator's startup evaluation process.	1 000 EUR
Total				93 000 EUR
Total purchase costs > 15% (all participants)				641 000 EUR
Remaining purchase costs < 15% (all participants)				111 000 EUR
Total purchase costs (all participants)				752 000 EUR

OTHER COST CATEGORIES

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

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:	EIS	
Cost category	Explanations	Costs (EUR)
Financial support to third parties	<p>NCCEE2 will design and operate a program to distribute innovation and development grants in order to promote the creation or development of state-of-the-art cybersecurity solutions. These grants will work in synergy with the overall goal of the NCCEE2 to increase cooperation between the private sector, the researchers and the possible end-users of cybersecurity solutions.</p> <p>EIS will provide competitive grants from 60 000 € to 100 000 € for new scientific discovery, product and service development in cybersecurity over 12-24 months with at least three cut-off dates. This task will rely on industry-academia cooperation, as every consortium applying for grants should include both businesses as well as academic entities.</p> <p>We foresee at least three general topics for grants, aligned with the DEP WP 2025-2027 and distributed between the cut-off dates in 2025 and 2026 for the projects to be completed by 2027 and 2028. We have planned for at least 3 cut-off dates for these projects, each time selecting 5-6 projects to be funded, and will initially propose the following topics:</p> <ul style="list-style-type: none"> 10/2025 for the topic “Cybersecurity automation” 3/2026 for the topic “AI use in cybersecurity” 6/2026 for the topic “Tools and strategies for the transition to quantum-safe cryptographic algorithms” <p>These topics and cut-off dates are subject to change based on feedback from the community members or developments in the design phase of the grants.</p> <p>We initially envision that the grants could be used for</p> <ul style="list-style-type: none"> - Creating and testing prototypes - The technological development, testing and demonstration of components necessary for the products - Product testing and industrial experiments, feasibility studies 	[1 500 000 EUR]

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

	<ul style="list-style-type: none"> - Consultations and registering a patent, utility model or an industrial design solution - Accreditation, certification, standardization, metrology etc. - Hiring cybersecurity doctoral students at private companies and supporting their research goals. <p>Over the 48 months of the project we foresee at least 18 projects being funded. As the projects will require a consortium to be formed, we anticipate the Estonian research entities (universities and research-heavy organizations) contributing to multiple consortia.</p> <p>Selection and fund allocation process: EIS has a tried and tested process of project selection and fund allocation already in place for various innovation and R&D grants (through different EU and adjacent funds). This process includes a committee of experts (in our case in the fields of cybersecurity, ICT, research and development, automation, etc) who will evaluate a project proposal according to the design of the grant system. This evaluation only happens once the legal requirements are fulfilled by the beneficiary.</p> <p>The projects will be selected based on the project proposal, contribution to the overall goal of the current topic, viability of the project and project maturity.</p> <p>We envision a competitive grant allocation process where project proposals are submitted by the cut-off dates detailed above.</p>	
Participant 2:	Tehnopol	
Cost category	Explanations	Costs (EUR)
Financial support to third parties	<p>Tehnopol will provide Development Grants in the value of 60 000€ per startup to the start-ups participating in the acceleration program. This funding is provided through a competitive process and the funding is aimed to create, develop and disseminate innovative and state-of-the-art cybersecurity solutions.</p> <p>The grants are provided to the participants of the Cybersecurity Accelerator Program described in Task 2.1 and will be used for various elements of business and product development to build, validate, and test the products or services and to develop the business model and implement go-to-market strategies. The Accelerator will be hosting periodic events to showcase project prototypes, invite feedback, and motivate start-ups to progress with their activities. CyberAccelerator Program, funding a total of 18 start-ups to encourage growth and innovation in the cybersecurity field.</p>	[1 080 000 EUR]

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

	<p>Selection and fund allocation process: the participants for the Accelerator will be selected through a competitive process. The consortium will put together a committee of experts in cybersecurity, digital innovation, business and start-up culture to ensure that a diverse pool of participants will be selected. The applicants will be selected based on their business proposal, project proposal, project maturity, value proposition and viability.</p> <p>As part of the selection process, the applicants will meet with the committee to present their case.</p> <p>Overall, the selection of the participants will be transparent, comprehensive and will focus on delivering the best, state-of-the-art projects to market.</p>	
Participant 3:	RIA	
Cost category	Explanations	Costs (EUR)
Financial support to third parties	<p>NCCEE2 will support third party activities with small but relevant financial incentives such as prizes, scholarships or incentives to procure professional trainers for local youth. These will range from 1000€ to 3000€ and can be used for example to fund activities of cybersecurity clubs in schools, facilitate participation of professionals and students in internship programs or fund preparation of cybersecurity-related educational materials. We intend to support 4 activities per year, totalling 16 initiatives.</p> <p>Selection and fund allocation process: the exact amount of the incentives will be calculated based on discussions with the organizer of the activity and a standard amount those activities have seen before. The activities will be selected by WP4 lead based on the following criteria: impact of the existing activity; extent of engagement with the local youth; potential outcomes of the prizes, incentives or scholarships.</p> <p>We expect many of those initiatives to be local competitions for small research projects or practical technology competitions that already have a myriad of prizes or scholarships that are awarded for different topics – from ecological sustainability to community empowerment. In such cases the process to select the winner of the prize, scholarship or incentive will be done through a jury process.</p>	[30 000 EUR]

TIMETABLE

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

Timetable (projects of more than 2 years) <i>Fill in cells in beige to show the duration of activities. Repeat lines/columns as necessary.</i> Note: 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	2025				2026				2027				2028				2029				2030			
	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	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4
Task 1.1 - Management of Project NCCEE2																								
Task 1.2 - Financial Management																								
Task 1.3 - Risk and Data Management																								
Task 2.1 - Cybersecurity Acceleration Program																								
Task 2.2 - Development Grants for start-ups in the Acceleration Program																								
Task 2.3 - CyberSecurity Mentor Pool																								
Task 2.4 - Cyber Transformation methodology development and maintenance																								
Task 3.1 - Cybersecurity Research Grants and Partnerships																								

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

[illegible]

#§WRK-PLA-WP§#

#@ETH-ICS-EI@#

5. OTHER

5.1 ETHICS

Ethical dimension of the objectives, methodology and likely impact

There are several aspects of the project that involve the processing of personal data. The data collected during the project period will be gathered and used solely for carrying out tasks aligned with the project objectives, specifically for:

- Supporting participation: Facilitating the involvement of Estonian companies in international activities (gathering information for organizing participation in cross-border events).
- Training activities: Promoting the development and spread of cybersecurity skills and encouraging more specialists to enter the field of cybersecurity (e.g., signing up trainees, including minors). In the case of minors, health information is also collected to ensure their needs are considered when organizing the summer camp.
- Communication and dissemination: Promoting project-related actions by signing up community representatives and maintaining a list of names and email addresses.

Privacy protection will be prioritized, with all personal data, including sensitive health information, securely stored and processed in compliance with GDPR and national laws.

Compliance with ethical principles and relevant legislation

RIA as the consortium leader and head of lead in all work packages understands their responsibility in synchronizing the data protection practices among all partners. RIA follows the Estonian Information Security Standard (E-ITS) and RIA's approach to processing the personal data can also be found on the website <https://www.ria.ee/en/authority-news-and-contact/processingpersonal-data>.

To ensure proper management of the data throughout the project, the consortium will provide a comprehensive Data Management Plan (DMP). The DMP will cover data management practices across all work packages, ensuring compliance with applicable data protection and security regulations and outline the data storage solutions for the safe handling and storage of personal and business data.

We confirm that compliance with ethical principles and applicable international, EU and national law in the implementation of activities not originally envisaged (or not described in detail) in the DoA will be ensured.

We confirm that if any ethical concerns are raised by those activities will be handled following rigorously the recommendations provided in the European Commission Ethics Self-Assessment Guidelines.

#§ETH-ICS-EI§# #@SEC-URI-SU@#

5.2 SECURITY

Security self-assessment

RIA is the cybersecurity competence center in Estonia, which is responsible for developing the cybersecurity standard E-ITS for the public sector in Estonia. RIA also has supervision and inspection authority over other government agencies. RIA inspects the implementation of security measures in the information systems of authorities and businesses listed in the Estonian and European legislation.

All project stakeholders will be advised of the importance of adhering to the GDPR and relevant national laws to safeguard personal and business-sensitive data throughout the project. The Risk Management Plan provides a comprehensive overview of the primary risks and outlines efficient mitigation strategies to guarantee complete compliance with these regulations and uphold the highest ethical standards. This approach will help ensure that data is handled responsibly, minimize risks, and foster trust among all parties involved.

We confirm that compliance with security principles and applicable international, EU and national law in the implementation of activities not originally envisaged (or not described in detail) in the DoA will be ensured.

We confirm that any security concern raised by those activities will be handled following rigorously the recommendations provided in the European Commission guideline “How to handle security-sensitive projects”.

#\$SEC-URI-SU\$# #@\$DEC-LAR-DL@\$#

6. DECLARATIONS

Double funding	
Information concerning other EU grants  Please note that there is a strict prohibition of double funding from the EU budget (except under EU Synergies actions).	YES/NO
We confirm that to our best knowledge none of the projects under the action plan as a whole or in parts have benefitted 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

Financial support to third parties (if applicable)
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.
Insert text

#\$DEC-LAR-DL\$#

ANNEXES

LIST OF ANNEXES

- Standard**
Detailed budget table/Calculator (annex 1 to Part B) — mandatory for certain Lump Sum Grants (see [Portal Reference Documents](#))
CVs (annex 2 to Part B) — not applicable
Annual activity reports (annex 3 to Part B) — not applicable
List of previous projects (annex 4 to Part B) — mandatory, if required in the Call document
- Special**
Other annexes (annex 5 to Part B) — mandatory, if required in the Call document

Project: [insert number] — [insert acronym] — [insert call identifier]

EU Grants: Description of the action (DoA) — Annex 1 (DEP): V2.0 – 01.09.2023

LIST OF PREVIOUS PROJECTS

List of previous projects					
Please provide a list of your previous projects for the last 4 years.					
Participant	Project Reference No and Title, Funding programme	Period (start and end date)	Role (COO, BEN, AE, OTHER)	Amount (EUR)	Website (if any)
Estonian Information System Authority (RIA)	Cybersecurity Community Building Activities and Deployment of the Estonian National Coordination Centre (101122044)	03/2023 - 02/2025	COO	3 585 500	www.ria.ee/en/cyber-security/national-coordination-center-ncc-ee
Estonian Information System Authority (RIA)	EU CYBER CAPACITY BUILDING NETWORK (IFS/2019/405-538)	09/2019 – 08/2025	Lead coordinator or (Contract or)	8 999 600	www.eucybernet.eu
Estonian Information System Authority (RIA)	Cyber Resilience for development (IFS/2017/390-290)	01/2018 – 06/2023	Partner	2 224 102	cyber4dev.eu
Estonian Information System Authority (RIA)	Regional policies for competitive cybersecurity SMEs (PGI05456 CYBER; Interreg)	06/2018 – 05/2023	Partner	174 141 (incl own contribution)	https://projects2014-2020.interregeurope.eu/cyber/
Estonian Information System Authority (RIA)	Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET — H2020-SU-SEC-2018-2019-2020 / H2020-SU-SEC-2019; H2020)	05/2020 – 04/2025	Partner	35 375	https://euhybnet.eu/

ANNEX 2

ESTIMATED BUDGET FOR THE ACTION

	Estimated eligible ¹ costs (per budget category)										Estimated EU contribution ²				
	Direct costs									Indirect costs	Total costs	EU contribution to eligible costs			Maximum grant amount ⁶
	A. Personnel costs		B. Subcontracting costs	C. Purchase costs			D. Other cost categories		E. Indirect costs ³	Funding rate % ⁴		Maximum EU contribution ⁵	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 ⁷	Actual costs	Actual costs	Actual costs	Actual costs	Actual costs	Unit costs (usual accounting practices)	Flat-rate costs ⁸					
	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 - RIA	1 471 120.00	0.00	0.00	0.00	92 000.00	0.00	540 000.00	30 000.00	0.00	149 318.40	2 282 438.40	50	1 141 219.20	1 141 219.20	1 141 219.20
2 - EBIA	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1 500 000.00	0.00	105 000.00	1 605 000.00	50	802 500.00	802 500.00	802 500.00
3 - TEHNOPOL	180 000.00	0.00	0.00	0.00	0.00	0.00	120 000.00	1 080 000.00	0.00	96 600.00	1 476 600.00	50	738 300.00	738 300.00	738 300.00
Σ consortium	1 651 120.00	0.00	0.00	0.00	92 000.00	0.00	660 000.00	2 610 000.00	0.00	350 918.40	5 364 038.40		2 682 019.20	2 682 019.20	2 682 019.20

¹ See Article 6 for the eligibility conditions. All amounts must be expressed in EUR (see Article 21 for the conversion rules).

² The consortium remains free to decide on a different internal distribution of the EU funding (via the consortium agreement; see Article 7).

³ 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.

⁴ See Data Sheet for the funding rate(s).

⁵ 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'.

⁶ The 'maximum grant amount' is the maximum grant amount decided by the EU. It normally corresponds to the requested grant, but may be lower.

⁷ See Annex 2a 'Additional information on the estimated budget' for the details (units, cost per unit).

⁸ 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 3

ACCESSION FORM FOR BENEFICIARIES

ETTEVOTLUSE JA INNOVATSIOONI SIHTASUTUS (EBIA), PIC 971995291, established in
SEPISE 7, TALLINN 11415, Estonia,

hereby agrees

to become beneficiary

in Agreement No 101226928 — NCCEE2 ('the Agreement')

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

and mandates

the coordinator to submit and sign in its name and on its behalf any **amendments** to the Agreement,
in accordance with Article 39.

By signing this accession form, the beneficiary accepts the grant and agrees to implement it in
accordance with the Agreement, with all the obligations and terms and conditions it sets out.

SIGNATURE

For the beneficiary

ANNEX 3

ACCESSION FORM FOR BENEFICIARIES

SIHTASUTUS TALLINNA TEADUSPARK TEHNOPOL (TEHNOPOL), PIC 999764257,
established in TEADUSPARAGI 6/1, TALLINN 12618, Estonia,

hereby agrees

to become beneficiary

in Agreement No 101226928 — NCCEE2 ('the Agreement')

between RIIGI INFOSUSTEEMI AMET (RIA) and European Cybersecurity Industrial, Technology and Research Competence Centre ('granting authority'), under the powers delegated by the European Commission ('European Commission'),

and mandates

the coordinator to submit and sign in its name and on its behalf any **amendments** to the Agreement, in accordance with Article 39.

By signing this accession form, the beneficiary accepts the grant and agrees to implement it in accordance with the Agreement, with all the obligations and terms and conditions it sets out.

SIGNATURE

For the beneficiary

ANNEX 4 DIGITAL EUROPE MGA — MULTI + MONO

FINANCIAL STATEMENT FOR [PARTICIPANT NAME] FOR REPORTING PERIOD [NUMBER]

Eligible ¹ costs (per budget category)												EU contribution ²					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 ²	Funding rate % ³		Maximum EU contribution ⁴	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 ⁵	Actual costs	Actual costs	Actual costs	Actual costs	Actual costs	Unit costs (usual accounting practices)	[Actual costs]	Flat-rate costs ⁶						
	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.

¹ See Article 6 for the eligibility conditions. All amounts must be expressed in EUR (see Article 21 for the conversion rules).

² 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.

³ See Data Sheet for the reimbursement rate(s).

⁴ 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.

⁵ See Annex 2a 'Additional information on the estimated budget' for the details (units, cost per unit).

⁶ 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 2015/444¹ 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

¹ 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.



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>)