



## EUROPEAN EDUCATION AND CULTURE EXECUTIVE AGENCY (EACEA)

EACEA.A – Erasmus+, EU Solidarity Corps  
A.2 – Skills and Innovation

### GRANT AGREEMENT

#### **Project 101140030 — CyberHubs**

#### **PREAMBLE**

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

**on the one part,**

the **European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or 'granting authority'), under the powers delegated by the European Commission ('European Commission'),

**and**

**on the other part,**

1. 'the coordinator':

**DIGITALEUROPE AISBL\* (DE)**, PIC 952919756, established in RUE DE LA SCIENCE 14, BRUXELLES 1040, Belgium,

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

2. **AGORIA ASBL (AGORIA)**, PIC 998981079, established in A REYERS 80 DIAMANT BUILDING, BRUXELLES 1030, Belgium,

3. **SOLVAY BRUSSELS SCHOOL LIFELONG LEARNING (SBSEM)**, PIC 882074448, established in AVENUE FRANKLIN ROOSEVELT 42 CP114/01, BRUXELLES 1050, Belgium,

4. **HOGESCHOOL WEST-VLAANDEREN HOWEST (HOWEST)**, PIC 998686684, established in MARKSESTEENWEG 58, KORTRIJK 8500, Belgium,

5. **EESTI INFOTEHNOLOOGIA JA TELEKOMMUNIKATSIOONI LIIT (ITL)**, PIC 935207556, established in LOOTSA 6, TALLINN 11415, Estonia,

6. **TALLINNA TEHNIKAÜLIKOOL (TalTech)**, PIC 999842536, established in EHITAJATE TEE 5, TALLINN 19086, Estonia,

7. **GOSPODARSKA ZBORNICA SLOVENIJE (CCIS)**, PIC 999780165, established in DIMICEVA ULICA 13, LJUBLJANA 1000, Slovenia,

8. **UNIVERZA V MARIBORU (UM)**, PIC 999903646, established in SLOMSKOV TRG 15, MARIBOR 2000, Slovenia,

9. **IVSZ - DIGITALIS VALLALKOZASOK SZOVETSEGE (IVSZ)**, PIC 999794230, established in TINODI U 1-3. FSZT 2., BUDAPEST 1095, Hungary,
10. **NEMZETI KOZSZOLGALATI EGYETEM (NKE)**, PIC 943340812, established in LUDOVICA TER 2, BUDAPEST 1083, Hungary,
11. **FEDERATION OF HELLENIC INFORMATION TECHNOLOGY AND COMMUNICATION ENTREPRISES (SEPE)**, PIC 997352546, established in FRANTZI 19, ATHINA 117 43, Greece,
12. **ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER (AUEB-RC)**, PIC 999896856, established in KEFALLINIAS STREET 46, ATHENS 11251, Greece,
13. **ASOCIACIJA INFOBALT (INFOBALT)**, PIC 970234450, established in GOSTAUTO STR. 8-313, VILNIUS LT-01108, Lithuania,
14. **KAUNO TECHNOLOGIJOS UNIVERSITETAS (KTU)**, PIC 999844961, established in K DONELAICIO 73, KAUNAS LT-44029, Lithuania,
15. **ASOCIACION MULTISECTORIAL DE EMPRESAS DE LA ELECTRONICA, LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACION, DE LAS TELECOMUNICACIONES Y DE LOS CONTENIDOS DIGITALES (AMETIC)**, PIC 968769750, established in CALLE PRINCIPE DE VERGARA 74, MADRID 28006, Spain,
16. **UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA (UNIR)**, PIC 956152281, established in AVENIDA DE LA PAZ 137, LOGRONO 26006, Spain,
17. **NUMEUM (Numeum)**, PIC 882036618, established in 148 BD HAUSSMANN, PARIS 75008, France,
18. **MUNSTER TECHNOLOGICAL UNIVERSITY (MTU)**, PIC 892106673, established in ROSSA AVENUE BISHOPSTOWN, CORK T12 P928, Ireland,
19. **BREYER PUBLICO S.L. (Breyer Publico)**, PIC 881967554, established in C VERDAGUER 2, BARCELONA 08198, Spain,
20. **EIT DIGITAL (EIT DIGITAL)**, PIC 954616286, established in GUIMARDSTRAAT 7, BRUSSEL 1040, Belgium,
21. **ADECCO FORMAZIONE SRL (ADECCO)**, PIC 919579789, established in VIA TOLMEZZO 15, MILANO 20132, Italy,

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

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

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

By signing the Agreement and the accession forms, the beneficiaries accept the grant and agree to

implement the action under their own responsibility and in accordance with the Agreement, with all the obligations and terms and conditions it sets out.

The Agreement is composed of:

Preamble

Terms and Conditions (including Data Sheet)

Annex 1 Description of the action<sup>1</sup>

Annex 2 Estimated budget for the action

Annex 3 Accession forms (if applicable)<sup>2</sup>

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

Annex 4 Model for the financial statements

Annex 5 Specific rules (if applicable)

---

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

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

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

## **TERMS AND CONDITIONS**

### **TABLE OF CONTENTS**

<b>GRANT AGREEMENT.....</b>	<b>1</b>
<b>PREAMBLE.....</b>	<b>1</b>
<b>TERMS AND CONDITIONS.....</b>	<b>4</b>
<b>DATASHEET.....</b>	<b>9</b>
<b>CHAPTER 1 GENERAL.....</b>	<b>14</b>
ARTICLE 1 — SUBJECT OF THE AGREEMENT .....	14
ARTICLE 2 — DEFINITIONS.....	14
<b>CHAPTER 2 ACTION.....</b>	<b>15</b>
ARTICLE 3 — ACTION.....	15
ARTICLE 4 — DURATION AND STARTING DATE.....	15
<b>CHAPTER 3 GRANT.....</b>	<b>15</b>
ARTICLE 5 — GRANT.....	15
5.1 Form of grant.....	15
5.2 Maximum grant amount.....	16
5.3 Funding rate.....	16
5.4 Estimated budget, budget categories and forms of funding.....	16
5.5 Budget flexibility.....	16
ARTICLE 6 — ELIGIBLE AND INELIGIBLE CONTRIBUTIONS.....	16
6.1 and 6.2 General and specific eligibility conditions.....	16
6.3 Ineligible contributions.....	17
6.4 Consequences of non-compliance.....	17
<b>CHAPTER 4 GRANT IMPLEMENTATION.....</b>	<b>17</b>
<b>SECTION 1 CONSORTIUM: BENEFICIARIES, AFFILIATED ENTITIES AND OTHER PARTICIPANTS.....</b>	<b>17</b>
ARTICLE 7 — BENEFICIARIES.....	17
ARTICLE 8 — AFFILIATED ENTITIES.....	19
ARTICLE 9 — OTHER PARTICIPANTS INVOLVED IN THE ACTION.....	19
9.1 Associated partners.....	19
9.2 Third parties giving in-kind contributions to the action.....	20
9.3 Subcontractors.....	20
9.4 Recipients of financial support to third parties.....	20

ARTICLE 10 — PARTICIPANTS WITH SPECIAL STATUS.....	20
10.1 Non-EU participants.....	21
10.2 Participants which are international organisations.....	21
10.3 Pillar-assessed participants.....	21
<b>SECTION 2 RULES FOR CARRYING OUT THE ACTION.....</b>	<b>24</b>
ARTICLE 11 — PROPER IMPLEMENTATION OF THE ACTION.....	24
11.1 Obligation to properly implement the action.....	24
11.2 Consequences of non-compliance.....	24
ARTICLE 12 — CONFLICT OF INTERESTS.....	24
12.1 Conflict of interests.....	24
12.2 Consequences of non-compliance.....	24
ARTICLE 13 — CONFIDENTIALITY AND SECURITY.....	24
13.1 Sensitive information.....	24
13.2 Classified information.....	25
13.3 Consequences of non-compliance.....	26
ARTICLE 14 — ETHICS AND VALUES.....	26
14.1 Ethics.....	26
14.2 Values.....	26
14.3 Consequences of non-compliance.....	26
ARTICLE 15 — DATA PROTECTION.....	26
15.1 Data processing by the granting authority.....	26
15.2 Data processing by the beneficiaries.....	26
15.3 Consequences of non-compliance.....	27
ARTICLE 16 — INTELLECTUAL PROPERTY RIGHTS (IPR) — BACKGROUND AND RESULTS — ACCESS RIGHTS AND RIGHTS OF USE.....	27
16.1 Background and access rights to background.....	27
16.2 Ownership of results.....	28
16.3 Rights of use of the granting authority on materials, documents and information received for policy, information, communication, dissemination and publicity purposes.....	28
16.4 Specific rules on IPR, results and background.....	29
16.5 Consequences of non-compliance.....	29
ARTICLE 17 — COMMUNICATION, DISSEMINATION AND VISIBILITY.....	29
17.1 Communication — Dissemination — Promoting the action.....	29
17.2 Visibility — European flag and funding statement.....	29
17.3 Quality of information — Disclaimer.....	30
17.4 Specific communication, dissemination and visibility rules.....	30

17.5	Consequences of non-compliance.....	30
ARTICLE 18 — SPECIFIC RULES FOR CARRYING OUT THE ACTION.....		30
18.1	Specific rules for carrying out the action.....	30
18.2	Consequences of non-compliance.....	30
<b>SECTION 3 GRANT ADMINISTRATION.....</b>		<b>31</b>
ARTICLE 19 — GENERAL INFORMATION OBLIGATIONS.....		31
19.1	Information requests.....	31
19.2	Participant Register data updates.....	31
19.3	Information about events and circumstances which impact the action.....	31
19.4	Consequences of non-compliance.....	31
ARTICLE 20 — RECORD-KEEPING.....		32
20.1	Keeping records and supporting documents.....	32
20.2	Consequences of non-compliance.....	32
ARTICLE 21 — REPORTING.....		32
21.1	Continuous reporting.....	32
21.2	Periodic reporting: Technical reports and financial statements.....	32
21.3	Currency for financial statements and conversion into euros.....	33
21.4	Reporting language.....	33
21.5	Consequences of non-compliance.....	33
ARTICLE 22 — PAYMENTS AND RECOVERIES — CALCULATION OF AMOUNTS DUE.....		34
22.1	Payments and payment arrangements.....	34
22.2	Recoveries.....	34
22.3	Amounts due.....	34
22.4	Enforced recovery.....	39
22.5	Consequences of non-compliance.....	40
ARTICLE 23 — GUARANTEES.....		40
23.1	Prefinancing guarantee.....	40
23.2	Consequences of non-compliance.....	41
ARTICLE 24 — CERTIFICATES.....		41
ARTICLE 25 — CHECKS, REVIEWS, AUDITS AND INVESTIGATIONS — EXTENSION OF FINDINGS.....		41
25.1	Granting authority checks, reviews and audits.....	41
25.2	European Commission checks, reviews and audits in grants of other granting authorities.....	43
25.3	Access to records for assessing simplified forms of funding.....	43
25.4	OLAF, EPPO and ECA audits and investigations.....	43

25.5	Consequences of checks, reviews, audits and investigations — Extension of findings.....	43
25.6	Consequences of non-compliance.....	44
ARTICLE 26 — IMPACT EVALUATIONS.....		45
26.1	Impact evaluation.....	45
26.2	Consequences of non-compliance.....	45
<b>CHAPTER 5 CONSEQUENCES OF NON-COMPLIANCE.....</b>		<b>45</b>
<b>SECTION 1 REJECTIONS AND GRANT REDUCTION.....</b>		<b>45</b>
ARTICLE 27 — REJECTION OF CONTRIBUTIONS.....		45
27.1	Conditions.....	45
27.2	Procedure.....	45
27.3	Effects.....	46
ARTICLE 28 — GRANT REDUCTION.....		46
28.1	Conditions.....	46
28.2	Procedure.....	46
28.3	Effects.....	46
<b>SECTION 2 SUSPENSION AND TERMINATION.....</b>		<b>47</b>
ARTICLE 29 — PAYMENT DEADLINE SUSPENSION.....		47
29.1	Conditions.....	47
29.2	Procedure.....	47
ARTICLE 30 — PAYMENT SUSPENSION.....		47
30.1	Conditions.....	47
30.2	Procedure.....	48
ARTICLE 31 — GRANT AGREEMENT SUSPENSION.....		48
31.1	Consortium-requested GA suspension.....	48
31.2	EU-initiated GA suspension.....	49
ARTICLE 32 — GRANT AGREEMENT OR BENEFICIARY TERMINATION.....		50
32.1	Consortium-requested GA termination.....	50
32.2	Consortium-requested beneficiary termination.....	51
32.3	EU-initiated GA or beneficiary termination.....	52
<b>SECTION 3 OTHER CONSEQUENCES: DAMAGES AND ADMINISTRATIVE SANCTIONS.....</b>		<b>55</b>
ARTICLE 33 — DAMAGES.....		55
33.1	Liability of the granting authority.....	55
33.2	Liability of the beneficiaries.....	55
ARTICLE 34 — ADMINISTRATIVE SANCTIONS AND OTHER MEASURES.....		56
<b>SECTION 4 FORCE MAJEURE.....</b>		<b>56</b>

ARTICLE 35 — FORCE MAJEURE.....	56
<b>CHAPTER 6 FINAL PROVISIONS.....</b>	<b>56</b>
ARTICLE 36 — COMMUNICATION BETWEEN THE PARTIES.....	56
36.1 Forms and means of communication — Electronic management.....	56
36.2 Date of communication.....	57
36.3 Addresses for communication.....	57
ARTICLE 37 — INTERPRETATION OF THE AGREEMENT.....	57
ARTICLE 38 — CALCULATION OF PERIODS AND DEADLINES.....	57
ARTICLE 39 — AMENDMENTS.....	58
39.1 Conditions.....	58
39.2 Procedure.....	58
ARTICLE 40 — ACCESSION AND ADDITION OF NEW BENEFICIARIES.....	58
40.1 Accession of the beneficiaries mentioned in the Preamble.....	59
40.2 Addition of new beneficiaries.....	59
ARTICLE 41 — TRANSFER OF THE AGREEMENT.....	59
ARTICLE 42 — ASSIGNMENTS OF CLAIMS FOR PAYMENT AGAINST THE GRANTING AUTHORITY.....	59
ARTICLE 43 — APPLICABLE LAW AND SETTLEMENT OF DISPUTES.....	60
43.1 Applicable law.....	60
43.2 Dispute settlement.....	60
ARTICLE 44 — ENTRY INTO FORCE.....	60



## DATA SHEET

### 1. General data

Project summary:

Project summary
<p>The CyberHubs project aims to enhance the cybersecurity skills ecosystem in Europe by establishing a network of 7 Cybersecurity Skills Hubs in Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain, which will promote the development of digital skills in cybersecurity and support the development of a skilled cybersecurity workforce. The project is coordinated by DIGITALEUROPE, the European umbrella organisation of the digital industry, and consists of 21 full partners covering 11 European Member States. The project's objectives include conducting a comprehensive cybersecurity skills mismatches analysis with mapping existing cybersecurity education and training offers across EU Member States, developing a national cybersecurity skills strategy in each partner country, organising a European Cybersecurity Hackathon to foster innovation, establishing twinnings between Cybersecurity Skills Hubs, and promoting collaboration between education and industry sectors. The project will benefit a wide range of stakeholders including industry players, learning providers, youth, students, NEETs, and professionals, policymakers, and public organisations, NGOs, CSOs, and other social partners who will get access to a variety of cybersecurity resources raising awareness and building their capacity, as well as learning and job opportunities. Expected results of the project include the establishment of a sustainable European Network of Cybersecurity Skills Hubs, the development of national cybersecurity skills strategies, the creation of innovative cybersecurity solutions through the Hackathon, the establishment of long-term partnerships and collaboration with the wider cybersecurity ecosystem, and the dissemination of project results through various communication channels. Overall, the CyberHubs project will play a significant role in strengthening the cybersecurity workforce in Europe and promoting the digital transformation of the industry.</p>

Keywords:

- Education-enterprises partnerships
- Identification of skills needs
- digital skills
- Cybersecurity, national reference centre, skills gaps, skills shortage

Project number: 101140030

Project name: Network of European Cybersecurity Skills Hubs

Project acronym: CyberHubs

Call: ERASMUS-EDU-2023-PI-ALL-INNO

Topic: ERASMUS-EDU-2023-PI-ALL-INNO-EDU-ENTERP

Type of action: ERASMUS Lump Sum Grants

Granting authority: European Education and Culture Executive Agency

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

Project starting date: first day of the month following the entry into force date

Project end date: starting date + months of duration

Project duration: 36 months

Consortium agreement: Yes

### 2. Participants

List of participants:

N°	Role	Short name	Legal name	Ctry	PIC	Max grant amount
1	COO	DE	DIGITALEUROPE AISBL*	BE	952919756	174 416.00
2	BEN	AGORIA	AGORIA ASBL	BE	998981079	90 731.00
3	BEN	SBSEM	SOLVAY BRUSSELS SCHOOL LIFELONG LEARNING	BE	882074448	42 085.00

N°	Role	Short name	Legal name	Ctry	PIC	Max grant amount
4	BEN	HOWEST	HOGESCHOOL WEST-VLAANDEREN HOWEST	BE	998686684	42 085.00
5	BEN	ITL	EESTI INFOTEHNOLOOGIA JA TELEKOMMUNIKATSIOONI LIIT	EE	935207556	83 349.00
6	BEN	TalTech	TALLINNA TEHNIKAÜLIKOOL	EE	999842536	53 181.00
7	BEN	CCIS	GOSPODARSKA ZBORNICA SLOVENIJE	SI	999780165	104 717.00
8	BEN	UM	UNIVERZA V MARIBORU	SI	999903646	43 617.00
9	BEN	IVSZ	IVSZ - DIGITALIS VALLALKOZASOK SZOVETSEGE	HU	999794230	91 149.00
10	BEN	NKE	NEMZETI KOZSZOLGALATI EGYETEM	HU	943340812	43 382.00
11	BEN	SEPE	FEDERATION OF HELLENIC INFORMATION TECHNOLOGY AND COMMUNICATION ENTREPRISES	EL	997352546	82 921.00
12	BEN	AUEB-RC	ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER	EL	999896856	36 929.00
13	BEN	INFOBALT	ASOCIACIJA INFOBALT	LT	970234450	92 179.00
14	BEN	KTU	KAUNO TECHNOLOGIJOS UNIVERSITETAS	LT	999844961	72 009.00
15	BEN	AMETIC	ASOCIACION MULTISECTORIAL DE EMPRESAS DE LA ELECTRONICA, LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACION, DE LAS TELECOMUNICACIONES Y DE LOS CONTENIDOS DIGITALES	ES	968769750	82 424.00
16	BEN	UNIR	UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA	ES	956152281	53 467.00
17	BEN	Numeum	NUMEUM	FR	882036618	45 465.00
18	BEN	MTU	MUNSTER TECHNOLOGICAL UNIVERSITY	IE	892106673	34 579.00
19	BEN	Breyer Publico	BREYER PUBLICO S.L.	ES	881967554	80 836.00
20	BEN	EIT DIGITAL	EIT DIGITAL	BE	954616286	125 728.00
21	BEN	ADECCO	ADECCO FORMAZIONE SRL	IT	919579789	24 751.00
22	AP	AAVIT	Asociace pro aplikovany vyzkum v IT, z.s.	CZ	885627461	0.00
23	AP	DTSL	DIGITAL TECHNOLOGY SKILLS LIMITED	IE	902231436	0.00
24	AP	IT Ukraine	Association "IT Ukraine"	UA	890001773	0.00
<b>Total</b>						<b>1 500 000.00</b>

**Coordinator:**

— DIGITALEUROPE AISBL\* (DE)

**3. Grant****Maximum grant amount, total estimated eligible costs and contributions and funding rate:**

Maximum grant amount (Annex 2)	Maximum grant amount (award decision)
1 500 000.00	1 500 000.00

**Grant form:** Lump Sum**Grant mode:** Action grant**Budget categories/activity types:** Lump sum contributions**Cost eligibility options:** n/a**Budget flexibility:** No**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/ financial guarantee (if required) – whichever is the latest
					Additional prefinancing	60 days from receiving additional prefinancing report/ financial guarantee (if required) – whichever is the latest
1	1	18	Additional prefinancing report	60 days after end of reporting period	Additional prefinancing	60 days from receiving additional prefinancing report/ financial guarantee (if required) – whichever is the latest
2	19	36	Periodic report	60 days after end of reporting period	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)	600 000.00	n/a	1 - DE	n/a
			2 - AGORIA	n/a
			3 - SBSEM	n/a
			4 - HOWEST	n/a
			5 - ITL	n/a
			6 - TalTech	n/a
			7 - CCIS	n/a
			8 - UM	n/a
			9 - IVSZ	n/a
			10 - NKE	n/a
			11 - SEPE	n/a
			12 - AUEB-RC	n/a
			13 - INFOBALT	n/a
			14 - KTU	n/a
			15 - AMETIC	n/a
			16 - UNIR	n/a
			17 - Numeum	n/a
			18 - MTU	n/a
			19 - Breyer Publico	n/a

Prefinancing payment		Prefinancing guarantee		
Type	Amount	Guarantee amount	Division per participant	
Prefinancing 2 (additional)	600 000.00	n/a	20 - EIT DIGITAL	n/a
			21 - ADECCO	n/a
			1 - DE	n/a
			2 - AGORIA	n/a
			3 - SBSEM	n/a
			4 - HOWEST	n/a
			5 - ITL	n/a
			6 - TalTech	n/a
			7 - CCIS	n/a
			8 - UM	n/a
			9 - IVSZ	n/a
			10 - NKE	n/a
			11 - SEPE	n/a
			12 - AUEB-RC	n/a
			13 - INFOBALT	n/a
			14 - KTU	n/a
			15 - AMETIC	n/a
			16 - UNIR	n/a
			17 - Numeum	n/a
			18 - MTU	n/a
			19 - Breyer Publico	n/a
			20 - EIT DIGITAL	n/a
			21 - ADECCO	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): 100% of the maximum grant amount

No-profit rule: n/a

Late payment interest: ECB + 3.5%

Bank account for payments:

BE56363056109688 BBRUBEBB

Conversion into euros: n/a

Reporting language: Language of the Agreement

**4.3 Certificates** (art 24): n/a**4.4 Recoveries** (art 22)

**First-line liability for recoveries:**

Beneficiary termination: Beneficiary concerned

Final payment: Coordinator

After final payment: Beneficiary concerned

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

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

Joint and several liability of affiliated entities — n/a

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

**Applicable law (art 43):**

Standard applicable law regime: EU law + law of Belgium

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

Standard dispute settlement forum:

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

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

**6. Other**

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

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

Confidentiality (for X years after final payment): 5

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

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

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

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

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

## **CHAPTER 1 GENERAL**

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

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

### **ARTICLE 2 — DEFINITIONS**

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

## **CHAPTER 2 ACTION**

### **ARTICLE 3 — ACTION**

The grant is awarded for the action **101140030 — CyberHubs** ('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**

---

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

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

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

The grant is an action grant<sup>8</sup> which takes the form of a lump sum grant for the completion of work packages.

## 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

Not applicable

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

The estimated budget for the action (lump sum breakdown) is set out in Annex 2.

It contains the estimated eligible contributions for the action (lump sum contributions), broken down by participant and work package.

Annex 2 also shows the types of contributions (forms of funding)<sup>9</sup> to be used for each work package.

## 5.5 Budget flexibility

Budget flexibility does not apply; changes to the estimated budget (lump sum breakdown) always require an amendment (see Article 39).

Amendments for transfers between *work packages* are moreover possible only if:

- the work packages concerned are not already completed (and declared in a financial statement) and
- the transfers are justified by the technical implementation of the action.

# ARTICLE 6 — ELIGIBLE AND INELIGIBLE CONTRIBUTIONS

## 6.1 and 6.2 General and specific eligibility conditions

Lump sum contributions are eligible ('eligible contributions'), if:

- (a) they are set out in Annex 2 and
- (b) the work packages are completed and the work is properly implemented by the beneficiaries and/or the results are achieved, in accordance with Annex 1 and during in the period set out in Article 4 (with the exception of work/results relating to the submission of the final periodic report, which may be achieved afterwards; see Article 21)

They will be calculated on the basis of the amounts set out in Annex 2.

<sup>8</sup> For the definition, see Article 180(2)(a) EU Financial Regulation 2018/1046: '**action grant**' means an EU grant to finance "an action intended to help achieve a Union policy objective".

<sup>9</sup> See Article 125 EU Financial Regulation 2018/1046.





### 6.3 Ineligible contributions

‘Ineligible contributions’ are:

- (a) lump sum contributions that do not comply with the conditions set out above (see Article 6.1 and 6.2)
- (b) lump sum contributions for activities already funded 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 case:
  - (i) Synergy actions: not applicable
- (c) other:
  - (i) country restrictions for eligible costs: not applicable.

### 6.4 Consequences of non-compliance

If a beneficiary declares lump sum 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. Lump sum 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): not applicable
  - the contribution to the deliverables and technical reports (see Article 21)
  - any other documents or information required by the granting authority under the Agreement
- (iv) submit via the Portal data and information related to the participation of their affiliated entities.

(b) The coordinator must:

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

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

However, coordinators which are public bodies may delegate the tasks set out in Point (b)(ii) last

indent and (iii) above to entities with ‘authorisation to administer’ which they have created or which are controlled by or affiliated to them. In this case, the coordinator retains sole responsibility for the payments and for compliance with the obligations under the Agreement.

Moreover, coordinators which are ‘sole beneficiaries’<sup>10</sup> (or similar, such as European research infrastructure consortia (ERICs)) may delegate the tasks set out in Point (b)(i) to (iii) above to one of their members. The coordinator retains sole responsibility for compliance with the obligations under the Agreement.

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

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

- the internal organisation of the consortium
- 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

The following entities which cooperate with a beneficiary will participate in the action as ‘associated partners’:

- **Asociace pro aplikovaný výzkum v IT, z.s. (AAVIT)**, PIC 885627461
- **DIGITAL TECHNOLOGY SKILLS LIMITED (DTSL)**, PIC 902231436
- **Association "IT Ukraine" (IT Ukraine)**, PIC 890001773

Associated partners must implement the action tasks attributed to them in Annex 1 in accordance with

---

<sup>10</sup> For the definition, see Article 187(2) EU Financial Regulation 2018/1046: “Where several entities satisfy the criteria for being awarded a grant and together form one entity, that entity may be treated as the **sole beneficiary**, including where it is specifically established for the purpose of implementing the action financed by the grant.”

Article 11. They may not charge contributions to the action (no lump sum contributions) and the costs for their tasks are not eligible (may not be included in the estimated budget in Annex 2).

The tasks must be set out in Annex 1.

The beneficiaries must ensure that their contractual obligations under Articles 11 (proper implementation), 12 (conflict of interests), 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 associated partners.

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 associated partners.

## **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 contributions to the action (no lump sum contributions) and the costs for the in-kind contributions are not eligible (may not be included in the estimated budget in Annex 2).

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 beneficiaries' costs for subcontracting are considered entirely covered by the lump sum contributions for implementing the work packages (irrespective of the actual subcontracting costs incurred, if any).

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: use qualified external auditors which are independent and comply with comparable standards as those set out in EU Directive 2006/43/EC<sup>11</sup>
- for the controls under Article 25: allow for checks, reviews, audits and investigations (including on-the-spot checks, visits and inspections) by the bodies mentioned in that Article (e.g. granting authority, OLAF, Court of Auditors (ECA), etc.).

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

### 10.2 Participants which are international organisations

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

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

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

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

### 10.3 Pillar-assessed participants

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

‘Pillar-assessment’ means a review by the European Commission on the systems, rules and procedures which participants use for managing EU grants (in particular internal control system, accounting

---

<sup>11</sup> Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts or similar national regulations (OJ L 157, 9.6.2006, p. 87).

system, external audits, financing of third parties, rules on recovery and exclusion, information on recipients and protection of personal data; see Article 154 EU Financial Regulation 2018/1046).

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

- record-keeping (Article 20): may be done in accordance with internal standards, rules and procedures
- currency conversion for financial statements (Article 21): may be done in accordance with usual accounting practices
- guarantees (Article 23): for public law bodies, prefinancing guarantees are not needed
- certificates (Article 24):
  - certificates on the financial statements (CFS): may be provided by their regular internal or external auditors and in accordance with their internal financial regulations and procedures
  - certificates on usual accounting practices (CoMUC): are not needed if those practices are covered by an ex-ante assessment

and use the following specific rules, for:

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

parties' rights by the participant or one of its employees or individual for whom the employees are responsible.

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

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

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

- eligibility (Article 6)
- consortium roles and set-up (Articles 7-9)
- security and ethics (Articles 13, 14)
- IPR (including background and results, access rights and rights of use), communication, dissemination and visibility (Articles 16 and 17)
- information obligation (Article 19)
- payment, reporting and amendments (Articles 21, 22 and 39)
- rejections, reductions, suspensions and terminations (Articles 27, 28, 29-32)

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

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

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

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



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

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

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

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

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

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

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

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

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

#### **12.1 Conflict of interests**

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

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

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

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

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

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

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

#### **13.1 Sensitive information**

The parties must keep confidential any data, documents or other material (in any form) that is identified





as sensitive in writing ('sensitive information') — during the implementation of the action and for at least until the time-limit set out in the Data Sheet (see Point 6).

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

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

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

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

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

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

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

The confidentiality obligations no longer apply if:

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

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

### **13.2 Classified information**

The parties must handle classified information in accordance with the applicable EU, international or national law on classified information (in particular, Decision 2015/444<sup>12</sup> and its implementing rules).

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

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

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

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

---

<sup>12</sup> Commission Decision 2015/444/EC, Euratom of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

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

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

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

## **ARTICLE 14 — ETHICS AND VALUES**

### **14.1 Ethics**

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

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

### **14.2 Values**

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

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

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

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

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

## **ARTICLE 15 — DATA PROTECTION**

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

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

For grants where the granting authority is the European Commission, an EU regulatory or executive agency, joint undertaking or other EU body, the processing will be subject to Regulation 2018/1725<sup>13</sup>.

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

The beneficiaries must process personal data under the Agreement in compliance with the applicable EU, international and national law on data protection (in particular, Regulation 2016/679<sup>14</sup>).

---

<sup>13</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

<sup>14</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural

They must ensure that personal data is:

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

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.

---

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).

## 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 and
- (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 the 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 lump sum 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 (proper implementation of the work and/or achievement of the results as described in Annex 1) in line with the accepted standards in the respective field (if any); beneficiaries do not need to keep specific records on the actual costs incurred.

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, lump sum contributions insufficiently substantiated will be ineligible (see Article 6) and will be rejected (see Article 27), and the grant may be reduced (see Article 28).

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

## ARTICLE 21 — REPORTING

### 21.1 Continuous reporting

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

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

### 21.2 Periodic reporting: Technical reports and financial statements

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

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

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



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

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

The financial part of the periodic report includes:

- the financial statement (consolidated statement for the consortium)
- the explanation on the use of resources (or detailed cost reporting table): not applicable
- the certificates on the financial statements (CFS): not applicable.

The **financial statement** must contain the lump sum contributions indicated in Annex 2, for the work packages that were completed during the reporting period.

For the last reporting period, the beneficiaries may exceptionally also declare partial lump sum contributions for work packages that were not completed (e.g. due to force majeure or technical impossibility).

Lump sum contributions which are not declared in a financial statement will not be taken into account by the granting authority.

By signing the financial statement (directly in the Portal Periodic Reporting tool), the coordinator confirms (on behalf of the consortium) that:

- the information provided is complete, reliable and true
- the lump sum contributions declared are eligible (in particular, the work packages have been completed, that the work has been properly implemented and/or the results were achieved in accordance with Annex 1; see Article 6)
- the proper implementation and/or achievement 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).

In case of recoveries (see Article 22), beneficiaries will be held responsible also for the lump sum contributions declared for their affiliated entities (if any).

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

The financial statements must be drafted in euro.

### **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.

This will be done on the basis of work packages already completed in previous interim payments. Payments for ongoing/not yet completed work packages which the beneficiary was working on before termination (if any) will therefore be made only later on, with the next interim or final payments when those work packages have been completed.

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, on the basis of the beneficiary's lump sum contributions for the work packages which were approved in previous interim payments.

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:

{total accepted EU contribution for the beneficiary  
 minus

{prefinancing and interim payments received (if any)}.

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**).

### 22.3.3 Interim payments

Interim payments reimburse the eligible lump sum contributions claimed for work packages implemented 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 and the work packages declared. Their approval does not imply recognition of compliance, authenticity, completeness or correctness of their content.

Incomplete work packages and work packages that have not been delivered or cannot be approved will be rejected (see Article 27).

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 first calculate the ‘accepted EU contribution’ for the action for the reporting period, by calculating the lump sum contributions for the approved work packages.

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 eligible lump sum contributions claimed for the implemented work packages (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 and the work packages declared. Their approval does not imply recognition of compliance, authenticity, completeness or correctness of their content.

Work packages (or parts of them) that have not been delivered or cannot be approved will be rejected (see Article 27).

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 lump sum contributions for the approved work packages.

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

Not applicable

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

Not applicable

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 lump sum 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 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:

{total accepted EU contribution for the beneficiary

divided by  
 total accepted EU contribution for the action}  
 multiplied by  
 final grant amount for the action}.

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

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

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

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

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

## 22.4 Enforced recovery

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

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

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

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

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

The amount to be recovered will be increased by **late-payment interest** at the rate set out in Article 23.5, from the day following the payment date in the debit note, up to and including the date the full payment is received.

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



Bank charges incurred in the recovery process will be borne by the beneficiary, unless Directive 2015/2366<sup>15</sup> applies.

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

## 22.5 Consequences of non-compliance

**22.5.1** If the granting authority does not pay within the payment deadlines (see above), the beneficiaries are entitled to **late-payment interest** at the reference rate applied by the European Central Bank (ECB) for its main refinancing operations in euros, plus the percentage specified in the Data Sheet (Point 4.2). The ECB reference rate to be used 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:

---

<sup>15</sup> Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).





- (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**

Not applicable

## **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 lump sum contributions, deliverables and reports.

#### **25.1.2 Project reviews**

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

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

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

The coordinator or beneficiary concerned must cooperate diligently and provide — within the deadline requested — any information and data in addition to deliverables and reports already submitted. The granting authority may request beneficiaries to provide such information to it directly. Sensitive information and documents will be treated in accordance with Article 13.

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

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

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

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

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

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

### 25.1.3 Audits

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- the European Anti-Fraud Office (OLAF) under Regulations No 883/2013<sup>16</sup> and No 2185/96<sup>17</sup>
- the European Public Prosecutor's Office (EPPO) under Regulation 2017/1939
- the European Court of Auditors (ECA) under Article 287 of the Treaty on the Functioning of the EU (TFEU) and Article 257 of EU Financial Regulation 2018/1046.

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

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

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

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

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

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

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.

<sup>16</sup> Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18/09/2013, p. 1).

<sup>17</sup> Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities (OJ L 292, 15/11/1996, p. 2).

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

Findings 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 lump sum 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, lump sum 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 CONTRIBUTIONS**

### **27.1 Conditions**

The granting authority will — at interim payment, final payment or afterwards — reject any lump sum 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 lump sum 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 lump sum contributions, it will deduct them from the lump sum contributions declared and then calculate the amount due (and, if needed, make a recovery; see Article 22).

## **ARTICLE 28 — GRANT REDUCTION**

### **28.1 Conditions**

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

- (a) the beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed:
  - (i) substantial errors, irregularities or fraud or
  - (ii) serious breach of obligations under this Agreement or during its award (including improper implementation of the action, non-compliance with the call conditions, submission of false information, failure to provide required information, breach of ethics or security rules (if applicable), etc.), or
- (b) the beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed — in other EU grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant (extension of findings; see Article 25.5).

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 extension procedure, queries about eligibility, need for a grant reduction, etc.) and additional checks, reviews, audits or investigations are necessary, or
- (c) there are other issues affecting the EU financial interests.

#### **29.2 Procedure**

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

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

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

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

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

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

#### **30.1 Conditions**

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

- (a) a beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed or is suspected of having committed:
  - (i) substantial errors, irregularities or fraud or
  - (ii) serious breach of obligations under this Agreement or during its award (including improper implementation of the action, non-compliance with the call conditions, submission of false information, failure to provide required information, breach of ethics or security rules (if applicable), etc.), or



- (b) a beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed — in other EU grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant (extension of findings; see Article 25.5).

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. Moreover, no work may be done. Ongoing work packages must be interrupted and no new work packages may be started.

## 31.2 EU-initiated GA suspension

### 31.2.1 Conditions

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

- (a) a beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed or is suspected of having committed:
  - (i) substantial errors, irregularities or fraud or
  - (ii) serious breach of obligations under this Agreement or during its award (including improper implementation of the action, non-compliance with the call conditions, submission of false information, failure to provide required information, breach of ethics or security rules (if applicable), etc.), or
- (b) a beneficiary (or a person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed — in other EU grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant (extension of findings; see Article 25.5)
- (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. Moreover, no work may be done. Ongoing work packages must be interrupted and no new work packages may be started.

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 lump sum contributions for activities implemented before the end of work date (see Article 22). Partial lump sum contributions for work packages that were not completed (e.g. due to technical reasons) may exceptionally be taken into account.

If the granting authority does not receive the report within the deadline, only lump sum contributions which are included in an approved periodic report will be taken into account (no 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
- (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 reports submitted in previous interim payments (i.e. beneficiary's lump sum contributions for completed and approved work packages).

Lump sum contributions for ongoing/not yet completed work packages will have to be included in the periodic report for the next reporting periods when those work packages have been completed.

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

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

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

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

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

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

### **32.3 EU-initiated GA or beneficiary termination**

#### **32.3.1 Conditions**

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

- (a) one or more beneficiaries do not accede to the Agreement (see Article 40)
- (b) a change to the action or the legal, financial, technical, organisational or ownership situation of a beneficiary is likely to substantially affect the implementation of the action or calls into question the decision to award the grant (including changes linked to one of the exclusion grounds listed in the declaration of honour)
- (c) following termination of one or more beneficiaries, the necessary changes to the Agreement (and their impact on the action) would call into question the decision awarding the grant or breach the principle of equal treatment of applicants
- (d) implementation of the action has become impossible or the changes necessary for its continuation would call into question the decision awarding the grant or breach the principle of equal treatment of applicants

- (e) a beneficiary (or person with unlimited liability for its debts) is subject to bankruptcy proceedings or similar (including insolvency, winding-up, administration by a liquidator or court, arrangement with creditors, suspension of business activities, etc.)
- (f) a beneficiary (or person with unlimited liability for its debts) is in breach of social security or tax obligations
- (g) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has been found guilty of grave professional misconduct
- (h) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed fraud, corruption, or is involved in a criminal organisation, money laundering, terrorism-related crimes (including terrorism financing), child labour or human trafficking
- (i) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) was created under a different jurisdiction with the intent to circumvent fiscal, social or other legal obligations in the country of origin (or created another entity with this purpose)
- (j) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed:
  - (i) substantial errors, irregularities or fraud or
  - (ii) serious breach of obligations under this Agreement or during its award (including improper implementation of the action, non-compliance with the call conditions, submission of false information, failure to provide required information, breach of ethics or security rules (if applicable), etc.)
- (k) a beneficiary (or person having powers of representation, decision-making or control, or person essential for the award/implementation of the grant) has committed — in other EU grants awarded to it under similar conditions — systemic or recurrent errors, irregularities, fraud or serious breach of obligations that have a material impact on this grant (extension of findings; see Article 25.5)
- (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 lump sum contributions for activities implemented before termination takes effect (see Article 22). Partial lump sum contributions for work packages that were not completed (e.g. due to technical reasons) may exceptionally be taken into account.

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 lump sum contributions which are included in an approved periodic report will be taken into account (no 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

- (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 reports submitted in previous interim payments (i.e. beneficiary's lump sum contributions for completed and approved work packages).

Lump sum contributions for ongoing/not yet completed work packages will have to be included in the periodic report for the next reporting periods when those work packages have been completed.

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

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

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

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

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

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

### **ARTICLE 33 — DAMAGES**

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

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

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

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

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





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

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

Nothing in this Agreement may be construed as preventing the adoption of administrative sanctions (i.e. exclusion from EU award procedures and/or financial penalties) or other public law measures, in addition or as an alternative to the contractual measures provided under this Agreement (see, for instance, Articles 135 to 145 EU Financial Regulation 2018/1046 and Articles 4 and 7 of Regulation 2988/95<sup>18</sup>).

## **SECTION 4 FORCE MAJEURE**

### **ARTICLE 35 — FORCE MAJEURE**

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

‘Force majeure’ means any situation or event that:

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

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

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).

---

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



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

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

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

### **36.2 Date of communication**

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

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

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

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

### **36.3 Addresses for communication**

The Portal can be accessed via the Europa website.

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

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

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

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

Annex 5 takes precedence over the Terms and Conditions.

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

Annex 2 takes precedence over Annex 1.

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

In accordance with Regulation No 1182/71<sup>19</sup>, periods expressed in days, months or years are calculated from the moment the triggering event occurs.

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

‘Days’ means calendar days, not working days.

## ARTICLE 39 — AMENDMENTS

### 39.1 Conditions

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

Amendments may be requested by any of the parties.

### 39.2 Procedure

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

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

The request for amendment must include:

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

The granting authority may request additional information.

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

---

<sup>19</sup> Regulation (EEC, Euratom) No 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time-limits (OJ L 124, 8/6/1971, p. 1).

#### 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**



## **Erasmus+ (ERASMUS+)**

### **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:	101140030
Project name:	Network of European Cybersecurity Skills Hubs
Project acronym:	CyberHubs
Call:	ERASMUS-EDU-2023-PI-ALL-INNO
Topic:	ERASMUS-EDU-2023-PI-ALL-INNO-EDU-ENTERP
Type of action:	ERASMUS-LS
Service:	EACEA/A/02
Project starting date:	first day of the month following the entry into force date
Project duration:	36 months

TABLE OF CONTENTS

Project summary ..... 3

List of participants ..... 3

List of work packages ..... 5

Staff effort ..... 13

List of deliverables ..... 15

List of milestones (outputs/outcomes) ..... 22

List of critical risks ..... 22

## 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.*

The CyberHubs project aims to enhance the cybersecurity skills ecosystem in Europe by establishing a network of 7 Cybersecurity Skills Hubs in Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain, which will promote the development of digital skills in cybersecurity and support the development of a skilled cybersecurity workforce. The project is coordinated by DIGITALEUROPE, the European umbrella organisation of the digital industry, and consists of 21 full partners covering 11 European Member States.

The project's objectives include conducting a comprehensive cybersecurity skills mismatches analysis with mapping existing cybersecurity education and training offers across EU Member States, developing a national cybersecurity skills strategy in each partner country, organising a European Cybersecurity Hackathon to foster innovation, establishing twinnings between Cybersecurity Skills Hubs, and promoting collaboration between education and industry sectors.

The project will benefit a wide range of stakeholders including industry players, learning providers, youth, students, NEETs, and professionals, policymakers, and public organisations, NGOs, CSOs, and other social partners who will get access to a variety of cybersecurity resources raising awareness and building their capacity, as well as learning and job opportunities.

Expected results of the project include the establishment of a sustainable European Network of Cybersecurity Skills Hubs, the development of national cybersecurity skills strategies, the creation of innovative cybersecurity solutions through the Hackathon, the establishment of long-term partnerships and collaboration with the wider cybersecurity ecosystem, and the dissemination of project results through various communication channels.

Overall, the CyberHubs project will play a significant role in strengthening the cybersecurity workforce in Europe and promoting the digital transformation of the industry.

## LIST OF PARTICIPANTS

### PARTICIPANTS

*Grant Preparation (Beneficiaries screen) — Enter the info.*

Number	Role	Short name	Legal name	Country	PIC
1	COO	DE	DIGITALEUROPE AISBL*	BE	952919756
2	BEN	AGORIA	AGORIA ASBL	BE	998981079
3	BEN	SBSEM	SOLVAY BRUSSELS SCHOOL LIFELONG LEARNING	BE	882074448
4	BEN	HOWEST	HOGESCHOOL WEST-VLAANDEREN HOWEST	BE	998686684
5	BEN	ITL	EESTI INFOTEHNOLOOGIA JA TELEKOMMUNIKATSIOONI LIIT	EE	935207556
6	BEN	TalTech	TALLINNA TEHNICAÜLIKOOL	EE	999842536
7	BEN	CCIS	GOSPODARSKA ZBORNICA SLOVENIJE	SI	999780165
8	BEN	UM	UNIVERZA V MARIBORU	SI	999903646



**PARTICIPANTS***Grant Preparation (Beneficiaries screen) — Enter the info.*

Number	Role	Short name	Legal name	Country	PIC
9	BEN	IVSZ	IVSZ - DIGITALIS VALLALKOZASOK SZOVETSEGE	HU	999794230
10	BEN	NKE	NEMZETI KOZSZOLGALATI EGYETEM	HU	943340812
11	BEN	SEPE	FEDERATION OF HELLENIC INFORMATION TECHNOLOGY AND COMMUNICATION ENTREPRISES	EL	997352546
12	BEN	AUEB-RC	ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER	EL	999896856
13	BEN	INFOBALT	ASOCIACIJA INFOBALT	LT	970234450
14	BEN	KTU	KAUNO TECHNOLOGIJOS UNIVERSITETAS	LT	999844961
15	BEN	AMETIC	ASOCIACION MULTISECTORIAL DE EMPRESAS DE LA ELECTRONICA, LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACION, DE LAS TELECOMUNICACIONES Y DE LOS CONTENIDOS DIGITALES	ES	968769750
16	BEN	UNIR	UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA	ES	956152281
17	BEN	Numeum	NUMEUM	FR	882036618
18	BEN	MTU	MUNSTER TECHNOLOGICAL UNIVERSITY	IE	892106673
19	BEN	Breyer Publico	BREYER PUBLICO S.L.	ES	881967554
20	BEN	EIT DIGITAL	EIT DIGITAL	BE	954616286
21	BEN	ADECCO	ADECCO FORMAZIONE SRL	IT	919579789
22	AP	AAVIT	Asociace pro aplikovany vyzkum v IT, z.s.	CZ	885627461
23	AP	DTSL	DIGITAL TECHNOLOGY SKILLS LIMITED	IE	902231436
24	AP	IT Ukraine	Association "IT Ukraine"	UA	890001773

## LIST OF WORK PACKAGES

<b>Work packages</b> <i>Grant Preparation (Work Packages screen) — Enter the info.</i>						
Work Package No	Work Package name	Lead Beneficiary	Effort (Person-Months)	Start Month	End Month	Deliverables
WP1	Managing the Alliance for Innovation	1 - DE	246607.00	1	36	D1.1 – Annual work plan D1.2 – Annual project collaboration and risk management report D1.3 – Quality assurance plan
WP2	Cybersecurity skills intelligence, forecast, and strategy	14 - KTU	270522.00	1	12	D2.1 – Cybersecurity skills mismatches analysis D2.2 – Cybersecurity skills Forecasting model D2.3 – Country-specific cybersecurity skills strategies
WP3	National Cybersecurity Skills Hubs for Innovation	7 - CCIS	333937.00	9	36	D3.1 – National CyberHub governance and sustainability strategies D3.2 – CyberHub country delegation visits D3.3 – CyberHub Twinning Programme D3.4 – Alliance sustainability and exploitation strategy
WP4	CyberHub Services	9 - IVSZ	457251.00	12	36	D4.1 – Cybersecurity workshops impact assessment D4.2 – European Cybersecurity Hackathon D4.3 – Skills Academy Platform's User Manual and capacity-building
WP5	Communication, dissemination, visibility and impact	1 - DE	191683.00	1	36	D5.1 – Project communication and dissemination plan D5.2 – Project website and other communication tools

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
						D5.3 – European Cybersecurity Fest

**Work package WP1 – Managing the Alliance for Innovation**

<b>Work Package Number</b>	WP1	<b>Lead Beneficiary</b>	1 - DE
<b>Work Package Name</b>	Managing the Alliance for Innovation		
<b>Start Month</b>	1	<b>End Month</b>	36

**Objectives**

SO1: to create a long-term, sustainable partnership of key European stakeholders within the cybersecurity sector who will cooperate to develop and implement new strategic approach to address the cybersecurity skills mismatches. More specific sub-objectives include:

- To ensure the overall management and effective monitoring of the project activities in administrative, technical, and financial terms
- To foster smooth collaboration among partners, preventing and managing potential risks and misunderstandings:
- To guarantee quality content and ensure effective progress, synergies, and coherence during the implementation of the activities
- To coordinate the involvement of the experts of the project Advisory Board in different project activities

**Description**

T1.1 - Administrative and financial management:

This task covers the overall administrative and financial management of the project. DE, as project coordinator, will ensure the efficient consortium partner management and coordination, financial allocation and instalments, and budget monitoring aligned with the Grant Agreement (GA).

T1.2 - Project coordination and risk mitigation:

This task covers several activities related to project management and risk mitigation. DE, as project coordinator, will ensure the coordination of the annual work plan in close collaboration with the work package leaders (WPL). It also includes knowledge transfer and technical assistance to WP activities, risk mitigation actions in collaboration with the project Steering Committee (SC), the implementation of efficient internal communication processes and tools to facilitate collaboration, as well as the organisation of transnational project meetings (TPM) online and in-person.

T1.3 - Reporting and quality assurance:

This task covers the reporting and quality assurance activities of the project. It includes the periodical internal reporting cycles and contractual periodic reporting (progress, final) of the project. DE, as coordinator, will be liaising with EACEA and coordinating the production of the reports. A quality assurance (QA) plan with clear key performance indicators (KPI) and appropriate evaluation and monitoring measures, tools, and processes will be put in place. The results of the periodical QA assessments will be considered to continuously enhance the quality and impact of the project.

All partners contribute by providing the necessary information and supporting documents to the coordinator (DE) for the proper completion of the reporting.

T1.4 - Advisory Board coordination:

This task covers the management and coordination of the Advisory Board (AB) of the project. It includes the organisation of bi-annual online meetings and the coordination of the involvement of AB members in project activities such as the reviewing of outputs according to their expertise. Yearly, AB members will be invited to provide recommendations on project activities and share their expertise on specific aspects to improve the project's value proposition and impact.

**Work package WP2 – Cybersecurity skills intelligence, forecast, and strategy**

<b>Work Package Number</b>	WP2	<b>Lead Beneficiary</b>	14 - KTU
<b>Work Package Name</b>	Cybersecurity skills intelligence, forecast, and strategy		
<b>Start Month</b>	1	<b>End Month</b>	12

**Objectives**

SO2: to improve the quality and relevance of cybersecurity education and training programmes through the identification of country-specific cyber skills mismatches and providing innovative skills need anticipation methodology (market/

educational offering) in Belgium, Estonia, Slovenia, Hungary, Greece, Lithuania, and Spain. More specific sub-objectives include:

- To develop well-rounded, country-specific cybersecurity skills mismatches analysis uncovering the critical gaps between the market needs and education and training offering, using a common skills framework and research methodology to ensure scalability, quality, and comparability of the results across the EU
- To provide a solid, innovative cybersecurity skills forecasting model supporting labour market and education and training actors to make informed decisions and reduce the risk of future mismatches and cybersecurity professional shortages
- To elaborate country-specific cybersecurity skills strategies to reduce the cybersecurity skills mismatches in the short, medium, and long-term

### Description

#### T2.1 - Country-specific cybersecurity skills mismatches analysis (M1-M9):

This task covers the development of country-specific reports on the cybersecurity skills mismatches in Belgium, Estonia, Slovenia, Hungary, Greece, Lithuania, and Spain. All the CyberHubs will follow a common research methodology, produced by Breyer Publico, based on a multi-method approach (both quantitative and qualitative) including surveys, job vacancies scrapping (powered by the EIT Digital's Skills Academy Platform (SAP)), desk research, and expert focus groups. The mapping of skills and roles from the job vacancies and education and training programmes will follow the ENISA European Cybersecurity Skills Framework (ECSF).

The country analysis will uncover the critical market needs in terms of cybersecurity skills and professional roles demand and the education and training programmes gaps. The reports will give an accurate picture of the country cybersecurity skills ecosystem maturity, opportunities, and peculiarities. This task also ensures that EIT Digital will be able to populate the tool with existing cybersecurity education and training programmes into the platform to anticipate the piloting of the SAP at the national level in T4.3.

#### T2.2 - Cybersecurity skills forecasting model (M3-M12):

This task aims to deliver a cybersecurity skills and roles forecasting model for long-term implementation. It will be a method for the anticipation of future cybersecurity professional skills and roles demand and supply to mitigate possible and labour market imbalances. It supports the education and training providers and labour market actors in making informed decisions.

Breyer Publico will lead on the development of the forecasting model. The data to forecast cybersecurity skills demand and supply will come from a number of sources such as trends in job vacancy analysis, CEDEFOP occupational forecasts, other forecasts of market trends and expert groups. The ECSF adoption within the forecasting model will significantly benefit the comprehensiveness of the results and subsequent actions to be taken. All CyberHub partners contribute to its development to ensure that all relevant aspects, also on a national level, will be considered in the model. The specific elements of the forecasting model will be tested and validated over the project lifetime (T4.3). In the long-term, the forecasting model can be used by the CyberHub consortium members and EU-wide as a whole (foreseen as part of the sustainability and exploitation plan) to produce their country-specific cybersecurity skills forecasts on a regular basis.

#### T2.3 - Country-specific cybersecurity skills strategy (M9-M12):

This task covers the elaboration of country-specific cybersecurity skills strategies to reduce the cybersecurity skills mismatches in the short, medium, and long-term. It will build on the results of the cybersecurity skills mismatches analysis of T2.1, the already existing documentation and studies (e.g., the European Cybersecurity Skills Strategy of the blueprint project REWIRE, and the cybersecurity skills forecast model (T2.2) to define specific approaches that are country relevant and viable, and involve the essential ecosystem players (mapping of national actors active in the cybersecurity field) to drive efficient, innovative, systemic cybersecurity upskilling and reskilling in the country.

KTU will benchmark the existing documentation and studies on cybersecurity skills development at the EU level and coordinate the alignment actions with regards to relevant European frameworks and tools such as the ENISA's European Cybersecurity Skills Framework (ECSF), ESCO, and Europass opportunities. All CyberHubs will produce a country strategy following guidance provided by KTU, Breyer Publico, and DE.

## Work package WP3 – National Cybersecurity Skills Hubs for Innovation

<b>Work Package Number</b>	WP3	<b>Lead Beneficiary</b>	7 - CCIS
<b>Work Package Name</b>	National Cybersecurity Skills Hubs for Innovation		
<b>Start Month</b>	9	<b>End Month</b>	36

**Objectives**

SO1: to create a long-term, sustainable partnership of key European stakeholders within the cybersecurity sector who will cooperate to develop and implement new strategic approach to address the cybersecurity skills mismatches. SO3: to foster the development of national cyber skills incubators (i.e., the “CyberHubs”) across the EU, promoting cyber skills development, innovation, and entrepreneurship. SO4: to facilitate knowledge transfer, the exchange of good practices and information between higher education institutions, vocational education and training, and the business sector in the field of cybersecurity. More specific sub-objectives include:

- To establish national cybersecurity incubators (i.e., the “CyberHubs”) across the EU, promoting cybersecurity skills development, innovation, and entrepreneurship
- To improve knowledge transfer and accelerate the exchange of good practices between education, industry, and the public actors in the field of cybersecurity
- To ensure the EU-wide exploitation of the project results, develop a financial sustainability approach for the CyberHubs, and develop relevant collaboration avenues with existing projects, initiatives, and actors in the cybersecurity field.

**Description**

T3.1 - Setting up, developing, and sustaining National CyberHubs (M9-M15):

This task covers the establishment and sustainable development of solid innovation ecosystems focused on skills in the cybersecurity field — the CyberHubs — in 7 countries (Belgium, Estonia, Slovenia, Hungary, Greece, Lithuania, and Spain). All CyberHubs (industry-education pairs) will collaborate to define their CyberHub modus operandi including:

- Developing the CyberHub collaboration processes and structure at the national level (inc. the organisation of CyberHub quarterly meetings)
- Establishing the governance of the CyberHub including a sustainability and exploitation strategy (inc. mapping of national and EU funding opportunities, invitations to key actors identified within T2.3)
- Developing an action plan for the delivery of the CyberHub services (inc. KPIs) stemming from the national cybersecurity skills strategies (D2.2).

It is to be noted that CyberHubs will consult students and student entrepreneurs to validate their needs and action plans and ensure the CyberHub can answer to their needs. DE will support the task to ensure an overall coherence between the CyberHubs and at the EU level.

T3.2 - Knowledge transfer activities (M9-M18):

This task aims to ensure efficient knowledge transfer and the exchange of innovative practices between the CyberHubs so they can support each other’s development and considerably reduce the learning curve. This task builds on the expertise of the two cybersecurity champion industry partners — Numeum and MTU (representing Cyber Ireland) who both have already well-established collaboration at the national level (France and Ireland) with industry, academia, start-ups, and government in the field of cybersecurity and Adecco which has longstanding expertise in VET and employment services. The knowledge transfer activities foreseen include:

- CyberHub country delegation visits to Champion partners. The 7 delegations will be composed of two representatives from the CyberHub partners (1 industry and 1 education representative). The visits will aim to present the functioning of the Campus Cyber (Numeum) and Cyber Ireland’s cluster (MTU). The detailed scope of the delegation visits will be developed and prepared by Numeum, in collaboration with Cyber Ireland.
- A CyberHub Twinning programme to support the actual implementation and adoption of practices/services under WP4. The twinning will focus on practices which have organically been developed as a good practice in a specific organisation/region/country (originator) within and beyond the partnership and are then being transferred to another (adopter) a.k.a. the CyberHubs. All CyberHubs (7 twinings) will be able to take part in the twinning programme with the aim to strengthen transnational cooperation for cybersecurity skills development, create synergies and fostering capacity to develop educational projects in higher education and VET, drive innovation and sustainable development in the cybersecurity field.

T3.3 - Alliance sustainability and exploitation strategy (M9-M36):

This task covers the design of a solid sustainability and exploitation strategy for the CyberHub Alliance for Innovation. DE, together with the WPLs, cybersecurity champion partners, Adecco, and Breyer Publico will develop a report including the identification of key exploitable results (KER) and ways to exploit them in the long-term, the investigation of funding opportunities at the local and EU level to ensure financial sustainability, a proposed model for expansion and other sustainability measures. The proposed strategy will be further reviewed and validated throughout the project duration and according to the input provided by the CyberHubs in their national CyberHub Governance and Sustainability strategies (D3.1).

This task also includes the definition and implementation of collaboration avenues with relevant organisations, projects,

and initiatives — such as ENISA, ECCC, ECCO, the Cybersecurity Skills Academy, EDHIs, DSJP, NCCs, ECSO, the REWIRE project, and more — to increase the relevance and impact of the project results and outputs.

## Work package WP4 – CyberHub Services

<b>Work Package Number</b>	WP4	<b>Lead Beneficiary</b>	9 - IVSZ
<b>Work Package Name</b>	CyberHub Services		
<b>Start Month</b>	12	<b>End Month</b>	36

### Objectives

SO5: to increase the number of cybersecurity professionals in Europe by matching skills supply and job demand, engaging key players at the national and EU level, and attracting and retaining more talents in the cybersecurity field in Europe. SO6: to promote an entrepreneurial mindset as well as diversity and inclusion in the field of cybersecurity by engaging youth and addressing underrepresented groups in the ICT industry in Europe. SO7: to increase awareness and understanding of cybersecurity threats and good practices for cyber resilience among the general public. More specific sub-objectives include:

- To build the capacity in and raise awareness about cybersecurity with the aim to increase the number of cybersecurity professionals, and attract and retain EU talents
- To foster an entrepreneurial mindset as well as ensure diversity and inclusion in the field of cybersecurity through the engagement of youth and underrepresented groups in relevant activities
- To pilot a cutting edge platform aiming to match EU citizens' skills with jobs in the cybersecurity field

### Description

T4.1 - Cybersecurity skills awareness raising, stakeholder engagement, and capacity-building activities (M15-M36): This task aims to implement awareness raising, stakeholder engagement, and capacity-building activities/workshops. The design of the activities aims to strengthen the impact of and work in synergy with the actions and services mapped in CyberHub action plan (MS5), while considering the country perspective (D.2.3). The awareness raising and capacity-building activities will be designed to offer value added to a wide range of individuals from cybersecurity professionals to C-level workers, to SMEs, to academic staff and student entrepreneurs. They will aim to have an inclusive reach towards underrepresented groups in the cybersecurity field such as women and girls. The activities (online, in-person, or hybrid) will be delivered in a multimodal way, when possible, to widen participation and increase flexibility. All CyberHubs will choose whether to offer the workshops in the national language or in English. Examples of the type of activities foreseen include but are not limited to:

- (Joint) talks and workshops by education and industry players
- Cybersecurity readiness sessions and awareness raising
- Design thinking workshops and/or coaching
- Career fairs
- Tandem meetings for a practical sharing of experience and skills in the sector

The task also includes stakeholder engagement activities such as organising roundtables with relevant actors at the national level to discuss cybersecurity employment trends, skills and jobs, innovation cafés to gather education and training and industry representatives to discuss talent retention, skills mismatches and public-private partnerships, etc. IVSZ is leading the task and develop processes to log and evaluate the performance of the activities. Adecco will ensure the VET perspective is taken into account when designing activities and MTU and Numeum will provide their expertise. All CyberHubs will implement a set of 10 activities throughout the duration of this task.

#### T4.2 - European Cybersecurity Hackathon (M9-M23):

This task covers the preparations and organisation of an online European Cybersecurity Hackathon (during the month of October—"European Cybersecurity Month") to gather student entrepreneurs and students from a wide range of fields, e.g., engineering, economics, social sciences, who are interested in cybersecurity to solve real-world problems. The challenges will be proposed and sponsored by organisations and the CyberHub ecosystems under various pillars. The competitors will be able to deepen their understanding of today's cybersecurity challenges and contribute with their ideas to the development of solutions that can be brought to life in the medium to long-term.

Groups of 3 to 5 participants will be given a real problem to solve in real time, working together in an international team.



Clear, inclusive, transparent selection and awarding criteria will be elaborated. The challenges will be relevant to the persons expertise allowing them to combine their complementary background and interests.

NKE, supported by UM, Adecco, will coordinate the conceptualisation of the Hackathon and manage the organisational and logistical aspects. The task involves the establishment of the jury, composed of experts and financial investors in the field of cybersecurity supported by MTU and Numeum. NKE will create a team of mentors, who will provide the competitor teams with guidance on how to take their ideas further during and after the competition.

#### T4.3 - Piloting of a national AI-assisted system to match skills and jobs and forecasting model testing (M12-M36):

This task covers the testing of the cybersecurity skills forecasting model and piloting of the EIT Digital SAP — an AI-assisted tool designed to match skills and jobs — in the 7 countries represented by the CyberHubs. The platform will be piloted with 140 users (20 per CyberHub). The rationale is for the CyberHubs to be able to offer a fully researched service to match the individuals' skills with cybersecurity jobs as well as to be able to anticipate the cybersecurity skills and roles demand in their country. The anonymised skills-matching solution enables a candidate to be discovered in a skills-first job and career-matching process that supports inclusivity. The candidates will be able to proactively apply for any great matches. This element will help (future) professionals to identify the most suitable career path based on their current skills and interests as well as the skills they will upskill or reskill. Equally, the recruiters will see anonymised skills-based matches and on that basis, they can decide to invite the candidate into the process bypassing any subconscious hiring bias, and in turn, supporting diversity and inclusion. SAP supports, in an innovative way, a student-centred learning approach offering personalised learning recommendations over 100+ learning and development programmes integrated and further populated in T2.1. The platform provides a seamless medium to measure the current skills in supply and an opportunity for the students to upskill or reskill for a desired role or position in the cybersecurity field.

EIT Digital will provide the technical and operational assistance to all CyberHubs.

Within this task, the CyberHubs will also test and validate specific elements of the cybersecurity skills forecasting model (D2.2) with the guidance of Breyer Publico. These elements include trends in the job vacancy analysis and input from reports, but also a test on how expert groups can contribute to improving the forecasting results of the model. Near the end of year 2 and year 3 it will be evaluated if the model is predicting the right trend based on the results of year 1 and year 2. The result of this sub-task will be a refined cybersecurity skills forecasting model.

## Work package WP5 – Communication, dissemination, visibility and impact

<b>Work Package Number</b>	WP5	<b>Lead Beneficiary</b>	1 - DE
<b>Work Package Name</b>	Communication, dissemination, visibility and impact		
<b>Start Month</b>	1	<b>End Month</b>	36

### Objectives

SO4: to facilitate knowledge transfer, the exchange of good practices and information between higher education institutions, vocational education and training, and the business sector in the field of cybersecurity. SO6: to promote an entrepreneurial mindset as well as diversity and inclusion in the field of cybersecurity by engaging youth and addressing underrepresented groups in the ICT industry in Europe. SO7: to increase awareness and understanding of cybersecurity threats and good practices for cyber resilience among the general public.

More specific sub-objectives include:

- To ensure the widespread dissemination of the project outputs and results during the project's lifetime
- To increase the impact of the project activities and EU-wide uptake of the outputs by the project's target groups
- To ensure high visibility for the CyberHubs at the EU and national level
- To raise awareness about cybersecurity and further the exchange of good practices for cybersecurity resilience

### Description

#### T5.1 - Alliance communication and dissemination coordination (M1-M36):

This task covers all the aspects related to the communication and dissemination of the project including:

- Defining and developing the CyberHub brand concept, strategy, and visual identity.
- Developing a communication and dissemination plan including audience segmentation, key messages, promotional strategy, communication tools.
- Setting up key performance indicators (KPIs) and internal dissemination processes for implementation and reporting.
- Setting up and management of the external project communication channels including the project website.



- Delivering communication packages and visual templates for the CyberHubs to facilitate efficient communication activities.
- Supporting WPs where needed for optimal delivery and publication of the outputs/results.

#### T5.2 - CyberHubs visibility and impact at the national and EU level (M1-M36):

This task aims at ensuring the widespread visibility and impact of the CyberHubs at the national and EU level.

At the national level, CyberHubs, in particular business associations, will coordinate and implement communication and dissemination activities in the local language to reach the local communities and ensure impact. It includes, but is not limited to, regular publishing of information about the CyberHubs and their activities on different platforms including their own websites and social media channels (using the common CyberHub branding), leveraging the relevant, established national channels of communication such as the National Coalition for Digital Skills and Jobs platforms in each represented countries (where CCIS, IVSZ, and AMETIC are already leading their respective coalitions), linking their activities with the work of the national nodes of the European Digital Innovation Hubs (especially those focused on cybersecurity in Spain, Slovenia, Lithuania, Hungary, Belgium, and Greece), running communication campaigns to raise awareness about cybersecurity, sending regular briefs to engaged stakeholders on the CyberHub activities, and organising a national conference (1 per CyberHub) to gather the key players in the cybersecurity field to discuss topical issues related to education and cybersecurity policies, and industry-education cooperation in the field of cybersecurity.

At the EU level, a large-scale “European Cybersecurity Fest” will be organised by Infobalt (final conference) to showcase and discuss the CyberHubs’ achievements and key benefits for member states and society at large with EU key players including policymakers, and industry and education representatives. DE will ensure representation to relevant third-party conferences such as the annual European Cybersecurity Conference where the learnings and strategic dimensions will be highlighted and transferred to ensure other actors can benefit from the project in the long-term — this activity will be linked to the long-term sustainability and exploitation strategy of the Alliance under WP3.

## 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 - DE	60377.00	23215.00	26959.00	7491.00	56376.00	174418.00
2 - AGORIA	15705.00	15405.00	16916.00	26488.00	16218.00	90732.00
3 - SBSEM	7557.00	5503.00	12517.00	11006.00	5503.00	42086.00
4 - HOWEST	7557.00	5503.00	12517.00	11006.00	5503.00	42086.00
5 - ITL	9200.00	10590.00	18627.00	32307.00	12624.00	83348.00
6 - TalTech	7574.00	9799.00	16209.00	14698.00	4900.00	53180.00
7 - CCIS	12959.00	10049.00	44091.00	27629.00	9988.00	104716.00
8 - UM	7446.00	6504.00	11267.00	15148.00	3252.00	43617.00
9 - IVSZ	9816.00	7857.00	16273.00	47729.00	9474.00	91149.00
10 - NKE	4780.00	4647.00	7334.00	25071.00	1549.00	43381.00
11 - SEPE	10035.00	15918.00	17429.00	25332.00	14207.00	82921.00
12 - AUEB-RC	6603.00	6650.00	10377.00	11083.00	2216.00	36929.00
13 - INFOBALT	9504.00	12555.00	16667.00	24476.00	28978.00	92180.00
14 - KTU	16068.00	20026.00	16659.00	14207.00	5049.00	72009.00
15 - AMETIC	10201.00	15161.00	19145.00	27823.00	10095.00	82425.00
16 - UNIR	11699.00	11502.00	11502.00	13012.00	5751.00	53466.00
17 - Numeum	9521.00		29097.00	6846.00		45464.00
18 - MTU	6988.00		14651.00	12940.00		34579.00
19 - Breyer Publico	11977.00	56381.00	6239.00	6239.00		80836.00

Staff effort per participant						
Grant Preparation (Work packages - Effort screen) — Enter the info.						
Participant	WP1	WP2	WP3	WP4	WP5	Total Person-Months
20 - EIT DIGITAL	5212.00	33257.00		87259.00		125728.00
21 - ADECCO	5828.00		9461.00	9461.00		24750.00
Total Person-Months	246607.00	270522.00	333937.00	457251.00	191683.00	1500000.00

## LIST OF DELIVERABLES

<b>Deliverables</b> <i>Grant Preparation (Deliverables screen) — Enter the info.</i> <i>The labels used mean:</i> <i>Public — fully open (🚩 automatically posted online)</i> <i>Sensitive — limited under the conditions of the Grant Agreement</i> <i>EU classified —RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision <a href="#">2015/444</a></i>						
Deliverable No	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month)
D1.1	Annual work plan	WP1	1 - DE	R — Document, report	SEN - Sensitive	24
D1.2	Annual project collaboration and risk management report	WP1	1 - DE	R — Document, report	SEN - Sensitive	36
D1.3	Quality assurance plan	WP1	1 - DE	R — Document, report	SEN - Sensitive	2
D2.1	Cybersecurity skills mismatches analysis	WP2	1 - DE	R — Document, report	PU - Public	9
D2.2	Cybersecurity skills Forecasting model	WP2	19 - Breyer Publico	R — Document, report	PU - Public	12
D2.3	Country-specific cybersecurity skills strategies	WP2	14 - KTU	R — Document, report	PU - Public	12
D3.1	National CyberHub governance and sustainability strategies	WP3	7 - CCIS	R — Document, report	SEN - Sensitive	12
D3.2	CyberHub country delegation visits	WP3	17 - Numeum	R — Document, report	PU - Public	18
D3.3	CyberHub Twinning Programme	WP3	21 - ADECCO	R — Document, report	PU - Public	18
D3.4	Alliance sustainability and exploitation strategy	WP3	1 - DE	R — Document, report	SEN - Sensitive	36
D4.1	Cybersecurity workshops impact assessment	WP4	9 - IVSZ	R — Document, report	PU - Public	36
D4.2	European Cybersecurity Hackathon	WP4	10 - NKE	OTHER	PU - Public	22

**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)
D4.3	Skills Academy Platform's User Manual and capacity-building	WP4	20 - EIT DIGITAL	R — Document, report	PU - Public	13
D5.1	Project communication and dissemination plan	WP5	1 - DE	R — Document, report	PU - Public	5
D5.2	Project website and other communication tools	WP5	1 - DE	R — Document, report	PU - Public	8
D5.3	European Cybersecurity Fest	WP5	13 - INFOBALT	OTHER	PU - Public	34

**Deliverable D1.1 – Annual work plan**

<b>Deliverable Number</b>	D1.1	<b>Lead Beneficiary</b>	1 - DE
<b>Deliverable Name</b>	Annual work plan		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	SEN - Sensitive
<b>Due Date (month)</b>	24	<b>Work Package No</b>	WP1

Description
Annual, operational work plans produced by DE and WPLs to present the active WP tasks, sub-tasks, and activities of the year ahead. They help to visualise and coordinate the work among involved partners including KPIs and timelines. // Electronic format, 10 pages, EN.

**Deliverable D1.2 – Annual project collaboration and risk management report**

<b>Deliverable Number</b>	D1.2	<b>Lead Beneficiary</b>	1 - DE
<b>Deliverable Name</b>	Annual project collaboration and risk management report		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	SEN - Sensitive
<b>Due Date (month)</b>	36	<b>Work Package No</b>	WP1

Description
Annual reports produced by DE with input from the SC and AB to present the main outcomes of TPMs and elaborate on the risk mitigation actions and decisions taken, as well as their potential impact on the work plan and implemented/foreseen adaptations. // Electronic format, 10 pages, EN.

**Deliverable D1.3 – Quality assurance plan**

<b>Deliverable Number</b>	D1.3	<b>Lead Beneficiary</b>	1 - DE
<b>Deliverable Name</b>	Quality assurance plan		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	SEN - Sensitive
<b>Due Date (month)</b>	2	<b>Work Package No</b>	WP1

Description
The quality assurance (QA) plan to present the QA and impact assessment procedures of the project. It will serve as a basis to periodically evaluate and further improve the overall impact of the project's results, outcomes, and outputs. // Electronic format, 25 pages, EN.

**Deliverable D2.1 – Cybersecurity skills mismatches analysis**

<b>Deliverable Number</b>	D2.1	<b>Lead Beneficiary</b>	1 - DE
<b>Deliverable Name</b>	Cybersecurity skills mismatches analysis		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	PU - Public
<b>Due Date (month)</b>	9	<b>Work Package No</b>	WP2

Description
7 country reports on the cybersecurity skills mismatches in Belgium, Estonia, Slovenia, Hungary, Greece, Lithuania, and Spain based on a common research methodological approach. // Electronic format, 30 pages, EN and local languages.

### Deliverable D2.2 – Cybersecurity skills Forecasting model

<b>Deliverable Number</b>	D2.2	<b>Lead Beneficiary</b>	19 - Breyer Publico
<b>Deliverable Name</b>	Cybersecurity skills Forecasting model		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	PU - Public
<b>Due Date (month)</b>	12	<b>Work Package No</b>	WP2

Description
Report to propose a novel methodological framework for forecasting demand for cybersecurity skills across EU countries and matching this against the educational offer. // Electronic format, 30 pages

### Deliverable D2.3 – Country-specific cybersecurity skills strategies

<b>Deliverable Number</b>	D2.3	<b>Lead Beneficiary</b>	14 - KTU
<b>Deliverable Name</b>	Country-specific cybersecurity skills strategies		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	PU - Public
<b>Due Date (month)</b>	12	<b>Work Package No</b>	WP2

Description
7 country-specific strategies to address the cybersecurity skills mismatches in the short, medium and long-term. // Electronic format, 20 pages, EN and local languages.

### Deliverable D3.1 – National CyberHub governance and sustainability strategies

<b>Deliverable Number</b>	D3.1	<b>Lead Beneficiary</b>	7 - CCIS
<b>Deliverable Name</b>	National CyberHub governance and sustainability strategies		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	SEN - Sensitive
<b>Due Date (month)</b>	12	<b>Work Package No</b>	WP3

Description
7 CyberHub-specific reports detailing the collaboration processes and structure, governance and sustainability and exploitation strategy. They will define the modus operandi of each CyberHub. // Electronic format, 20 pages, EN

### Deliverable D3.2 – CyberHub country delegation visits

<b>Deliverable Number</b>	D3.2	<b>Lead Beneficiary</b>	17 - Numeum
<b>Deliverable Name</b>	CyberHub country delegation visits		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	PU - Public

<b>Due Date (month)</b>	18	<b>Work Package No</b>	WP3
-------------------------	----	------------------------	-----

Description
Report on the results and learnings of the CyberHub country delegation visits to the two cybersecurity champion partners. // Electronic format, 10 pages, EN.

### Deliverable D3.3 – CyberHub Twinning Programme

<b>Deliverable Number</b>	D3.3	<b>Lead Beneficiary</b>	21 - ADECCO
<b>Deliverable Name</b>	CyberHub Twinning Programme		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	PU - Public
<b>Due Date (month)</b>	18	<b>Work Package No</b>	WP3

Description
Report on the results and learnings of the 7 CyberHub twinnings. // Electronic format, 10 pages, EN.

### Deliverable D3.4 – Alliance sustainability and exploitation strategy

<b>Deliverable Number</b>	D3.4	<b>Lead Beneficiary</b>	1 - DE
<b>Deliverable Name</b>	Alliance sustainability and exploitation strategy		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	SEN - Sensitive
<b>Due Date (month)</b>	36	<b>Work Package No</b>	WP3

Description
Report (updated each year) to define the sustainability and exploitation strategy of the Alliance. // Electronic format, 10 pages, EN.

### Deliverable D4.1 – Cybersecurity workshops impact assessment

<b>Deliverable Number</b>	D4.1	<b>Lead Beneficiary</b>	9 - IVSZ
<b>Deliverable Name</b>	Cybersecurity workshops impact assessment		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	PU - Public
<b>Due Date (month)</b>	36	<b>Work Package No</b>	WP4

Description
Yearly impact assessment report on the awareness raising, stakeholder engagement, and capacity-building activities across the 7 CyberHubs. // Electronic format, 10 pages, EN.

### Deliverable D4.2 – European Cybersecurity Hackathon

<b>Deliverable Number</b>	D4.2	<b>Lead Beneficiary</b>	10 - NKE
<b>Deliverable Name</b>	European Cybersecurity Hackathon		



<b>Type</b>	OTHER	<b>Dissemination Level</b>	PU - Public
<b>Due Date (month)</b>	22	<b>Work Package No</b>	WP4

Description
Online European Cybersecurity Hackathon gathering pan-European, multi-disciplinary teams to solve real-world problems in the cybersecurity field.

### Deliverable D4.3 – Skills Academy Platform’s User Manual and capacity-building

<b>Deliverable Number</b>	D4.3	<b>Lead Beneficiary</b>	20 - EIT DIGITAL
<b>Deliverable Name</b>	Skills Academy Platform’s User Manual and capacity-building		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	PU - Public
<b>Due Date (month)</b>	13	<b>Work Package No</b>	WP4

Description
User Manual detailing how to use the functionalities and navigate the EIT Digital’s Skills Academy Platform and capacity building to the CyberHubs. // Electronic format, 15 pages, EN.

### Deliverable D5.1 – Project communication and dissemination plan

<b>Deliverable Number</b>	D5.1	<b>Lead Beneficiary</b>	1 - DE
<b>Deliverable Name</b>	Project communication and dissemination plan		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	PU - Public
<b>Due Date (month)</b>	5	<b>Work Package No</b>	WP5

Description
The communication and dissemination plan sets a clear framework that ensures consistent and coherent communication and dissemination activities throughout the project’s lifetime. // Electronic format, 20 pages, EN

### Deliverable D5.2 – Project website and other communication tools

<b>Deliverable Number</b>	D5.2	<b>Lead Beneficiary</b>	1 - DE
<b>Deliverable Name</b>	Project website and other communication tools		
<b>Type</b>	R — Document, report	<b>Dissemination Level</b>	PU - Public
<b>Due Date (month)</b>	8	<b>Work Package No</b>	WP5

Description
The project website and other communication tools and channels (e.g., social media, videos...) will serve the project dissemination and outreach activities during the project’s lifetime. // Electronic format, EN

**Deliverable D5.3 – European Cybersecurity Fest**

<b>Deliverable Number</b>	D5.3	<b>Lead Beneficiary</b>	13 - INFOBALT
<b>Deliverable Name</b>	European Cybersecurity Fest		
<b>Type</b>	OTHER	<b>Dissemination Level</b>	PU - Public
<b>Due Date (month)</b>	34	<b>Work Package No</b>	WP5

<b>Description</b>
The European Cybersecurity Fest will serve as the final conference of the project and will be organised during October 2026 (“European Cybersecurity Month”). // EN

## 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	Transnational project meetings (TPM)	WP1	1 - DE	Minutes of the meetings	34
2	Research methodology	WP2	19 - Breyer Publico	Timely delivery	3
3	National CyberHub action plans	WP3	7 - CCIS	CyberHub education and industry partners as well as student entrepreneurs validate the action plans	15
4	Completed piloting of the EIT Digital's Skills Academy Platform (SAP)	WP4	20 - EIT DIGITAL	140 users (20 per CyberHub) on the SAP.	36
5	Communication Performance analysis reports	WP5	1 - DE	All CyberHub have filled in the reporting tool in time to perform the analysis.	36

## 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	Delayed delivery of project outputs. The project may experience delays in delivering its outputs, which could have a negative impact on the project timeline and budget.	WP1	The project consortium will establish a detailed project schedule with realistic timelines, monitor progress closely, and adjust the schedule as necessary to keep the project on track.
2	Inadequate stakeholder engagement Failure to engage effectively with stakeholders could result in	WP1	The project consortium will establish a communication and dissemination plan (including

<b>Critical risks &amp; risk management strategy</b> <i>Grant Preparation (Critical Risks screen) — Enter the info.</i>			
<b>Risk number</b>	<b>Description</b>	<b>Work Package No(s)</b>	<b>Proposed Mitigation Measures</b>
	a lack of support or buy-in for the project, which could hinder its success.		stakeholder engagement tactics) and regularly communicate with stakeholders to keep them informed and involved throughout the project.
3	Incomplete or inaccurate data If the project relies on data that is incomplete or inaccurate (the skills mismatches analysis at the national level), it may not be able to achieve its objectives or deliver its outputs.	WP2	The Project consortium will establish data quality standards and procedures for data collection and analysis, and implement regular checks and audits to ensure data accuracy and completeness.
4	Technological issues. The project may encounter technological issues that could impact its ability to deliver its outputs or achieve its objectives (for example in the piloting of the EITs Digital AI-assisted Skills Academy Platform (SAP) to match jobs and skills across the 7 CyberHubs	WP4, WP1	The project consortium will establish a technology risk management plan and work with experts to identify and address potential issues early on. The Project Director has also a strong background in ICT and information management, that will facilitate the early identification of potential issues related to technology.
5	Budget overrun If the project experiences unexpected costs or cost overruns, it could impact its ability to deliver its outputs and achieve its objectives.	WP1	The Project Director and the Project Manager at DIGITALEUROPE will establish a detailed budget and regularly monitor expenses to ensure that the project stays on track financially.
6	Inadequate team capacity If the project team within a partner or the whole project team working in a task lacks the necessary skills or resources to deliver its outputs, it could impact the project's success.	WP4, WP2, WP1, WP3, WP5	The Project Director at DIGITALEUROPE will regularly assess team capacity and identify any gaps or areas for improvement, and provide training or additional resources as needed.
7	Changes in policy or regulations Changes in EU policy or regulations on cybersecurity or skills management could impact the project's ability to deliver its outputs or to a certain extent, to achieve its objectives.	WP4, WP2, WP1, WP3, WP5	The policy team at DIGITALEUROPE will regularly monitor relevant policies and regulations in the area and the Project Director and Project Manager will adjust the project plan as necessary to ensure compliance.
8	Intellectual property issues The project may encounter issues related to intellectual property-related to the background of the partners or	WP4, WP1	The Project Director will establish an intellectual property policy and work with legal experts to identify and address potential issues early on. The Consortium Agreement will include

<b>Critical risks &amp; risk management strategy</b> <i>Grant Preparation (Critical Risks screen) — Enter the info.</i>			
<b>Risk number</b>	<b>Description</b>	<b>Work Package No(s)</b>	<b>Proposed Mitigation Measures</b>
	ownership disputes regarding project outputs at the country level.		a considerable number of clauses related to intellectual property and the availability of the project outcomes.
9	Language and cultural barriers The project involves multiple partners from different countries, which could result in language and cultural barriers that impact communication and collaboration.	WP1	The Communication Manager in coordination with the Project Manager at DIGITALEUROPE will establish communication protocols and provide training to team members to ensure effective cross cultural communication.
10	Lack of interest or uptake from target audiences If the project outputs are not of interest or relevant to its target audiences, it could affect the impact and overall success of the project (for example lack of interest by national stakeholders in using AI assisted Skills Academy Platform (SAP) to match jobs and skills in their context)	WP4, WP2, WP1, WP3, WP5	The Project Director with the support and overall advice of the AB will conduct regular market research to ensure that the project outputs are meeting the needs of the target audience and adjust the project plan as necessary to ensure relevance and uptake



## TECHNICAL DESCRIPTION (PART B)

PROJECT	
Project name:	European Network of Cybersecurity Skills Hubs
Project acronym:	CyberHubs
Coordinator contact:	Jose Martinez-Usero, DIGITALEUROPE

## TABLE OF CONTENTS

<b>TECHNICAL DESCRIPTION (PART B)</b>	<b>1</b>
<b>PROJECT SUMMARY</b>	<b>2</b>
<b>1. RELEVANCE</b>	<b>2</b>
1.1 Background and general objectives	2
1.2 Needs analysis and specific objectives	4
1.3 Complementarity with other actions and innovation — European added value	8
<b>2. QUALITY</b>	<b>16</b>
2.1 PROJECT DESIGN AND IMPLEMENTATION	16
2.1.1 Concept and methodology	16
2.1.2 Project management, quality assurance and monitoring and evaluation strategy	19
2.1.3 Project teams, staff and experts	23
2.1.4 Cost effectiveness and financial management	29
2.1.5 Risk management	31
2.2 PARTNERSHIP AND COOPERATION ARRANGEMENTS	32
2.2.1 Consortium set-up	32
2.2.2 Consortium management and decision-making	40
<b>3. IMPACT</b>	<b>41</b>
3.1 Impact and ambition	41
3.2 Communication, dissemination and visibility	46
3.3 Sustainability and continuation	49
<b>4. WORK PLAN, WORK PACKAGES, ACTIVITIES, RESOURCES AND TIMING</b>	<b>53</b>
4.1 Work plan	53
4.2 Work packages, activities, resources and timing	53
Work Package 1	55
Work Package 2	59
Work Package 3	63
Work Package 4	68
Work Package 5	73
Staff effort (n/a for Lump Sum Grants)	77
Subcontracting (n/a for prefixed Lump Sum Grants)	80
Events meetings and mobility	80
Timetable	83
<b>5. OTHER</b>	<b>86</b>
5.1 Ethics	86
5.2 Security	87

**6. DECLARATIONS..... 87****ANNEXES..... 89**

#@APP-FORM-ERASMUSBLSII@#

#@PRJ-SUM-PS@# [This document is tagged. Do not delete the tags; they are needed for the processing.]

**PROJECT SUMMARY****Project summary (in English)**

The CyberHubs project aims to enhance the cybersecurity skills ecosystem in Europe by establishing a network of 7 Cybersecurity Skills Hubs in Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain, which will promote the development of digital skills in cybersecurity and support the development of a skilled cybersecurity workforce. The project is coordinated by DIGITALEUROPE, the European umbrella organisation of the digital industry, and consists of 21 full partners covering 11 European Member States.

The project's objectives include conducting comprehensive cybersecurity skills mismatches analysis including mapping existing cybersecurity education and training offers across EU Member States, developing a national cybersecurity skills strategy in each partner country, organising a European Cybersecurity Hackathon to foster innovation, establishing twinnings between Cybersecurity Skills Hubs, and promoting collaboration between education and industry sectors. The project will benefit a wide range of stakeholders including industry players, learning providers, youth, students, NEETs, and professionals, policymakers, and public organisations, NGOs, CSOs, and other social partners who will get access to a variety of cybersecurity resources raising awareness and building their capacity, as well as learning and job opportunities.

Expected results of the project include the establishment of a sustainable European Network of Cybersecurity Skills Hubs, the development of national cybersecurity skills strategies, the creation of innovative cybersecurity solutions through the Hackathon, the establishment of long-term partnerships and collaboration with the wider cybersecurity ecosystem, and the dissemination of project results through various communication channels.

Overall, the CyberHubs project will play a significant role in strengthening the cybersecurity workforce in Europe and promoting the digital transformation of the industry.

#\$PRJ-SUM-PS\$# #@REL-EVA-RE@# #@PRJ-OBJ-PO@#

**1. RELEVANCE****1.1 Background and general objectives****Background and general objectives**

Please address all guiding points presented in the Call document/Programme Guide under the award criterion 'Relevance'.

Describe the background and rationale of the project.

How is the project relevant to the scope of the call? How does the project address the general objectives of the call? What is the project's contribution to the priorities of the call (if applicable)?

**1.1.1. Background and rationale of the project**

Digital skills shortages are hampering the growth and competitiveness of companies across Europe. In 2020, more than half of European enterprises that recruited (or tried to recruit) ICT specialists had difficulties filling their vacancies (DESI 2022) and the situation was particularly acute when it came to advanced digital skills required for specialist ICT positions related to cybersecurity.

Studies across the globe show that the cybersecurity professional skills gap continues to grow while cyber threats and attacks are on the rise. In this context, cybersecurity is not only important to ensure the EU market's competitiveness and the well-being of its enterprises but essential to improve Europe's digital resilience and support its workforce in transition. Addressing the need for cybersecurity skills and professionals in Europe is therefore a top priority which can be achieved by fostering and consolidating strategic collaboration between higher education, vocational education and training, and industry.

The European Network of Cybersecurity Skills Hubs (CyberHubs) project's rationale is based on the fact that the demand for cybersecurity professionals is rapidly increasing. This shortage is driven by a range of factors, including the increasing number and sophistication of cybersecurity threats, the growing importance of data privacy and security, and the rise of new technologies such as the Internet of Things, Cloud Computing, and Data Spaces.

The CyberHubs project aims to address the cybersecurity skills needs in Europe by uncovering the critical cybersecurity skills mismatches, providing tailored-made approaches on how to bridge the gap (now and in the future) across the EU

Member States, raising awareness and understanding of cybersecurity, connecting relevant actors at the national and EU level to share knowledge, skills, and good practices, strengthening close cooperation between the vocational education and training, higher education, and enterprises, and delivering a set of concrete actions to boost the attractiveness of cybersecurity job and learning opportunities and talent retention while fostering innovation.

In recent years, the European Union has acknowledged the need to adopt a whole-of-society approach to tackling the digital skills mismatches and shortages of skilled professionals — especially in key areas such as cybersecurity. The [Digital Decade Communication](#) recognises that the empowerment of Europe's enterprises and citizens, together with maintaining the security and resilience of its digital supply chains, are the cornerstones of the European Union's path to a digitally transformed economy and society. Moreover, the European Commission has proposed a [Digital Compass](#), one of the cardinal points being digital skills and education. This has set the target of 20 million employed ICT specialist in the EU by 2023. At the Member State level, there are several policies and initiatives related to digital skills and cybersecurity, including those of the [Recovery and Resilience Plans](#), that are aligned to this project such as the [Digital Innovation Hubs](#) and the [national coalitions for Digital Skills and Jobs](#) that are supported at the European level.

The CyberHubs project aims to build stronger links between education, business, and research at both the local and European level. The European network fosters the setting up of incubators (a.k.a. "CyberHubs") within 7 pilots in Belgium, Spain, Slovenia, Hungary, Greece, Lithuania, and Estonia with the clear objective to improve the quality and relevance of cybersecurity professional skills developed and certified through education and training systems. It facilitates the flow and co-creation of knowledge, information, and good practices as well as enhances cooperation in cybersecurity skills development and management with key stakeholders and related projects and initiatives. The project will also count on the support and expert knowledge of two national cybersecurity champion partners — the French Campus Cyber (Numeum) and Cyber Ireland (MTU).

At the proposal stage, each of the CyberHubs is composed of one National Trade Association (leading ICT business association) and at least one education and training partner with longstanding expertise in cybersecurity. These CyberHubs will then extend their ecosystem and reach to both public and private sector actors, over the course of the project. In this light, the CyberHubs project brings a clear response to the need of strengthening collaboration between higher education, research and business to tackle future skills mismatches and promote excellence in skills development, ensuring higher education institutions are connected and contribute to innovation — as highlighted in the [renewed EU agenda for higher education](#).

In the European context, traditional approaches to cybersecurity education and training have been criticised for being too theoretical and disconnected from the real-world challenges faced by organisations. This has led to a mismatch between the skills that cybersecurity professionals possess and the skills that are needed in the market. There are different projects looking at addressing these mismatches, for example, the Erasmus+ Blueprint Sector Skills Alliance REWIRE. It is important to note that the CyberHubs project seeks to complementarily address these challenges by developing a more practical and collaborative approach to cybersecurity skills management and development, but also by adopting an innovative and targeted, yet comparable, approach to tackling the skills mismatches in the countries represented by the CyberHubs.

### 1.1.2. Relevance of the project according to the scope of the call

The EU's Erasmus+ Programme's (2021-2027) "Alliances for Innovation" call aims to boost innovation through cooperation and flow of knowledge among higher education, vocational education and training, and the broader socio-economic environment, including research. The CyberHubs project brings an adequate response by the fact that it brings together higher education, vocational education and training, and business representatives to develop an innovative approach to tackling the skills mismatches in the 7 countries represented by the CyberHubs, while addressing the quality and relevance of cybersecurity education and training and fostering knowledge transfer at the European level via specific activities such as the country delegation visits to champion partners, and the twinning programme. These combined actions will be informed by solid market research on cybersecurity professional skills and roles current demand and supply, as input to national cybersecurity capacity building strategies developed together in the first project phase.

The CyberHubs project will implement a coherent and comprehensive set of cross-sectoral activities focusing on awareness raising, capacity building, and stakeholder engagement to boost cybersecurity skills development and management, foster EU citizen's entrepreneurial mindset, and overall enhance the EU's capacity in cybersecurity and digital resilience. More importantly, the CyberHubs will support cybersecurity skills development and talents by ensuring efficient skills matches with cybersecurity job and learning opportunities through the cutting-edge Skills Academy Platform provided by EIT Digital. The CyberHub activities will be closely aligned with EU-level recent progress and action in the cybersecurity skills development field; in particular the European Cybersecurity Skills Framework (ECSF) used as common reference point for cybersecurity professional skills and competences.

### 1.1.3. Alignment with the call objectives

- **Project vision:** The CyberHubs project envisions a future where Europe has a thriving cybersecurity workforce, equipped with the relevant skills and knowledge to tackle emerging threats, and protect digital systems and data. By bringing together higher education, vocational education and training, and business,



CyberHubs aims to create a well-coordinated, long-lasting, and sustainable ecosystem for cybersecurity skills development and innovation capable to answer the needs of the market — now and in the future.

- **Project mission:** The CyberHubs' mission is to address Europe's cybersecurity skills needs by developing an efficient, collaborative European network of multi-stakeholder cybersecurity skills incubators ("CyberHubs") in 7 pilot countries to support the skills development, promote innovation, and facilitate the matching of skills with job and learning opportunities in the cybersecurity field.

#### 1.1.4. How the project addresses the general objectives of the call

The CyberHubs project aims to address four objectives of the call, as follows:

- **Objective 1:** *Facilitating the flow and co-creation of knowledge between higher education and vocational education and training, research, the public sector and the business sector.*

The CyberHubs project will enable the flow and co-creation of knowledge between higher education, vocational education and training, and business in 7 European Member States (Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia and Spain) by establishing reliable and sustainable relationships under the umbrella of the hubs, and with the ultimate goal of strengthening the cybersecurity ecosystem at the national levels and in Europe. In each CyberHub, at least one higher education institution with large expertise in cybersecurity professional training and one national trade association of the ICT sector representing the labour market players will join forces.

- **Objective 2:** *Fostering the setting up of incubators within education and training institutions across Europe.*

The European network of Cybersecurity Skills Hubs fosters the setting up of incubators (a.k.a. "CyberHubs") within 7 pilot initiatives in Belgium, Spain, Slovenia, Hungary, Greece, Lithuania, and Estonia. The 7 national CyberHubs will propose strategies and actions/services for the alignment between current European labour market skills needs and the education and training offering in cybersecurity. During the project, the CyberHubs will expand and recruit/integrate key stakeholders from cybersecurity field in the country.

- **Objective 3:** *Improving the quality and relevance of skills developed and certified through education and training systems (including new skills and tackling skills mismatches).*

The CyberHubs project will conduct extensive market research on cybersecurity professional skills and roles demand and supply in Europe. The results of the country-specific skills mismatches analysis will inform the development of the strategies that will be considered for immediate follow-up actions by the CyberHubs with contribution from higher education, vocational education and training, and business, as well as the extended ecosystem of each Hub. An agile cybersecurity skills forecasting model, based on solid methodology, will be developed and specific elements tested in order to ensure continued implementation by the CyberHubs partners — and the society at large — in the short, medium, and longer term.

- **Objective 4:** *Supporting skills development in the deep tech domains; supporting Europe's innovation capacity by broadening its talent pool in these new, disruptive technologies.*

The CyberHubs project aims to support skills development in a crucial area embedded across all deep tech domains: cybersecurity. The project will make a key contribution to ensure the provision of education and training opportunities required by the market for cybersecurity professional skilling, upskilling, and reskilling. The CyberHubs project will address this by identifying existing innovative education and training programmes and mapping and matching them to the latest market needs. This exercise will allow CyberHubs to produce a detailed gap analysis and action-oriented national strategy and action plan for immediate uptake in the 7 piloting countries. Additionally, the CyberHubs will support cybersecurity skills development and talents by ensuring efficient skills matches with cybersecurity job and learning opportunities through the cutting-edge Skills Academy Platform provided by EIT Digital.

## 1.2 Needs analysis and specific objectives

### Needs analysis and specific objectives

Please address the specific conditions/objectives set out in the Call document/ Programme Guide, if applicable.

Describe how the objectives of the project are based on a sound needs analysis in line with the specific objectives of the call. What issue/challenge/gap does the project aim to address?

The objectives should be clear, measurable, realistic and achievable within the duration of the project. For each objective, define appropriate indicators for measuring achievement (including a unit of measurement, baseline value and target value).

#### 1.2.1. Needs analysis according to the specific objectives of the call

Cyberattacks are at record levels and projected to continue to increase over the coming years, according to European Union Agency for Cybersecurity (ENISA). It has become urgent for Europe to increase cybersecurity requirements in

European legislations and begin to solve the cybersecurity professional skills gap — which continues to grow exponentially over the coming years. Cybersecurity threats pose a significant risk to digital resilience and innovation for governments, businesses, and individuals. These cybersecurity challenges are exacerbated by a lack of relevant and student-centred education and training opportunities for young people and adults, and workforce shortages.

Last year, the EU's cybersecurity workforce needs were estimated at 883,000 professionals while the shortage of cybersecurity professionals was already ranging between 260,000 and 500,000. With the sophistication and rise of cybersecurity threats and attacks, Europe needs a well-coordinated, sustainable, and innovative approach to address these challenges, bringing together higher education, research, vocational education and training, and enterprises while considering both Member State and European perspectives.

Cybersecurity professionals are among the most critical roles to be filled in the European ICT sector. In 2021, about 9 million people worked as ICT professionals in the EU. The highest numbers were reported in Germany (2 million ICT specialists), France (1.2 million) and Italy (0.8 million). At the current pace, it will be difficult to reach the 2030 Digital Compass target of 20 million ICT specialists by 2030 — especially in key areas such as cybersecurity.

Filling open ICT specialist vacancies is difficult, with 55% of companies reporting having issues (DESI 2022). People do not have with the technical and managerial cybersecurity skills needed to fill open jobs, and those who have cybersecurity skills lack the management expertise to allow businesses to achieve a high maturity level and create proactive preventative strategies around cybersecurity.

The 2021 [World Economic Forum's \(WEF\) Global Risks Report](#) listed cyberattacks on global Critical Infrastructure (CI) as a top concern. WEF noted that "attacks on critical infrastructure have become the new normal across sectors such as energy, healthcare, and transportation." That global risk was exemplified in the Russian invasion of Ukraine which set a new stage for the use of cybersecurity weapons aimed at disabling critical infrastructure. The Cybersecurity skills shortage is a global problem. There will be 3.5 million job vacancies by 2025 representing a 350% increase over an eight-year period, according to Cybersecurity Ventures in an article released on November 2021. Microsoft have created a Power BI report in 2021 to shed light on the cybersecurity skills gap in some European countries, using LinkedIn data. The data shows that the demand for cybersecurity skills has grown by an average of 22% over 2021 alone in many European markets, at least 60,000 additional cybersecurity professionals were needed to meet the demand between 2022 and 2023 and much more demand will be needed in the coming years. In cybersecurity professionals, the workforce gap remains the number-one barrier to meeting their organisations' security needs. Sixty percent of respondents report that a cybersecurity staffing shortage is placing their organisations at risk. The consequences of cybersecurity staff shortages are real and create challenges for organisational success.

In conclusion, EU policy initiatives and that latest market research data demonstrate the urgent need to increase the number of Cybersecurity experts in the EU, particularly among SMEs and smaller companies.

### 1.2.2. Challenges and gaps that the CyberHubs project is addressing

The CyberHubs project consortium will join forces to address several major challenges and gaps related to the continuously increasing cybersecurity professional skills shortage in Europe. These are identified as follows:

**Shortage of cybersecurity professionals.** The shortage of cybersecurity professionals in Europe is estimated to be ranging between 260,000 and 500,000. The European network of CyberHubs will practically contribute to facilitating and nurturing a growth in the number of skilled cybersecurity professionals across countries, and increasing overall awareness about the attractiveness of the cybersecurity professional field, which is not only about technology.

**Lack of relevant education and training.** There is a lack of relevant education and training programmes that can equip individuals with the necessary cybersecurity professional skills. The project consortium will address this by developing comprehensive cybersecurity skills mismatches analysis including mapping existing innovative education and training programmes to the latest market needs identified, making use of the recently launched ENISA European Cybersecurity Skills Framework (ECSF) producing cybersecurity skills strategies and action-oriented plan for immediate take-up by the 7 CyberHubs.

**Lack of collaboration between academia and industry.** There is a gap between academia and industry in terms of cybersecurity skills development. The project aims to address this by fostering collaboration between academia and industry through the CyberHubs, and by developing joint relevant initiatives focused on knowledge transfer, awareness raising and short and efficient strategic capacity building.

**Limited access to training and education.** Access to cybersecurity training and education is limited, particularly in certain geographic areas and among underrepresented groups. The project aims to address this by analysing the skills mismatches and leverage the AI-assisted Skills Academy Platform to match skills to job and learning opportunities in the cybersecurity field.

**Rapidly evolving cybersecurity threats.** Cyber-threats are increasing and threaten all industry sectors. The cybersecurity threat landscape is constantly evolving, which requires cybersecurity professionals to continuously update their skills and knowledge. The project aims to address this by developing awareness raising and capacity building activities that can quickly adapt to the changes of the landscape.

As overall approach, the CyberHubs project seeks to address these challenges and gaps by fostering collaboration between higher education, vocational education and training, and enterprises, as well as other key stakeholders in the value chain of cybersecurity skills.

### 1.2.3. How the project is addressing digital, green, and resilience skills

The CyberHubs project will be making contributions to the development of skills in the following ways:

**Digital skills.** The project aims to create a network of Cybersecurity Skills Hubs. The development and maintenance of these Hubs will require digital skills in areas such as cybersecurity, data analysis, and software development. As such, the project may indirectly contribute to the development of digital skills in these areas. Moreover, in the context of awareness raising and capacity building activities related to cybersecurity skills, the project may also contribute to the development of digital skills.

**Green skills.** The project may contribute to the development of green skills by promoting the adoption of sustainable practices in the cybersecurity industry. For instance, the project may encourage the use of renewable energy sources, the reduction of energy consumption, and the proper disposal of electronic waste. It is also to be noted that professionals, especially in the ICT industry, tend to require skills that are more horizontal (e.g., soft skills and profession-related skills), in complementary to the technical skills in a specific field. Green skills can be understood as both digital skills and transversal skills. The project will uncover the need for these horizontal skills in cybersecurity professionals when conducting the in-depth cybersecurity skills mismatches analysis.

**Resilience skills.** The project may indirectly contribute to the development of resilience skills by promoting collaboration and partnership between different stakeholders, including industry players, learning providers, public organisations, and policymakers. By fostering a collaborative approach, the project may encourage the development of skills related to adaptability, change management, and community building.

### 1.2.4. CyberHubs project's specific objectives

The clear, measurable, realistic, and achievable specific objectives (SO) of the CyberHubs project within the duration of the project are the following ones:

- The baseline value refers to the minimum requirements to be achieved by the project.
- The target value refers to the most optimistic value to be reached by project activities.

**SO1: to create a long-term, sustainable partnership of key European stakeholders within the cybersecurity sector who will cooperate to develop and implement new strategic approach to address the cybersecurity skills mismatches.**

Unit of measurement	Baseline value	Target value
No. transnational project meetings (online and in-person)	36 (1 per month)	36 (1 per month)
No. associated partners active in the project	3	10
No. successful links to other relevant projects and initiatives at the national and EU level	5	7

**SO2: to improve the quality and relevance of cybersecurity education and training programmes through the identification of country-specific cybersecurity skills mismatches and providing innovative skills need anticipation methodology (market/educational offering) in Belgium, Estonia, Slovenia, Hungary, Greece, Lithuania, and Spain.**

Unit of measurement	Baseline value	Target value
No. relevant education and training offerings on cybersecurity across the 7 countries collected	140 (20 per hub)	280 (40 per hub)
No. expert participants in the expert focus groups	35 (5 per hub)	70 (10 per hub)
No. survey respondents	210 (30 per hub)	350 (50 per hub)
No. job vacancies analysed	350 (50 per hub)	700 (100 per hub)
No. articles and publications on cybersecurity skills reviewed during the data analysis	20	30

**SO3: to foster the development of national cybersecurity skills incubators (i.e., the "CyberHubs") across the EU, promoting cybersecurity skills development, innovation, and entrepreneurship.**

Unit of measurement	Baseline value	Target value
No. national CyberHubs established during the project lifetime	7	7

No. national CyberHub candidates to join the European Network of Cybersecurity Skills Hubs	2	5
No. country-specific cybersecurity skills strategies delivered	7	7
No. capacity-building, awareness raising, stakeholder engagement activities conducted across the 7 CyberHubs during the project lifetime	70	80
<b>SO4: to facilitate knowledge transfer, the exchange of good practices and information between higher education institutions, vocational education and training, and the business sector in the field of cybersecurity.</b>		
Unit of measurement	Baseline value	Target value
No. organisations from the business and education and training sectors represented across the 7 CyberHubs ecosystems	300	450
No. transferable good practices identified	7	14
No. country delegation visits organised to champion partners	7	7
No. participants in the CyberHubs quarterly meetings across the 7 CyberHubs	35	70
No. student involved in the validation of the CyberHubs action plans	14	35
No. twinnings completed	7	7
No. education-industry joint activities conducted during the project lifetime	35	50
<b>SO5: to increase the number of cybersecurity professionals in Europe by matching skills supply and jobs demand, engaging key players at the national and EU level, and attracting and retaining more talents in the cybersecurity field in Europe.</b>		
Unit of measurement	Baseline value	Target value
No. participants in capacity-building, awareness raising, stakeholder engagement activities across the 7 CyberHubs	700	1,700
No. individuals using the Skills Academy Platform (SAP) to match jobs and skills across the 7 CyberHubs	120	140
No. matches realised via the SAP	240	310
No. new cybersecurity education and training programmes referenced on the SAP	80	100
<b>SO6: to promote an entrepreneurial mindset as well as diversity and inclusion in the field of cybersecurity by engaging youth and addressing underrepresented groups in the ICT industry in Europe.</b>		
Unit of measurement	Baseline value	Target value
No. participants in the European Cybersecurity Hackathon	30	50
No. challenges at the European Cybersecurity Hackathon	3	5
No. solutions hacked at the European Cybersecurity Hackathon	9	15
No. individuals from underrepresented groups reached via the project activities	100	300
<b>SO7: to increase awareness and understanding of cybersecurity threats and good practices for cybersecurity resilience among the general public.</b>		
Unit of measurement	Baseline value	Target value
No. individuals reached through the cybersecurity awareness raising campaigns conducted during the project lifetime	1,000	3,500

No. participants in the European Cybersecurity Fest	150	200
No. participants across the 7 CyberHubs national conferences	350	490

#@COM-PLE-CP@#

### 1.3 Complementarity with other actions and innovation — European added value

#### Complementarity with other actions and innovation

*Explain how the project builds on the results of past activities carried out in the field, and describe its innovative aspects (if any).*

*Explain how the activities are complementary to other activities carried out by other organisations (if applicable). Illustrate the trans-national dimension of the project; its impact/interest in the EU area; possibility to use the results in other countries, potential to develop /cross-border cooperation among Programme countries and Partner countries, if applicable, etc.*

*If your proposal is based on the results of one or more previous or ongoing projects, please provide precise references to these projects.*

#### 1.3.1. How the project builds on the results of past activities

The project on CyberHubs is proposed by a powerful consortium with considerable track of work which directly connects with and/or builds on activities of relevance to the cybersecurity education and training field. One of the main challenges in the field has been the shortage of qualified cybersecurity professionals, which has led to a skills gap that threatens the security of our digital infrastructure. In response, a number of initiatives have been launched to address this issue.

The European Cybersecurity Skills Framework, published by ENISA in September 2022, together with other complementary European frameworks and structures of relevance to the domain, will be used by the CyberHubs consortium as a key enabler to consistently integrate, inner-connect and/or build upon past and ongoing activities with the goal of improving the skills of cybersecurity professionals and increase the number of qualified workers in the field.

Another initiative of key relevance is the Cybersecurity Competence Centres, which were launched under the EU's Horizon 2020 research and innovation program. These centres bring together researchers, industry and government partners to collaborate on cybersecurity research and development, with the aim of improving the security of our digital infrastructure.

In recent years, there have been several initiatives aimed at addressing this issue. These include the creation of cybersecurity programs at universities and vocational schools, as well as the development of certification programs for cybersecurity professionals. However, these initiatives have not been able to keep up with the demand for skilled cybersecurity professionals, and many organizations still struggle to find qualified candidates for cybersecurity roles. The CyberHubs project builds on these past initiatives, and it aims to establish a network of CyberHubs across Europe, each of which will offer a range of skills related services tailored to the needs of the local community.

The CyberHubs project builds on past initiatives in the field of cybersecurity education and training, while also introducing new and innovative approaches to address the skills gap by fostering collaboration and knowledge sharing between higher education, VET training providers and the industry.

#### 1.3.2. Innovative aspects of the project

The CyberHubs project is innovative in several ways. First, it takes a decentralised approach to cybersecurity education and training. Instead of relying on traditional education and training models, the project seeks to leverage existing resources and expertise within local communities to provide cybersecurity education and training related services.

Second, the project is focused on developing a flexible and adaptable model for cybersecurity capacity building processes. This includes using a range of delivery methods, such, workshops, and mentoring programs, study visits, twinnings, hackathons, etc., to meet the needs of learners with different backgrounds and skill levels.

Third, the consortium will make maximised use of EU-level frameworks and tools to harmonise common understanding of cybersecurity professional skills needs, supply, identifying mismatches and further related challenges, in order to reach harmonised view on most recent insights and forthcoming findings of this partnership, their complementary activities outside the consortium and further reach the project will have. The recently published European Cybersecurity Skills Framework (ECSF) will play a major role in this regard.

The CyberHubs project provides an innovative approach to addressing the shortage of skilled cybersecurity professionals in the short, medium and longer term. By leveraging existing resources and expertise within local communities and developing a flexible and adaptable model for cybersecurity education and training, the project has the potential to make a significant impact in the field of cybersecurity skills.

#### 1.3.3. Complementary to other activities carried out by other organisations



The activities of the CyberHubs project are complementary to other activities carried out by other organizations in the field of cybersecurity education and training.

The project seeks to act complementary and contribute best possible to the activities of ENISA, the European Agency for Cybersecurity, which is dedicated to achieving a high common level of cybersecurity across Europe. ENISA provides guidance on the implementation of the NIS Directive, and the CyberHubs project can help to address the serious skills shortages on the European labour market ENISA is outlining on regular basis in its reports. The recently launched ECSF will play a key role in implementing the CyberHubs activities, and contributions to the Cyber Higher Education Database (CyberHEAD) will be made by the universities involved in the project.

Furthermore, the CyberHubs project is complementary to the activities of the European Cybersecurity Organization (ECSO), which is a public-private partnership that aims to develop the cybersecurity ecosystem in Europe. ECSO focuses on promoting innovation and cooperation between cybersecurity stakeholders, and the CyberHubs project can contribute to this goal by providing training and education opportunities for cybersecurity professionals.

Moreover, the Cybersecurity Competence Centre (C4Cyber) is a European-wide initiative that brings together experts from academia, industry, and government to advance cybersecurity research and innovation. The CyberHubs project can collaborate with C4Cyber by providing development opportunities for cybersecurity professionals and researchers.

In addition, the project is complementary to the activities of universities and other educational institutions that offer cybersecurity courses and programs. The project can provide a platform for sharing best practices and resources among these institutions and can help to address the practical skills gap that is often identified in traditional academic cybersecurity programs.

The CyberHubs project is designed to complement and enhance existing activities in the field of cybersecurity education and training, and to provide additional resources and opportunities for cybersecurity stakeholders in the 7 piloting countries: Belgium, Slovenia, Lithuania, Estonia, Hungary, Greece, and Spain.

#### **1.3.4. Transnational dimension of the project**

The CyberHubs project has a strong transnational dimension. While the project is creating seven national virtual hubs in Belgium, Slovenia, Lithuania, Estonia, Hungary, Greece, and Spain. These hubs will also be interconnected to form a pan-European network of cybersecurity skills hubs (CyberHubs) and will receive orientation from the European Champions: Campus Cyber in France and Cyber Ireland.

The project's transnational dimension is important because it allows for the sharing of knowledge, best practices, and experiences across different national contexts, which can lead to the development of more effective and efficient solutions to the cybersecurity skills gap challenge. The project's transnational partnerships also enable the creation of a pan-European network of cybersecurity professionals, education and training providers, and other relevant stakeholders, which can help to foster greater collaboration and cooperation in this field. These informal networks and networking activities will be coordinated with other similar initiatives fostered by the EC or other relevant projects.

The project's transnational dimension also ensures that the future experts will have homogeneous capacity and the solutions developed are tailored to the needs of the entire EU area, rather than just one country, and that they take into account the specific challenges and opportunities of each national context. This can help to ensure that the project's impact is maximised and that the solutions developed are relevant and useful across the entire EU area.

Furthermore, the project includes transnational awareness raising and knowledge transference activities. These activities will provide opportunities for individuals and organizations from different countries to collaborate and exchange knowledge and experience, further enhancing the transnational dimension of the project.

#### **1.3.5. Impact of the project in the EU area**

The CyberHubs project has the potential to have a significant impact on the EU area by addressing the urgent need for more skilled cybersecurity professionals. The project aims to contribute to the EU's path to a digitally transformed economy and society, as well as the achievement of the Digital Europe Programme's ambitious goals for strengthening the quality of EU educational and training institutions in digital fields, specifically in cybersecurity.

By addressing the cybersecurity skills gap in the EU, the project can help increase the number of skilled cybersecurity professionals and reduce the risk of cyberattacks on critical infrastructure. This can enhance the overall cybersecurity posture of the EU, which is crucial for maintaining the security and resilience of its digital supply chains and protecting the enterprises and citizens within its borders.

Moreover, the project's emphasis on fostering collaboration between academic institutions and enterprises can facilitate the flow and co-creation of knowledge, which is vital for promoting innovation in the field of cybersecurity. This can help the EU remain competitive in the global market and attract more investments and opportunities in the field of cybersecurity.

Finally, the project's emphasis on supporting skills development in the deep tech domains can help broaden Europe's talent pool in new, disruptive technologies, which can have a positive impact on the EU's innovation capacity and overall economic growth.

**1.3.6. Possibility to use the results in other countries**

Considering that the project is working towards developing specific national cybersecurity skills strategies. These strategies could serve as a model for other countries facing similar challenges and looking to improve their cybersecurity skills capacity. The project will make these seven national cybersecurity skills strategies public to foster their benchmarking in other countries.

The project's focus on collaboration and knowledge sharing among partner countries and stakeholders can also help promote a culture of cybersecurity awareness and best practices across the EU. By working together and sharing experiences and resources, the project can contribute to building a more robust and resilient cybersecurity workforce and ultimately improve the overall cybersecurity posture of the EU.

Furthermore, the project's approach of establishing virtual CyberHubs could potentially serve as a model for other countries or regions looking to build their own cybersecurity skills capacity. The virtual nature of the hubs allows for greater flexibility and scalability, which can be particularly useful for countries with limited resources or facing other constraints.

The project's impact can be significant not only in the pilot countries but also in promoting best practices and capacity building across the EU and potentially beyond.

**1.3.7. How CyberHubs builds on the results of one or more previous or ongoing projects**

The Cybersecurity Skills Hubs project builds on the results of several previous and ongoing projects that address the need for improving the cybersecurity skills gap in Europe. As the number of projects is enormous, the table below is considering only the projects where the CyberHubs partners are participating and the connection with the project is more feasible:

Project information and partners involved	Brief description of the project	How can the CyberHubs project connect to this project
Digital Europe Programme. <b>Data Space for Skills</b> (101083483) Partners involved: <b>DE</b> , CCIS, Adecco	The Data Space for Skills (DS4Skills) project is a preparatory action led by DIGITALEUROPE that aims to identify and develop a European Data Space of Skills (EDSS)f. The project focuses on developing a common framework for data sharing and interoperability in the field of skills development.	The CyberHubs project can connect to DS4Skills in several ways. First, the national cybersecurity skills strategies developed in the pilot countries could be integrated into the European Data Space for Skills (EDSS) to promote the development of cybersecurity skills across Europe. Second, the EDSS could serve as a platform for promoting the forecasting of skills and jobs. In fact, the idea of piloting it comes from the DS4Skills project.
Erasmus+. <b>ESSA</b> (562364-EPP-1-2015-1-IT-EPPKA2-SSA) Partners involved: <b>DE</b> , CCIS, Adecco, Formazione, IVSZ, Breyer Publico SLU,	ESSA (European Software Skills Alliance) is a project, led by DE, that aims to tackle the skills gap in the software services sector by bringing together stakeholders from industry, education, and policymaking to create a European skills agenda for the sector. The project focuses on identifying the skills and competencies needed for the software services industry, and developing solutions to address the skills gap, including creating new training programs and certifications.	The CyberHubs project can bring significant benefit to ESSA by sharing in-depth professional expertise on cybersecurity skills and knowledge needs that are of particular relevance in the software domain related ICT professional roles ("acting on the source"). The CyberHubs project can provide insights into the specific cybersecurity skills needed in the software professional workplace, and ESSA can use this information to develop and implement the most suitable training programmes.
Erasmus+. <b>ARISA</b> (101056236) Partners involved: <b>DE</b> , CCIS, IVSZ, UNIR, Breyer Publico SLU, Adecco	The ARISA (Artificial Intelligence Sector Skills Alliance) project, led by DE, aims to build a European AI talent pipeline and boost AI adoption across all sectors. The project will create a framework for AI skills, develop learning materials, and create new qualifications to support the development of AI talent across Europe.	The CyberHubs project can connect to ARISA in several ways. First, cybersecurity is a critical component of trustful and robust AI development and use, and the AI related cybersecurity skills identified by the CyberHubs project could be integrated into the ARISA framework. Second, the development of a strong cybersecurity talent pipeline is essential for the adoption of AI technologies in a secure and

		responsible manner, which is a key goal of ARISA.
DigitalEurope Programme. <b>EDIH – WalHub</b> (101083685)  Partners involved: AGORIA	WalHub is a European Digital Innovation Hub – EDIH based in Wallonia (Belgium) to support manufacturing companies in their digital transformation. WalHub aims to boost the digital transformation of manufacturing companies and the adoption of key technologies, such as AI, HPC, Cybersecurity and IoT in their industrial and supply chain processes.	Both projects have a common goal of supporting the digital transformation of companies, and as such, there may be opportunities for collaboration or knowledge sharing between the two initiatives. For example, the CyberHubs project could potentially provide expertise or training on cybersecurity to manufacturing companies working with WalHub.
INNOVIRIS. <b>SECLOUD</b>  Partners involved: ULB	Cloud security in partnership with 10 other faculties from various universities in Brussels.	Thanks to this project, we have connections with most academics and researchers in cybersecurity in Belgium.
Digital Europe Programme. <b>EDIH - DIGITALIS</b>  Partners involved: HOWEST	DIGITALIS is the European Digital Innovation Hub (EDIH) focusing on supporting the digital transformation of manufacturing SMEs. Financed by the European Commission, a group of experts from business, academia and industry guide the manufacturing into the 21st century. (Cybersecurity , AI , Blockchain , 5G , Photonics , IoT/Edge/Cloud and AR/VR). Services : Skills and training , Test before invest , Access to finance and Get Connected.	The cybersecurity in-depth professional focus of the CyberHub joined initiative can provide valuable insight to EDIH on the most critical factors for cybersecure manufacturing SME's. In turn, practical experience and know-how can flow from EDIH to CyberHub, e.g. on main cybersecurity related challenges faced by manufacturing SMEs in the digital transformation, and synergies identified and created together.
LIVING LAB Industry 4.0 (Vlaio Flanders). <b>LIVING LAB INNOVATIVE CYBRSECURITY FOR INDUSTRY &amp; LOGISTICS 4.0</b>  Partners involved: HOWEST	In the Living Lab Innovative Cybersecurity for Industry and Logistics 4.0, additional innovations in cybersecurity can be further demonstrated, which can be inspiring for other companies and organisations, and can enthuse additional companies to set up cases within their own context. We will also discuss the existing and future regulations concerning network and information systems.	The CyberHubs project can collaborate with the Living Lab project to exchange knowledge and expertise on cybersecurity practices and technologies, as well as identify innovative solutions and approaches that can be implemented in the industry and logistics sectors.
Horizon 2020. <b>INFIMO</b> (EIE-2022-CONNECT-01)  Partners involved: ITL	The project focuses on building an interconnected and inclusive innovation ecosystem linking primarily ICT-related initiatives and networks in three countries (Estonia, Georgia, Spain/Portugal), focused on exploring the ways of how to speed up the circular economy movement and pursue the goals of European Green Deal via ICT and industry 5.0 developments, supporting the twin transition.	In the CyberHubs project, we can leverage the experience gained from INFIMO project, especially on how to best build networks, link relevant initiatives in the participating countries, as well as adopt best practices of acting as a driving force in the topic of cybersecurity skills and competencies to engage stakeholders, raise awareness and make acquiring cybersecurity skills more desirable, as well as accessible.
ERDF. <b>Estonian ICT Cluster Project</b>  Partners involved: ITL	ICT cluster is a collaboration platform for enterprises, created to boost the innovation and foster cluster companies export to the international market. The focus fields of the cluster are smart mobility and logistics, e-governance, and industry digitalisation.	The CyberHubs project can build on the extensive experience and know-how of building a well-functioning collaboration network and a hub with enterprises, stakeholders, academics, education, and training providers in the field of cybersecurity.



<p><b>Raising the security awareness of young people to cope in the information society</b> (Noorte turvateadlikkuse tõstmine infoühiskonnas toimetulekuks)</p> <p>Partners involved: ITL</p>	<p>The main goal of the project was to raise the awareness of young people and people who work with them for orientation in the information society and security-conscious behaviour. The specific objectives were: - conducting conferences on Internet security for people working with young people in 6 regions of Estonia. - preparing instructional materials in both Estonian and Russian for teachers and youth workers to support and guide young people in preventing the misuse of computers and the Internet.</p>	<p>ITL has been participating in the mapping of cybersecurity skills and consecutive awareness raising in collaboration with companies as well as public sector and training/education providers among different target groups for many years now. Therefore, we have a good existing network to start building on, constantly developing overview of the main necessities as well as experience in which approaches tend to work the best to awareness raising.</p>
<p>Horizon 2020. <b>ECHO</b> (H2020-SU-ICT-2018-2)</p> <p>Partners involved: TalTech</p>	<p>ECHO delivers an organized and coordinated approach to improve proactive cybersecurity defence of the European Union, through effective and efficient multi-sector collaboration. The Central Competence Hub serves as the focal point for the ECHO Multi-sector Assessment Framework enabling multi-sector dependencies management, provision of an ECHO Early Warning .</p>	<p>The CyberHubs project can build on the ECHO project and take advantage of the good base of needs analysis about training possibilities for ICT specialists and SMEs.</p>
<p>DIGITAL-2021-SKILLS-01 Programme. <b>CyberSecPro</b> (101083594)</p> <p>Partners involved: TalTech</p>	<p>EU Higher Education Institutions (HEIs) have more than 128 cybersecurity academic programs (undergraduate and graduate) as identified by ENISA (CyberHEAD), JRC (ATLAS) and a variety of reports by the 4 pilot projects (Sparta, CyberSec4Europe, ECHO, CONCORDIA). These academic programs, with their static curricula, do not provide the dynamic capabilities and emerging skills needed in the market. The digital transformation imposes the HEIs to enhance their role in preparing the new generation workforce and to upskill the existing one in meeting the challenging and ever-growing cybersecurity challenges (e.g., massive AI attacks).</p>	<p>The CyberHubs project can potentially connect to the CyberSecPro project by leveraging their experience and knowledge in developing practical and hands-on cybersecurity training programs.</p> <p>Through this collaboration, the CyberHubs project can benefit from the practical and innovative approach of the CyberSecPro project, while the CyberSecPro project can expand its reach and impact through the national CyberHubs.</p>
<p>Horizon 2020. <b>CHESS</b> (101087529)</p> <p>Partners involved: TalTech</p>	<p>The proposed Cybersecurity Excellence Hub in Estonia and South Moravia (CHESS) will integrate leading cybersecurity institutions and capitalize on the strengths of both regions to address important Europe-wide challenges. South Moravia is a major ICT industry &amp; education powerhouse of the Czech Republic, with a very focused and coherent smart specialization strategy targeting cybersecurity.</p>	<p>The CyberHubs project can connect to the CHESS project by collaborating and sharing knowledge, resources, and best practices to promote cybersecurity excellence and skills-building in Europe.</p>
<p>Interreg Europe. <b>CYBERSECURITY</b></p> <p>Partners involved: CCIS</p>	<p>Interreg Europe CYBERSECURITY – for the strong European Cybersecurity Smart Regions. Interreg Europe CYBERSECURITY aims to boost the competitiveness of the European cybersecurity SMEs by creating</p>	<p>First, the outputs like local cybersecurity strategies could be shared across both projects to promote the development of cybersecurity skills across Europe, especially for SMEs. Second, both projects could serve as a platform for sharing best</p>

	synergies among European Cybersecurity Smart Regions. Through a series of interregional cooperation initiatives, CYBERSECURITY aims to improve the sharing of good practices and public policies and to strengthen cybersecurity ecosystems implementation and monitoring of regional Action Plans in order to boost the competitiveness of local cybersecurity SMEs.	practices and training resources related to cybersecurity skills development. Third, projects could connect the ecosystems across the Europe to grow the Cybersecurity Hubs network.
CEF. <b>Digitalna.si</b> (CEF – TC-2019-2)  Partners involved: CCIS	European Platform for Digital Skills and Jobs provides open access to a wide variety of high-quality information and resources for everyone interested in the broad topic of digital skills and jobs. It interconnects 11 National Coalitions websites to the Platform to publish relevant digital technology resources, such as trainings, strategies, events, founding opportunities.	The CyberHubs project can leverage the National Skills & Jobs platform by sharing knowledge, news, outputs and invitation to the events, conferences and other networking activities and reach wider target audiences.
ARRS-CRP - Slovenian Research Agency's Targeted research program. <b>RUKIV - Development of cybersecurity training programs</b> (V2-2132)  Partners involved: UM	The proposed research project addressed training and education in the field of cybersecurity. It produced a comprehensive way to tackle the deficiency of professionals in the cybersecurity field. The aim and objective of the proposed research project was to provide an additional knowledge and skills or competences through education and/or training in the field of cybersecurity in a structured and comprehensive way.	The CyberHub project will build on the idea of creating regional cybersecurity hubs, which will promote cybersec skills and knowledge. Project RUKIV has prepared a proposal for an official HE study programmes (one 120 ECTS, one 60 ECTS), as well as a catalogue of cybersecurity seminars and workshops. This can be used as a basis for any activities of CyberHubs related to skills and training.
Horizon 2020. <b>CONCORDIA - Cybersecurity Competence for Research and Innovation</b> (830927)  Partners involved: UM, EITD	CONCORDIA is a major H2020 consortium to interconnect Europe's Cybersecurity capabilities. It was established as a pilot for a Cybersecurity Competence Network and lead the development of a common Cybersecurity Research & Innovation Roadmap for Europe.	CONCORDIA was a project that delivered 21 results to strengthen European cybersecurity and we can bring lessons learned and developed sections into the CyberHub project, which will be continuing the goal of increasing cybersecurity skills, evolving threat landscape etc.
Horizon 2020. <b>CyberSec4Europe: Cybersecurity Network of Competence Centres for Europe</b> (830929)  Partners involved: UM	The main objective of the project is to establish and operate a pilot for a Cybersecurity Competence Network with the aim to strengthen research and deepen cooperation in the field of cybersecurity in the EU. CyberSec4Europe's aim is to operate a pilot for a Cybersecurity Competence Network and to develop and implement a common cybersecurity research and innovation roadmap.	CyberSec4Europe project was involved in EU regulations and the outputs from the project could be well used in the part of compliance with regulations in the CyberHub project. It has also built cybersecurity skills and capacity-building building outputs where CyberHub can continue the mission.
Internal Security Fund. <b>FRISCO Fighting teRrorISt Content Online</b> (101080100)  Partners involved: IVSZ	The general objective of FRISCO is to support Hosting Service Providers (HSP) to comply to the Terrorist Content Online (TCO) regulation. It aims to i) inform and increase HSPs' awareness of the TCO Regulation and their new obligations, ii)	FRISCO could help the CyberHubs project via mutual promotion, organisation of joint events, for example connecting with the partners to become CyberHubs' ambassadors in various countries.

	develop and validate tools, frameworks and mechanisms to support HSPs in the implementation of the TCO regulation, iii) Sharing experience, best practices and tools to support the implementation of the TCO regulation. As a result of the project targeted HSPs will have a better understanding of what is TCO and will be better prepared to deal with it and to comply to the TCO Regulation. This will lead to safer navigation online by reducing the risk to encounter TCO.	
Digital Europe Programme. <b>DigitalTech EDIH - Cybersecurity and digital competencies</b> (101083965)  Partners involved: IVSZ	DigitalTech EDIH is the reference Hub in Hungary to support start-ups, SMEs, mid-caps and public sector entities in their digital transformation focusing on key pillars of European priorities.	DigitalTech EDIH could help the CyberHubs project via mutual promotion, organisation of join events, providing input for the cybersecurity skills needs analysis.
Erasmus+. <b>Cybersecurity Aware Students for Public Administration (CASPA)</b> (2020-1-EE01-KA203-077958)  Partners involved: NKE, UPS, TalTech	The Cybersecurity Aware Students for Public Administration (CASPA) project aims to develop and maintain innovative courses in the field of cybersecurity, specially designed for university students who will work in public administrations as end users or as user having special role in cybersecurity.	Both UPS and TalTech were involved in this project, therefore the results can be directly used in the CyberHub project.
Erasmus+. <b>Interdisciplinary training on EU security, resilience and sustainability (EUSecure)</b> (2020-1-HU01-KA203-078719)  Partners involved: NKE	The core of our project is the development of a Simulation Supported HEI-level Massive Open Online Course entitled "Interdisciplinary training on EU security, resilience and sustainability" (EUSecure SimMOOC) - that also appears as an accredited elective in our universities' curricula.	Educational results from the EUSecure project can be transferred to the CyberHub project.
<b>REWIRE. The Cybersecurity Skills Establishing and operating a pilot for a European Cybersecurity</b> (621701-EPP-1-2020-1-LT-EPPKA2-SSA-B)  Partners involved: INFOBALT	REWIRE – is the Alliance formed from the four winning pilot projects of the 2018 Horizon 2020 cybersecurity call "establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap": CONCORDIA, ECHO, SPARTA and CyberSec4Europe.	The CyberHubs project can potentially connect with the REWIRE Alliance through collaboration on the development and implementation of a new sectoral strategic approach to cooperate on cybersecurity skills. The expertise and resources of the REWIRE Alliance in cybersecurity research and education, as well as its extensive network of partners, could be leveraged to support the CyberHubs project in achieving its objectives.
Horizon 2020. <b>SPARTA - Strategic Programs for Advanced Research and Technology in Europe</b> (830892)  Partners involved: KTU	SPARTA project developed a cybersecurity skills framework (CSF) model, which can be used as a reference by education providers to develop appropriate curricula. Employers may use it to help assess their cybersecurity workforce and improve job descriptions. Citizens may use it to reskill themselves. The Interactive Education map ( <a href="https://www.sparta.eu/study-programs/">https://www.sparta.eu/study-programs/</a> ) was created, which has been used in	The CyberHubs project can connect to the SPARTA project by leveraging the skills framework model developed by SPARTA to inform the development of cybersecurity skills hubs. The model can serve as a reference point for the design of appropriate curricula for the cybersecurity training programs. Additionally, the Interactive Education map developed by SPARTA can be used to help provide a

	various exchanges with the other pilots to help provide a unified and collective map.	collective map of cybersecurity education and training programs across Europe.
<p>CEF Telecom Program. <b>Digital Skills and Jobs Coalition Spain: Spanish Web Antenna</b> (INEA/CEF/ICT/A2019/2065474)</p> <p>Partners involved: AMETIC</p>	The website aims to be a reference for the debate on digital skills, as well as for the dissemination of information in relation to services, resources, training materials, and other relevant data related to said skills.	As the previous project, it can be useful as a network to find capacities, establish debates and help with diffusion and reinforce the Cybersecurity ecosystem.
<p>Agencia Estatal de Investigación (National Research Agency). <b>DDOL: Digital Inequality and job opportunities: study of the use of online platforms for job search in Spain</b> (RTI2018-098967-A-I00)</p> <p>Partners involved: UNIR</p>	The main purpose of this project is to test the hypotheses of the third digital divide in relation to the uses of the internet aimed at finding employment. The third gap is related to the social difference between expert knowledge and so-called social knowledge, i.e., between the contributions that exist in the network of specialists and all the information of little value that circulates on the internet, recently promoted by social networks.	The CyberHubs project could establish collaboration links to share data related to cybersecurity upskilling and reskilling, as well as digital skills and online reputation in the workplace. The project could provide insights into the digital skills and competencies required for finding employment and improving one's working position.
<p>Erasmus+. <b>ReWork: Leading inclusion in a hybrid and remote workplace</b> (2022-1-FR01-KA220-ADU-000086404)</p> <p>Partners involved: UNIR</p>	The principles of equality, inclusiveness and fairness are part of the core values of the European Union, and the new and boundaryless HRW environment has created increased concerns for a host of challenges especially around inclusivity and discrimination. <a href="https://rework-project.eu/">https://rework-project.eu/</a>	Both projects aim to develop skills. There may be opportunities to share best practices, collaborate on training activities, or jointly developing resources. Moreover, CyberHubs could support organizations to future-proof their DEI initiatives in the new and boundaryless HRW environment.
<p>Call for expressions of interest "Skills and jobs of the future" ("Compétence et métiers d'avenir"). <b>FORE-CY</b></p> <p>Partners involved: NUMEUM</p>	Establish a diagnosis of cybersecurity skills needs in the Grand - Nancy area in France.	The AMI CMA system illustrates the French State's desire to invest effectively in cybersecurity. The FORE-CY project could inspire other organizations and its method could be exported.
<p>Higher Education Authority of Ireland, Human Capital Initiative. <b>Cybersecurity Skills</b></p> <p>Partners involved: MTU - Cyber Ireland</p>	<p>"Cybersecurity Skills" project (€8.1m) is a national programme that provides online, fully flexible, university accredited, micro-credentials and pathways that focus specifically on creating new skills, upskilling and reskilling in cybersecurity for industry professionals in Ireland.</p> <p>Cyber Ireland is the industry partner to Cybersecurity Skills. We are hosted at Munster Technological University, who are the lead partner of the project.</p>	<p>Possible connections on the use of ENISA Cybersecurity Skills Framework for identifying job roles and skills demand, then developing course pathways for upskilling.</p> <p>The use of online training &amp; micro-credentials.</p>
<p>Science Foundation Ireland. <b>Cybersecurity Academy Project</b></p>	Cybersecurity Futures features information about the type of roles in cybersecurity and the Cybersecurity Academy provides technical training to young people / students (15-18 yrs) to	Education and outreach programmes to school students.

Partners involved: MTU - Cyber Ireland	educate the cybersecurity workforce of the future.	
<b>ENISA AdHoc Work Group on Cybersecurity Skills Framework (ECSF)</b>  Partners involved: Breyer Publico	The Ad Hoc Working Group	The CyberHubs project will provide a key opportunity to practically implement the European Cybersecurity Skills Framework (ECSF) launched by ENISA The European Agency for Cybersecurity across countries and in close collaboration between all project partners.
Horizon Europe 2020. <b>SME4DD</b>  Partners involved: EIT Digital	Training SMEs for the Digital Decade (SME4DD)- Horizon Europe (HE) will deliver short-term training programmes in three strategic digital technologies for Europe: 1) Artificial Intelligence, 2) Blockchain, 3) Cybersecurity.	The CyberHubs project can collaborate with SME4DD to design relevant cybersecurity training programs for small and medium-sized enterprises (SMEs) in Europe. The Cybersecurity Skills Hubs project can also share its expertise and best practices in cybersecurity skills development with SME4DD, particularly in designing short-term training programs that cater to the specific needs of SMEs. Additionally, the two projects can work together to promote the importance of cybersecurity skills and digital technologies for the success of European SMEs in the digital decade.
Digital Europe Programme. <b>Digital4Business</b> (101084013)  Partners involved: Adecco	Digital4Business - European Online Masters Programme focused on the practical application of Advanced Digital Skills within European SMEs and Companies aims to design and implement a highly innovative, effective, and sustainable European Masters Programme in Advanced Digital Skills (cybersecurity, AI, big data). Adecco (Myliia) is co-leading the Programme Rollout & Delivery also providing support to design training material and support programmes.	The CyberHubs project can connect to Digital4Business by sharing knowledge and expertise on cybersecurity skills needs that will be addressed by D4B too. The Digital4Business project can provide insights into the specific cybersecurity skills needed in the industry, and CyberHubs can use this information to develop targeted training programs to address the skills gap. Additionally, Digital4Business can share information on best practices for skills development with the CyberHubs project, which can help inform the development of cybersecurity skills strategies in the pilot countries.

#\$COM-PLE-CP\$# # \$PRJ-OBJ-PO\$# # \$REL-EVA-RE\$# # @QUA-LIT-QL@# # @CON-MET-CM@#

## 2. QUALITY

### 2.1 PROJECT DESIGN AND IMPLEMENTATION

#### 2.1.1 Concept and methodology

##### Concept and methodology

Please address all guiding points presented in the Call document/Programme Guide under the award criterion 'Quality of the project design and implementation'.

Outline the approach and methodology behind the project. Explain why they are the most suitable for achieving the project's objectives.

##### 2.1.1.1. Overall project design

The overall objective of the CyberHubs project is to establish and operate a transnational network of cybersecurity skills hubs across Europe to address the skills gap in the field of cybersecurity. This will be achieved through the development of a common framework, tools and methodologies for cybersecurity skills training, the establishment of regional cybersecurity skills hubs, and the implementation of pilot projects to test and validate the effectiveness of the approach.



The project also aims to facilitate collaboration and knowledge sharing between stakeholders, and to promote the adoption of best practices and standards in the field of cybersecurity.

To address the CyberHubs project global objectives, the consortium partners propose a project delivery methodology is organised by five interconnected Work Packages, each one addressing a separate but critical element of the project and delivered in sequence over the 3-year project duration.

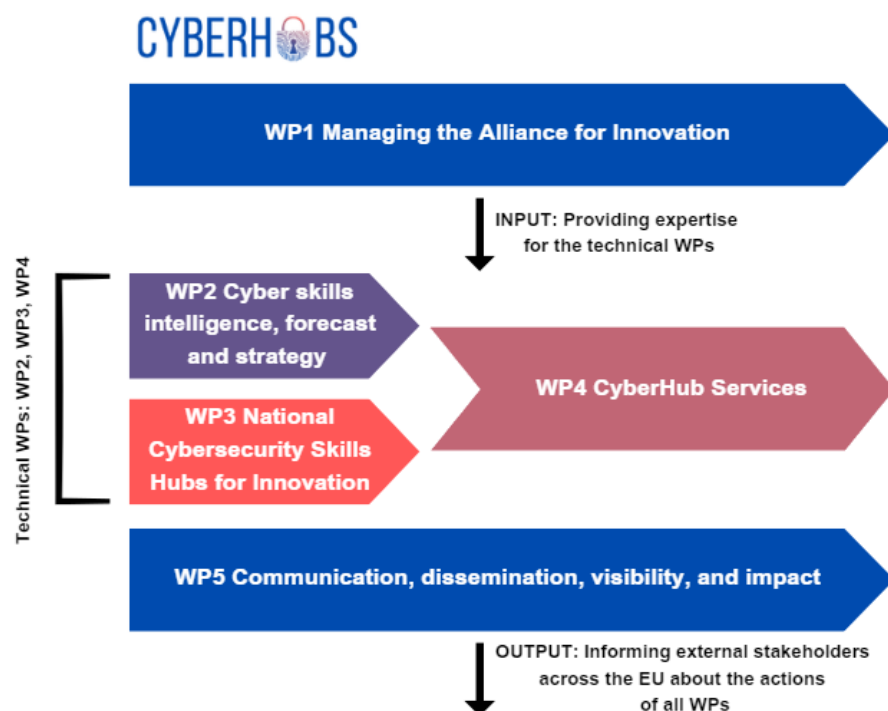


Figure 1: CyberHubs' Work Packages

This figure shows how the 5 Work Packages complement each other and represent, in particular at technical WP level, the logical progression in achieving the main technical content related project outputs of the CyberHubs project.

#### 2.1.1.2. Structure of the work programme

The following table shows the 5 Work Packages (WPs) with their respective tasks and key deliverables in more detail and illustrates how in particular the results from the successive technical work packages WP2 (Year 1), WP3 and WP4 (Year 2 and 3) build steadily upon each other and how WP3 and WP4 feedback each other. Moreover, WP1 and WP5 are horizontal WPs that support the more technically oriented WPs in carrying out their activities with good management and efficient communication, dissemination and exploitation aspects in mind.

Outline of Work Packages for CyberHubs		
Work Packages	Activities and Tasks	Deliverables
<b>WP1 - Managing the Alliance for Innovation</b> (M1 – M36)  WP Leader: DIGITALEUROPE (DE)	<ul style="list-style-type: none"> <li>T1.1 – Administrative and financial management</li> <li>T1.2 – Project coordination and risk mitigation</li> <li>T1.3 – Reporting and quality assurance</li> <li>T1.4 – Advisory Board coordination</li> </ul>	<ul style="list-style-type: none"> <li>D1.1 – Annual work plan</li> <li>D1.2 – Annual project collaboration and risk management report</li> <li>D1.3 – Quality assurance plan</li> </ul>
<b>WP2 - Cybersecurity skills intelligence, forecast, and strategy</b> (M1 – M12)	<ul style="list-style-type: none"> <li>T2.1 – Country-specific cybersecurity skills mismatches analysis</li> <li>T2.2 – Cybersecurity skills forecasting model</li> <li>T2.3 – Country-specific cybersecurity skills strategy</li> </ul>	<ul style="list-style-type: none"> <li>D2.1 – Cybersecurity skills mismatches analysis</li> <li>D2.2 – Cybersecurity skills Forecasting model</li> <li>D2.3 - Country-specific cybersecurity skills strategies</li> </ul>

WP Leader: Kaunas University of Technology (KTU)		
<b>WP3- National Cybersecurity Skills Hubs for Innovation</b> (M9 – M36)  WP Leader: Chamber of Commerce and Industry of Slovenia (CCIS)	<ul style="list-style-type: none"> <li>T3.1 – Setting up, developing, and sustaining National CyberHubs</li> <li>T3.2 – Knowledge transfer activities</li> <li>T3.3 – Alliance sustainability and exploitation strategy</li> </ul>	<ul style="list-style-type: none"> <li>D3.1 – National CyberHub governance and sustainability strategies</li> <li>D3.2 – CyberHub country delegation visits</li> <li>D3.3 – CyberHub Twinning Programme</li> <li>D3.4 – Alliance sustainability and exploitation strategy</li> </ul>
<b>WP4- CyberHub Services</b> (M12 – M36)  WP Leader: ICT Association of Hungary (IVSZ)	<ul style="list-style-type: none"> <li>T4.1 – Cybersecurity skills awareness raising, stakeholder engagement, and capacity-building activities</li> <li>T4.2 – European Cybersecurity Hackathon</li> <li>T4.3 – Piloting of a national AI-assisted system to match skills and jobs and forecasting model testing</li> </ul>	<ul style="list-style-type: none"> <li>D4.1 – Cybersecurity workshops impact assessment</li> <li>D4.2 – European Cybersecurity Hackathon</li> <li>D4.3 – Skills Academy Platform's User Manual and capacity-building</li> </ul>
<b>WP5- Communication, dissemination, visibility and impact</b> (M1 – M36)  WP Leader: DIGITALEUROPE (DE)	<ul style="list-style-type: none"> <li>T5.1 – Alliance communication and dissemination coordination</li> <li>T5.2 – CyberHubs visibility and impact at the national and EU level</li> </ul>	<ul style="list-style-type: none"> <li>D5.1 – Project communication and dissemination plan</li> <li>D5.2 – Project website and other communication tools</li> <li>D5.3 – European Cybersecurity Fest</li> </ul>

#### 2.1.1.3. Methodological approach using EU instruments and tools related to skills, occupations and roles

The CyberHubs project is designed to make use of several EU instruments and tools related to cybersecurity professional skills, occupations and roles.

The **ECSF (European Cybersecurity Skills Framework)** is a key EU-level available instrument for cybersecurity professional skills and workforce development that the CyberHubs project will adopt and integrate during the entire project lifecycle. The ECSF provides an open European tool to build a common understanding of the cybersecurity professional role profiles and common mappings with the appropriate skills and competences required. This Skills Framework was recently launched by ENISA (the European Agency for Cybersecurity), as a key enabler for joined multi-stakeholder action to tackle the enormous cybersecurity professional skills shortage on the European labour market today and perform in close interaction with other relevant initiatives in the field. For example, the project will use the ENISA Framework to identify the most critical cybersecurity skills, competences and roles needed by different sectors of the economy, and in particular in the deep tech domains, and to ensure the national strategies and related training offerings on cybersecurity skills are formulated in a way that can be understood and practically implemented across Europe.

Other relevant instruments and tools related to skills that the CyberHubs project will use are:

- **EQF (European Qualifications Framework).** The project will align the learning outcomes of the training offering with the EQF, which provides a common framework for describing and comparing qualifications across different countries and education systems.
- **ESCO (European Skills, Competences, Qualifications and Occupations).** In its 2023 update, ESCO considered elements of the above mentioned ECSF to inform the European classification on latest evolutions in cybersecurity professional skills, roles and jobs. Benefitting from these synergies achieved by the EU-level structures, the project will use ESCO complementarily and also consistently during the project.
- **EN16234-1 (e-CF)** common European Framework for ICT Professionals in all sectors and EU ICT Professional Role Profiles CWA 16458 will be used complementarily.
- **Europass.** The project will make use of Europass to provide learners with a portfolio of their skills and qualifications that is recognised across the EU, facilitating their mobility within the European labour market.
- **EQAVET (European Quality Assurance in Vocational Education and Training).** The project will recommend EQAVET to ensure the quality of the training planned by the Cybersecurity Skills Hubs, by implementing a quality assurance system that is based on the EQAVET framework.
- **ESG (European Standards and Guidelines for Quality Assurance in Higher Education).** The project will also recommend the use of the ESG to ensure the quality of the training offering planned by the Cybersecurity

Skills Hubs in the context of their national Cybersecurity Skills strategies, by aligning the quality assurance system with the ESG.

By making best use of these instruments and tools, the CyberHubs project will ensure that the Cybersecurity Skills Hubs national strategies are of high quality, meet the needs of cybersecurity learners and employers, and are recognised across the EU.

#§CON-MET-CMS# #@PRJ-MGT-PM@#

## 2.1.2 Project management, quality assurance and monitoring and evaluation strategy

### Project management, quality assurance and monitoring and evaluation strategy

*Describe the measures foreseen to ensure that the project implementation is of high quality and completed in time.*

*Describe the methods to ensure good quality, monitoring, planning and control.*

*Describe the evaluation methods and indicators (quantitative and qualitative) to monitor and verify the outreach and coverage of the activities and results (including unit of measurement, baseline and target values). The indicators proposed to measure progress should be relevant, realistic and measurable.*

#### 2.1.2.1. Project management structure and tools

DIGITALEUROPE (DE) will be responsible for WP1 Project Management, intended to coordinate and administrate project actions, as well as to communicate and to report to EACEA. DE is the European Association representing the Digital Industry in Europe, with more than 35 000 companies represented throughout DE members. The organisation has a strong Project Team with considerable experience in managing multiple, complex projects such as three Sector Skills Alliance Projects granted in 2020 and 2021 (ESSA, CHAISE and ARISA), and contractor in the development of the Digital Skills and Job Platform. DE coordinates the projects ESSA (European Software Skills Alliance) and ARISA (Artificial Intelligence Skills Alliance), as well as the Preparatory Action (CSA) for the European Data Space for Skills. Finally, DE has a long experience in engaging its members through Working Groups in two of the main topics of the present proposal, Digital Skills and Cybersecurity.

**Project management approach.** The coordinator will implement a robust project management approach based on the PM<sup>2</sup> methodology developed and supported by the European Commission, to successfully manage the delivery of the contract and ensure the achievement of the CyberHubs project objectives. We will apply the PM<sup>2</sup> project management principles to coordinate, communicate, align, manage and control the activities and tasks involved in the set up and ongoing management of the overall contract and the coordination of each individual working group. The consortium is committed to ensuring that best-practice management methods and procedures are used to ensure the high-quality delivery of this project overall, and the quality of each individual deliverable in particular.

**Project management team.** For management of the proposed project, a strong and dedicated governance structure will be established to achieve the goals within time and cost limits and at high quality standards. To that end a Project Management Team (PMT) will be set up. The PMT will clarify the roles and responsibilities within the consortium. All consortium partners have extensive experience in managing multi-country EU funded projects and all project partners have previous experience of working together in various projects.

Project coordination will be led by Jose Martinez-Usero (PhD.), who is a Senior Project Manager at DE and has more than 15 years of experience in project and programme management. He is the coordinator of the Blueprint Sector Skills Alliance ESSA and the CSA regarding the preparatory action of the European Data Space for skills. Both projects can bring close working practices, tools and methods across to the present project, making it more efficient. He will be assisted by a team of specialists, including project managers, research and innovation managers and project communication and dissemination managers.

The overall operation management of the project activities is assigned to DE, which will lead the project in close collaboration with the Work Package leaders, and Task Leaders.

Project management aims at managing partners' human resources, knowledge and budget. Every six months, DE will make a so-called "deviation analysis". DE will require partners to provide a summary of the performed activities and will compare their implementation with the actual work-plan. In a six month basis, DE will also prepare an internal summary including a dissemination report and a financial report.

The operation management will be supported by three main tools:

- **The project annual Work Plan.** At the beginning of each year DE and the WPs leaders draw up an overall project plan which lists in chronological order all project activities grouped by work package. This work-plan is the backbone of the project and is, therefore, a crucial instrument for all partners to understand the technical side of the project, helping them to know at any stage of the project what needs to be done, by whom and by when. The work plan also serves as a monitoring instrument for project implementation.



- **The collaborative platform.** Following the long track record of successful experience of DE using Microsoft Teams for project coordination, this platform will be the software use to provide a common repository and discussion space to the consortium. The platform could be combined with mailing list to facilitate the delivery of important messages to partners, associated partners, work package leaders or the advisory board.
- **The project meetings.** These meetings will be organised both face-to-face and online, opening the possibility to organise hybrid meeting in order keep the budget for travels in an extensive consortium to the minimum. The project will organise 4 transnational meetings, including a kick-off meeting in Brussels and 3 annual meetings during the 36-month implementation of the project. Moreover, periodic meetings between the active Work Packages Leaders (and task leaders) and DE will be organized (at least once a month) to assure the smooth implementation of the different WPs, and, most importantly, to assure the collaboration and interaction among WPs. Bilateral meeting with single partners will be organized to tackle specific issues during the project implementation.

The CyberHubs project involves a number of different project bodies and functions to ensure the smooth and effective implementation of the project. These project bodies and functions include the Project Steering Committee (SC), the Project Director (PD), the Project Manager (PM), the Advisory Board (AB), and the Project Management Team (PMT). Each of these bodies and functions plays a critical role in ensuring that the project is completed successfully and that its objectives are achieved within the designated time frame.

This figure shows how the project bodies and functions interrelate to ensure an efficient implementation of the project.

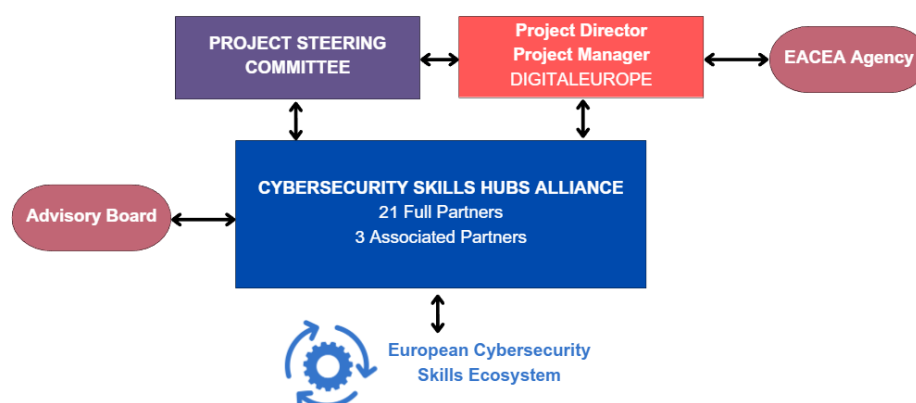


Figure 2: CyberHubs Project Bodies and Functions

The following table provides a more detailed description of each of these bodies and functions, their respective roles in the project and their composition.

Bodies and functions	Key role	Composition
<b>Project Steering Committee (SC)</b>	Key decision-making and issue-resolution body for the project. Any significant decisions that may affect the project or the team's ability to deliver on the objectives will be escalated to the SC. Approval of key documents, resolution of important project issues or significant change requests will be discussed and decided upon here. The SC meets regularly to discuss and make decisions on significant project issues, changes in scope or objectives, and other key documents or deliverables.	The SC includes representatives from each partner organization involved in the project, as well as external experts with relevant expertise and experience in the field of cybersecurity and skills development. The SC is typically led by the Project Director and includes the Project Manager, representatives from each partner organization, and external experts as necessary. The specific composition of the SC may vary throughout the project, as different expertise and perspectives may be needed at different stages of the project.
<b>Project Director (PD)</b>	The Project Director (PD) is responsible for overseeing the implementation of the project and directing key management activities. They are accountable to the Project Steering Committee (SC) for the successful delivery of the project within the specified time frame and budget, as well as for ensuring that the project meets its objectives and requirements. The PD works	The Project Director (PD) is a key individual responsible for overseeing the implementation of the project and directing key management activities. In the case of the CyberHubs project, the PD will be appointed by the coordinating institution (DE) and will have overall responsibility for ensuring the project is delivered on time, within budget, and to the required quality standards.

	<p>closely with the Project Manager (PM) to ensure that all project activities are aligned with the project's goals and objectives, and that the project is delivered to the highest quality standard. They are also responsible for managing relationships with stakeholders, including partners, funders, and relevant authorities. The PD reports to the SC and provides regular updates on the project's progress, risks, and issues.</p>	<p>In general, the PD will be a senior manager with significant experience in project management and in the specific field of the project. They will have a strong understanding of the technical and business requirements of the project, as well as the ability to manage complex projects involving multiple stakeholders. At the time of the proposal the appointed PD is Dr. Jose Martinez-Usero, Senior Project Manager at DIGITALEUROPE.</p>
<b>Project Manager (PM)</b>	<p>The Project Manager (PM) plays a critical role in ensuring the successful implementation and delivery of the project. The PM works closely with the Project Director and the Project Management Team (PMT) to develop and implement the project plan, and to identify and mitigate any risks or issues that may arise during the project lifecycle. They also serve as the primary point of contact for project stakeholders, including the Project Steering Committee (SC), the Industry Advisory Board (IAB), and the external partners involved in the project. One of the key responsibilities of the PM is to ensure that the project deliverables meet the quality standards set out in the project plan. They achieve this by reviewing project processes and documents, identifying any non-conformities with the set quality standards, and recommending corrective actions where necessary.</p>	<p>The Project Manager (PM) is responsible for the day-to-day management of the project and ensuring that it is delivered on time, within scope and budget, and to the required quality standards. The PM is typically a member of the project team and reports directly to the Project Director (PD).</p> <p>The PM may have a team of project coordinators or administrators to assist with their duties, and they may work closely with the Quality Assurance Team (QAT) to ensure that project deliverables meet the required quality standards.</p> <p>At the time of the proposal the appointed PM is Katarzyna Udala, Project Manager at DIGITALEUROPE.</p>
<b>Advisory Board (AB)</b>	<p>The Advisory Board (AB) is a group of external experts who provide strategic guidance and quality control for the project. The AB is responsible for reviewing and providing feedback on the project's progress, as well as identifying potential issues and opportunities for improvement. The AB is typically composed of individuals with relevant expertise in the project's domain, such as industry leaders, policymakers, and academic experts. The Project Director coordinates the AB and works closely with its members to ensure that the project is aligned with its goals and objectives. The AB also plays a key role in planning and implementing the business changes necessary to integrate the project deliverables into the organization's everyday work.</p>	<p>The composition of the Advisory Board (AB) in the CyberHubs project will depend on the specific needs and objectives of the project. However, typically, the AB is composed of external experts, industry representatives, stakeholders, and end-users who have relevant experience, knowledge, and skills in the field of cybersecurity, education, and training.</p> <p>The number of members on the AB may vary, but usually, it is between 5 to 10 individuals. The initial AB of the project will be composed by the associated partners.</p>
<b>Project Management Team (PMT)</b>	<p>The Project Management Team (PMT) is responsible for creating the project deliverables, which involves carrying out project activities according to the Project Work Plan and schedule. The team participates in developing the project scope and planning project activities and provides the Project Manager with information on the progress of activities. The PMT is composed of the project team members who are assigned specific tasks and responsibilities within the project. They work collaboratively to ensure that project</p>	<p>The composition of the PMT may vary depending on the specific needs of the project, but typically it includes individuals with technical and subject matter expertise related to the project objectives, namely: Work Package leaders and Task leaders of the active activities. The PMT may also include key representatives from partner organizations or associated partners involved in the project. The PMT reports to the Project Manager and provides them with information on the progress of activities.</p>

	goals are met, and deliverables are produced on time and within budget. The PMT is accountable to the Project Manager and is expected to provide regular updates on the progress of the project.	
--	--	--

### 2.1.2.2. Methods to ensure the highest quality in project implementation

The CyberHubs project is committed to ensuring the highest level of technical quality throughout its implementation, as well as the successful accomplishment of its strategic objectives and the production of transferable results with a wide impact. To achieve this, the project has established well-defined monitoring procedures and tools to review, control, predict, and verify the quality of implemented activities. This section will provide an overview of the quality assurance and control measures put in place by the project, including the Quality Assurance Team, the Project Steering Committee, and the Advisory Board.

- **The Quality Assurance Team.** The project foresees well-defined monitoring procedures & tools to review, control, predict and verify the quality of implemented activities. The aim is to ensure that the CyberHubs project will successfully accomplish its strategic objectives, assure the desired and expected quality of project results and achieve an impact going far beyond the partner organisations themselves, producing results that are widely transferable. To ensure the highest possible level of technical quality throughout the project we will set up a quality assurance team independently of the Project Management Team to advise on strategy and methodology and review all project outputs and deliverables. The Team will ensure the high quality of the project and its deliverables, by reviewing processes and documents, identifying non-conformities with the set quality standards and recommending corrective actions. To guarantee there is no conflict of interest or bias the experts will not be directly involved in the delivery of specific tasks and their role will be to critically evaluate all aspects of the project and advise on corrective measures needed.
- **The Project Steering Committee** will provide an additional level of quality control, ensuring the outputs are remaining closely aligned with market needs at each stage.
- **The Advisory Board** will provide an additional layer of strategic guidance and quality control, the project will establish an external Advisory Board, inviting domain experts from industry/academia. This mechanism has been used in other projects with great success and it provides an extra layer of external validation and leadership to the whole project.

The CyberHubs project has established a comprehensive Quality Assurance (QA) framework that ensures the highest level of quality in the project outputs and deliverables. The QA framework is designed around three key instruments: Quality Assurance Planning, Language Quality Check, and Risk Management and Mitigation Measures.

- **Quality Assurance planning.** A Quality Assurance Plan and the associated processes will be specifically developed for the needs of this project. The main objective of the Quality Assurance Plan is to ensure a consistent and qualitative assessment of the various Work Packages, their related key outcomes and activities during the project. Feedback from the entire partnership on collaboration and processes quality will be gathered on a regular basis, for fast take-up of lessons learned and allowing for continuous process improvement during the entire project lifecycle. For key outcomes external quality reviews by key stakeholders in the field will be performed (associated partners). This will be accompanied by solid KPI's tracking during the entire project.
- **Language quality check.** One of the key quality requirements during the project will be accurate local language translations for outputs such as Communications Campaigns and Tools.
- **Risk management and mitigation measures.** A Risk Management Plan will be included as part of the overall project Work Plan and it will include foreseen risks, estimated impacts and mitigation measures. Monitoring of the Risk Management Plan will be conducted on a quarterly basis and outputs will be incorporated into a quarterly report to the steering committee. The different risks for the individual tasks will be identified in a Critical risks and risk management strategy risk table. The risk table for this project will serve as the main register for all risks identified throughout the project duration.

### 2.1.2.3. Methods to ensure effective monitoring and evaluation

Monitoring and evaluation are critical components of any project, including the CyberHubs project, as they help ensure that the project is on track and achieving its objectives. The project will employ several methods to ensure effective monitoring and evaluation throughout its lifecycle.

- One of the key methods for monitoring progress will be **continuous monitoring by the Project Director and Work Package leads**, based on regular reporting and online collaboration, as well as weekly project management meetings. This approach will enable the project team to identify any issues or challenges early on and address them in a timely manner.
- In addition to progress monitoring, **financial monitoring** will also be conducted on a continuous basis, with a focus on checking implementation costs and monthly staff engagement evaluation and expenditures reports. This will ensure that the project is staying within budget and that resources are being used effectively.

- To evaluate the effectiveness of collaboration and overall partnership satisfaction, **annual partnership surveys** will be conducted. This will allow the project team to gather feedback from all partners and stakeholders and make any necessary adjustments or improvements to the project.
- The project will also use a **task monitoring system** to monitor and evaluate the performance of each task. This will help ensure that each task is completed on time and to the required standard, and that any issues or challenges are addressed as soon as possible.
- Finally, the project will facilitate **independent quality assessment** through the Quality Assurance Team. This team will provide an external perspective on the project's progress and outcomes, identifying any areas where improvements can be made. The Quality Assurance Team's report will be submitted together with the annual project progress and final reports respectively, providing an additional layer of evaluation and monitoring.

#\$PRJ-MGT-PM\$# #@\$CON-SOR-CS@#

### 2.1.3 Project teams, staff and experts

#### 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. and describe shortly their tasks. If required by the call, provide CVs of all key actors. If required by the Call document/Programme Guide.*

##### 2.1.3.1. The project teams and how they will work together to implement the project

The CyberHubs project involves three different roles: Manager, Researcher, and Administrative staff.

- The Managers are staff members from CyberHub partners who will lead or contribute to the coordination of a WP (Work Package) or a Task in the project. Their role is to oversee the implementation of the project at a strategic level and ensure that the objectives are being met. They are responsible for the overall coordination of the project, managing resources, and ensuring that milestones are achieved within the allocated timeframe. They will work closely with the Project Director, the Project Management Team (PMT), and the Project Steering Committee (PSC) to ensure that the project is on track.
- The Researchers are staff members responsible for the partner level implementation of the project. They act like project managers at the partner level or national Hub managers. Their tasks include not only the research activities in WP2 but also those that are linked to the establishment and development of the hubs in the 7 target countries, as well as the implementation of the Hubs' services. They focus on partner level activities and do not take any transnational coordination task. They will work closely with the Managers to ensure that the activities are implemented effectively and efficiently.
- The Administrative staff members support the work of the Managers and Researchers and/or implement complementary, preparatory activities. Their role is to ensure that the project runs smoothly, providing administrative support, and implementing the necessary administrative and financial procedures. They will work closely with the Managers and Researchers to ensure that the project is well-coordinated and that all project activities are being carried out in a timely manner.

All three roles will work together to implement the project by collaborating effectively and communicating regularly with each other. The Managers will provide overall guidance and direction, the Researchers will implement the activities at the partner level, and the Administrative staff will provide support to both roles. The PMT will oversee the implementation of the project and ensure that the activities are being carried out in accordance with the project plan. The PSC and the Advisory Board will provide guidance and quality control, ensuring that the project outputs are aligned with market needs and meet the set quality standards. By working together in a coordinated and collaborative manner, the project teams will ensure the successful implementation of the CyberHubs project.

##### 2.1.3.2. List of staff included in the project

The success of any project largely depends on the quality and expertise of the staff involved. The CyberHubs project has identified the key staff members who will be responsible for carrying out the various tasks and responsibilities in the project. These staff members come from different partner organizations and will work collaboratively to ensure the project objectives are achieved. The project team comprises of individuals with different skills and experience levels, including project managers, researchers, and administrative staff. Each role has specific responsibilities and tasks that they will perform throughout the project lifecycle. By leveraging the expertise of the project team, CyberHubs will be able to successfully implement its various work packages and achieve its intended impact.

Name and function	Organisation	Role/tasks	Professional profile and expertise
-------------------	--------------	------------	------------------------------------

José Martinez-Usero, Manager	DE	Project Coordinator	Senior Project Manager at DIGITALEUROPE. Project coordinator with 15 years of experience as project coordinator of more than 20 EU projects (Studies, CSA, RIA, IA, etc.). Jose has written several books and around 100 scientific articles in ICT related fields, and he is used to be a speaker in a wide range of international conferences and scientific events. M Sc Computer Science and PhD on Interoperability Technologies.
Alberto Di Felice, Researcher	DE	Policy expert	Director for Infrastructure, Privacy and Security Policy at DE. Expert in telecoms regulation and the impact of digital on innovation and business models. A certified Information Privacy Professional (CIPP/E). He holds degrees in law and European studies from the universities of Teramo and Trento in Italy, and a masters in diplomacy from the Institute for International Political Studies in Milan.
Marie Montaldo, Manager	DE	Communication manager - WP5 Leader	Communication manager, WP5 Leader. Experienced in designing and implementing communication strategies and dissemination actions, producing visual assets, and organising on-site and online events. She has worked with various EU-funded projects and leads the communications activities in European Software Skills Alliance (ESSA) and Artificial Intelligence Skills Alliance (ARISA). Marie holds a Master's degree in Communications and Project Management.
Katarzyna Udała, Manager	DE	Project Manager	Project and Communication Manager, she worked for a non-profit organisation towards implementing a yearly communication strategy, building brand visibility, and maintaining relationships with clients and institutional partners. She has delivered several training events and workshops across Europe, including training events co-developed with the Council of Europe. She holds a Bachelor's degree in Management and Sociology in Business and Media from Kozminski University. She also studied Business Administration at IE University in Madrid, Spain.
Eric van Cangh, Administrative	AGORIA	Senior Business Group Leader	Cybersecurity group leader at AGORIA. Experienced in IT resilience, co- author of the first socio-economic study of cybersecurity in Belgium, co-president of two working groups (ICS/OT and EU cybersecurity regulations) of the Cybersecurity Coalition. Security consultant for more than 10 years, notably at Sibelga, Ores, Generali. Engineer in Physical & Theoretical Chemistry and holder of an Executive Master in IT Management, IT Business, IT Governance & IT Security.
Floriane de Kerchove, Researcher	AGORIA	Overall coordination	Government Affairs Coordinator at Agoria, with a special focus on digital. Before that, she led fixed & mobile telecom infrastructure deployment in Belgium (mostly 4G and 5G) for Agoria and its members. She was also chairwoman of the Board for a new training center for digital skills (digitalcity.brussels), being the driving force behind its launch and development with public and private partners (4 years).
Georges Ataya, Researcher	SBSEM	Leading the project	Co-founder and manager of the Digital Governance and Trust at Solvay Brussels School. He participated in the development of the body of knowledge for the CISM credential (Certificate in Information Security Management) with more than 70.000 certified professional worldwide. He also co-created the body of knowledge of CGEIT credential as well as participated in the development of the COBIT Digital Governance framework.
Christophe Pierre, Researcher	SBSEM	Implementing changes and improvements on the Skillsbeam tool.	Certified project manager with an expertise in cybersecurity, mainly in the area of Information Security and Data Protection. Christophe holds a Master's degree in Business Engineering. He completed a European Data Protection Programme at Solvay Business School of Economics and Management.
Kurt Callewaert Valorisation, Researcher	HOWEST	Project manager, Dessimination & valorisation manager	Valorisation Manager in the field of Digital Transformation and former coordinator of the research group of Applied Informatics at HOWEST. He was responsible for the well-known Cybersecurity Professional track. For 12 years, he led a team that conducted research on Web3, Blockchain, Cybersecurity (including Industrial security), Data Protection (GDPR), RPA, AR and AI.



Gert-Jan Wille, Researcher	HOWEST	CS Researcher	Security Researcher at HOWEST, a CS Red Team expert and a CS SOC expert. Gert-Jan holds Bachelor's degree in Computer & Cyber Crime, Machine Learning and Applied Computer Science from HOWEST and an MBA degree from International Business Management Institute.
Doris Pöld, Researcher	ITL	Project Manager	CEO of ITL and the ICT Cluster Manager for over 10 years. Doris leads the collaboration and knowledge sharing between ICT companies in Estonia, supports companies' internationalization and implementation of innovation projects. She leads the cluster's team of project managers and the implementation of the cluster strategy.
Heleri Vahemäe, Administrative	ITL	Administrative	Office manager for over 18 years. Heleri also has over 16 years of experience in project administration, including the use of the project budget, developing and implementing action plans, preparing financial reports.
Birgy Lorenz, Researcher	TalTech	researcher	Expert in cybersecurity and experienced trainer in cybersecurity-related awareness. IT-Didactic Centre manager at TalTech (supporting lecturers, developing programs, doing research on HE level). Her research contributes to the curriculum of informatics in Estonia. Birgy holds a Degree in Information Society Technologies (Natural Sciences).
Anu Baum, Researcher	TalTech	Project manager	Experienced in managing and implementing international projects, previously worked in the Estonian Police, fighting against cybercrime, including online child abuse. Anu has the competence of creating learning materials on cybersecurity and legislation for commoners, parents and students. She holds a Master's degree in Law.
Andreja Lampe, Manager	CCIS	Director of Projects	Head of the ICT Innovation Network with over 30 years of experience in the ICT industry, from managerial positions in different ICT companies, project management, program management, to managing international teams. Founder of Gaia-x Hub Slovenia and member of Gaia-X Dataspace business committee and Gaia-X Governance workgroup, active in several data related associations.
Mateja Pucihar Baebler, Researcher	CCIS	Project Manager	Consultant and Project Manager at CCIS with experience in EU-funded projects. She is a project manager of two sector skills alliance projects: Erasmus+ Alliances projects: ESSA European Software Skills Alliance and ARISA Artificial Intelligence Skills Alliance.
Flavio Fuart, Administrative	CCIS	Project manager	Coordinator of the ICT Innovation Network and Gaia-X Hub Slovenia. He worked for Slovenian SMEs and research institutions, as well as for the European Commission. He has extensive experience in obtaining access to EU R&D funds and managing highly innovative R&D ICT projects in areas of IoT, text mining, Data Analytics, Industry 4.0, AI and cybersecurity.
Muhamed Turkanović, Researcher	UM	Researcher	Associate professor in data technology and information security. Holder of a PhD in the field of Computer Science and Informatics on the topic of cryptographic authentication protocols within the Internet of Things. Author of highly quoted articles with an impact factor in the field of computer science and informatics. He has more than 10 years of industry experience on an international base.
Tatjana Welzer Družovec, Researcher	UM	Researcher	Holder of a professorship for the following classes: Advanced Information Security, International and Intercultural Communication, Radio and Radio Programme, and Databases for Media. National delegate for IFIP TC 11 and a member of many other boards, including Conference PC and OC. Her research covers many areas, ranging from database technology to cross-cultural communication.
Marko Hölbl, Administrative	UM	Administrative	Assistant professor in informatics. His research work covers cybersecurity and privacy in the broadest sense, ranging from cryptography to user aspects of information security and privacy. He holds a professorship for several courses on the topic of cybersecurity. He has been involved in many EU-funded projects such as: EC H2020 project CyberSec4Europe - Cybersecurity for

			Europe, ATHENA - Advanced Technology Higher Education Network Alliance and Cyber F-IT - Cyber Security
Krisztina Bodáné Tajthy, manager	IVSZ	Secretary General, Supervisor, Liaison Manager	Secretary general, MSc. She is responsible for the coordination of the association and being involved as manager in the implementation of its projects. She has a wide network in the ICT industry which goes far beyond the membership of the association. She has 15+ years EU project and leadership experience. She gained cluster manager experience due to a Hungarian ICT cluster.
Klara Süveges-Heilingbrunner, Researcher	IVSZ	Project Manager	EU project expert, MSC in innovation management and EU policies. Throughout her 20 years of professional career, she was responsible for over 25 European funded projects as coordinator or WP leader. Coordinator of EU-funded projects at organisation level, involved both in the professional implementation as well as the administration of the projects.
Tamás Süveges, Manager	IVSZ	Project Expert and Leader	Director of projects, responsible for coordinating the implementation of all projects of the Association from the technical and financial sides. He has over 11 years of experience in project management planning and implementing large-scale projects targeting SMEs.
Dóra Halász, Administrative	IVSZ	Assistant	Assistant, she is responsible for supporting the implementation of various activities within the association, especially, event organisation, communication and administrative activities.
Csaba Krasznay, Manager	NKE	Leading task, managing the professional activities at UPS	Associate professor at the Ludovika – University of Public Service with cybersecurity being his field of research. Head of the university's Institute of Cybersecurity. Board member of the Voluntary Cyberdefence Cooperation, member of ISACA Budapest Chapter, Magyary Zoltán E-government Association, Hungarian Association of Military Science, Scientific Association for Infocommunications and the Hungarian Association for Electronic Signature.
Péter Bányász, Researcher	NKE	Participating in the cybersecurity education related tasks	Political science graduate from the Faculty of Law and Political Science of the ELTE, and holder of a doctorate from the Military Technical Doctoral School of the National University of Public Service. His research interests include the human aspect of cybersecurity, network theories of psychological operations, and the relationship between privacy and surveillance.
Bettina Hurja, Administrative	NKE	Administrative Assistant	Administrative assistant, she is responsible for supporting various administrative activities.
Anna Matsouka, Researcher	SEPE	Policy expert, Operational Programs & Digital Technology Initiatives Coordinator	Operational Programs & Digital Technology Initiatives Coordinator at SEPE. Anna has over 20 years of extensive experience in networks design, telecoms regulation, project management, coordination of digital technology initiatives. She holds a Bachelor's degree in Physics, a Master's degree in Electronics & Telecommunications, and an MBA.
Despina Kontopoulou, Researcher	SEPE	Communication & dissemination manager	Public affairs, communications and operations coordinator at SEPE with over 25 years of experience in Event Marketing & Management, PR, Corporate Communications. She works on projects such as Digital Economy Forum, the annual event for the digital technology industry.
Myriam Vassiliadou, Administrative	SEPE	Team coordinator	She is in charge of SEPE's general administration and active as a facilitator in the execution of many initiatives. She has been involved in the implementation of the training programs and public relations campaigns for the development of ICT for more than 15 years.
Georgia Bazoti, Administrative	SEPE	Project Coordinator, Project Manager	She holds a Bachelor's degree and a Master's degree in Electrical Eng. She has almost 35 years of professional experience in procurement, implementation, and support of IT systems (ERP, CRM, BILLING SYSTEMS, etc). She has been IT director for more than 10 years.
Dimitris Gritzalis, Researcher	AUEB-RC	Cybersecurity expert, Chair Professor of	Director of the M.Sc. Programme on Information Systems Security & Development. Director of the INFOSE Laboratory. Served as: Associate Data Protection Commissioner (GR), Vice

		Cybersecurity, Dept. of Informatics at AUEB-RC	Rector for Research, President of the Life-Long Training Centre of AUEB, President of the Greek Computer Society. Has >35 years of full-time research, consulting & teaching experience in cybersecurity. Directed/participated in >120 such projects. Author of >250 publications (papers, books, monographs).
George Iakovakis, Researcher	AUEB-RC	Cybersecurity Expert.	Cybersecurity Expert. Member of the INFOSEC Lab with over 10 years professional experience in research, training and consulting on cybersecurity, data protection, penetration testing, and risk assessment, for several public and private organizations. Certified GDPR professional, holder of a degree in Cybersecurity.
Mina Karagianni, Administrative	AUEB-RC	Project team Co-ordinator	Project team Coordinator with over 10 years of professional extensive experience in participating in cybersecurity, resilience, and data protection projects, mainly in designing and implementing communication policies and dissemination activities, including organising on-site and online events.
Virgilijus Dirma, Administrative	INFOBAL T	Project lead, managing director of Infobalt, Vice-chair of of Consumer Policy Working Group, PhD	Head of EU and International Relations at Infobalt. He manages the REWIRE Cybersecurity Skills Alliance. Panel discussion moderator in cybersecurity conferences, pro-active participant and content builder of the topic for Lithuanian authorities.
Milda Savickaite, Researcher	INFOBAL T	Project expert, head of innovation development	Milda has more than 10 years of experience in international project management in the field of sustainable energy, digitalisation, sustainable production lines, innovative solutions development and its internationalization. For 5 years she worked in the Netherlands Embassy in Lithuania, where the focus areas were: European Affairs, politics and economics, namely within the topics of Cybersecurity, Green Deal, Circular Economy and International Business Development, cooperation between Baltic and Nordic countries.
Algimantas Venčkauskas, Manager	KTU	Project manager; project expert and leader	Head of the Computer Science Department and research group of Cybersecurity of KTU. His research areas are information technology, Internet of Things, cybersecurity, application of distance learning technologies. Author and co-author of 65+ articles and 11 textbooks. Organiser and manager of the Information and IT Security master's program, running for 12 years in a blended learning way using DL technologies.
Nerijus Morkevičius, Researcher	KTU	Project expert	Associate Professor at Department of Computer Science at KTU. His main research interests are information and information technology security, enterprise application integration and intelligent control, Internet of Things technologies, and cybersecurity. Author and co-author of more than 20 scientific publications. Participated in several national and EU-funded research projects.
Rasa Brūzgienė, Administrative	KTU	Project expert	Associate Professor at Department of Computer Science at KTU. Her main research interests are cyber security, communication networks and security of critical infrastructure and cyber-physical systems. She is a lecturer in integrated cyber security trainings for employees of state and municipal institutions on control and management of systems in critical, high-incertitude situations as well as on risk management in the electronic resources managed by the institution.
Eduardo Valencia, Researcher	AMETIC	Project Coordinator	Eduardo has 15 years of experience in business industry dynamization, which includes project coordination, implementation of collaborative dynamics and methodologies, the application of analysis and diagnostic tools, as well as the drafting of positions and articulation of consensus. Director of AMETIC headquarters since 2017. Former director of the Spanish Cluster of home automation.
Cristina Protasio, Researcher	AMETIC	Policy expert	Digital Policy Manager of the Electronic Industry and Mobility at AMETIC. Physicist by Autonomous University of Barcelona, former telescope operator and an Astrophysics observer. She has collaborated in software development projects in different



			multinationals, including IDNEO for HP projects in the repair lines and more recently in Giesecke&Devrient in Cybersecurity.
Manuel Moreno, Administrative	AMETIC	Communication Manager	He has over 9 years of experience managing communication strategies for tech and digital industry projects. He is a Business & Marketing expert with expertise in Business Management. He currently oversees dissemination tasks for several European projects, including eVIA Technology Platforms, eNEM Platform, Digital Skills & Jobs Coalition, and ESSA Project. He has a bachelor's degree in Advertising and Public Relations from the University of Seville, Spain, and is currently pursuing an MBA with a specialization in digital marketing.
Daniel Burgos, Researcher	UNIR	Vice-rector for International Research	Full Professor of Technologies for Education & Communication and Vice-rector for International Research at UNIR. He holds a UNESCO Chair on eLearning and is a consultant to The United Nations Economic Commission for Europe (UNECE), in the secretariat of Education for Sustainable Development. Previously, he worked as Director of Education Sector and Head of User Experience Lab at the Research & Innovation Department of Atos, Spain, since 2007.
Javier Bermejo Higuera, Researcher	UNIR	Researcher	Professor at the School the School of Engineering and Technology of UNIR, specialised in Cybersecurity. Specialist cryptologist from the National Cryptologic Centre and a holder of three international certifications in Cybersecurity Defense from the Cybersecurity Forum Initiative (CSFI).
Alicia Fernández, Administrative	UNIR	Project Manager	She holds a bachelor's degree in Environmental Science and a postgraduate diploma in Science and Technology Communication. Her expertise includes writing proposals, project management, and communicating, disseminating, and exploiting R&D&I results
Anissa Kemiche, Manager	NUMEUM	Leading and supervising	Expert in European and French public policy. Anissa has 7 years of experience in the European policy field. She was a digital policy advisor at MEDEF and since 2020 she has been working in public affairs at NUMEUM. Anissa holds a Master's degree in European Governance from Sciences Po University.
Paul Pastor, Researcher	NUMEUM	Leading and supervising	Expert in digital law and leading project in cybersecurity. Paul has 7 years of experience in law with a special focus on telecoms and technology. Currently he works as a Legal Affairs and Cybersecurity Officer at NUMEUM. He holds a Master's degree in Space and Telecommunication Law.
Eoin Byrne, Researcher	MTU	Project Lead Cluster Manager	Eoin set-up Cyber Ireland in 2019 to bring together industry, academia and government to support the growth of the cybersecurity industry through collaboration, skills development, building an innovation ecosystem, and support internationalisation of SMEs. Previous to Cyber Ireland, he co-founded the V-LINC Group at Munster Technological University, specialising in industry cluster research in Ireland and internationally.
Fiona Kearney, Researcher	MTU	Communications & Dissemination	Digital Marketing expert with 9 years of experience in the field, with a focus on technologies and innovation. Fiona holds a postgraduate degree in Management and Marketing from the University College Cork.
Jutta Breyer, Manager/researcher	Breyer Publico SLU	Senior Consultant and Director Managing the contribution behalf of Breyer Publico	Director of Breyer Publico SLU, and senior consultant for human resources (HR) and pan-European multi- stakeholder collaboration, in business, education and politics on national and international level. Currently, Jutta is involved in the ENISA AdHocWorkGroup (AHWG) on the European Cybersecurity Skills Framework that was launched by ENISA in September 2022, and she has been member and rapporteur of the former ENISA AHWG on Cybersecurity Skills that developed this framework. She will be ensuring consistent implementation of the European Cybersecurity Skills Framework (ECSF) and complementary structures across project lifecycle.

Paul Aertsen, Manager/Researcher	Breyer Publico SLU	Senior consultant and manager/ researcher Leading design of methodology for skills needs analysis and skills forecasts	Senior Consultant with long-standing experience in skills needs analysis and forecasting, and translating identified needs into practical action, leading dedicated projects and chairing expert committees. Paul has over 25 years of experience in higher education as a researcher, author and lecturer in the fields of business and ICT, especially focusing on methodology. Over the course of his career, he has worked for several universities and vocational institutes. He is also a registered expert for EU assessing projects.
Wanda Saabeel, Researcher	Breyer Publico SLU	Senior consultant, manager/ researcher Managing design of methodology, researching input for methodology	Consultant in the educational field with over 20 years of experience, including projects related to designing curricula, arranging accreditation, formulating educational profiles including learning outcomes, formulating certification frameworks, coordinating development teams and managing learning programmes. She is also active in the field of standardisation with projects not only at national but also at European level. Moreover, she gained worldwide level experience too.
Àlex Galea Aixalà, Administrative	Breyer Publico SLU	Administration responsible	Àlex Galea Aixalà has long-standing experience in finances administration and management and is the administrator of the company.
Salvatore Moccia, Manager, Researcher	EIT Digital	Head of Master and Doctoral School	Head of EIT Digital Master and Doctoral School managing a portfolio of master programs. He has vast experience as manager in the higher education sector, as project manager and team leader, as director of human resource, as business consultant, as professional trainer & lecturer (leadership and team building, innovation, and management), as editor-author and as entrepreneur. He holds a Ph.D. from the University of Navarra, Pamplona, Spain, and an MBA from St. John's University, New York, US.
Alessandro Prunesti, Researcher	Adecco	Learning Designer	Alessandro has over 15 years of experience in the development of digital transformation and digital marketing projects in the sectors: banking, insurance, sport, media, IT, education. He also has experience in designing training programmes in advanced digital skills (Cybersecurity, AI, Virtual reality, Cloud, IoT and gamification). As a business consultant, he has managed technological integration projects in the web, social, mobile and Internet of Things fields.
Chiara Longobardi, Researcher	Adecco	Eu Funding Project Manager	Expert in European Project Management, since 2014 she worked on more than 20 EU Project for a variety of stakeholders. She works for Adecco as EU Funding Project Manager and is responsible for designing and delivering projects with a focus on education and digital skills and employment inclusion. She holds a Master's degree in Cooperation and Development, with a focus on EU funding.

**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).*

*If there is subcontracting, please also complete the table in section 4.*


Not applicable.

#§CON-SOR-CS\$# #@FIN-MGT-FM@#

**2.1.4 Cost effectiveness and financial management****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.*

#### **2.1.4.1. Measures for cost effectiveness**

The CyberHubs project has adopted several measures to ensure that the proposed results and objectives are achieved in the most cost-effective way. Firstly, the project has a clear and well-defined Work Plan with detailed deliverables, milestones, and deadlines. This helps to ensure that project activities are executed efficiently, and resources are allocated appropriately. The Work Plan also provides a clear framework for monitoring progress and identifying any deviations from the planned budget.

Secondly, the project has established a strong quality assurance process that ensures the high quality of project deliverables. This helps to reduce the likelihood of errors and rework, which can be costly in terms of time and resources. The Quality Assurance Team will review all project outputs and deliverables, identify non-conformities with set quality standards, and recommend corrective actions. This process will help to minimize the risk of costly mistakes and ensure that the project delivers the expected outcomes.

Thirdly, the project has established effective risk management strategies. The Risk Management Plan identifies potential risks and the estimated impact they may have on the project. The plan also outlines mitigation measures to be taken to reduce the impact of identified risks. By proactively identifying and addressing potential risks, the project can avoid costly delays and budget overruns.

Finally, the project team will regularly monitor the budget and expenses to ensure that costs are kept under control. Monthly staff engagement evaluation and expenditure reports will be conducted to monitor implementation costs. Any discrepancies will be addressed promptly, and corrective measures will be taken to ensure that project activities are executed within the planned budget.

Overall, by implementing these measures, the CyberHubs project aims to achieve its proposed results and objectives in the most cost-effective way possible, while maintaining the highest quality standards and minimizing risks.

#### **2.1.4.2. Financial management of the project**

The financial management of the CyberHubs project will be a crucial aspect of the project's success. To ensure that the proposed results and objectives are achieved in the most cost-effective way, the project will be managed in a highly professional and efficient manner.

DIGITALEUROPE has extensive experience in managing EU and nationally funded grant programs. With its large administrative, financial, and legal team, DIGITALEUROPE will provide comprehensive support to all aspects of the CyberHubs project, ensuring sound administrative and financial management.

To ensure that the project budget is carefully controlled and monitored, the project will make use of project management and accounting tools. These tools will allow for precise control and monitoring of the budget, with regular internal financial reports and a forecasting exercise to monitor project partners' expenditures. This will alert the Project Manager to early signs of delay or budget overrun, allowing them to take corrective action as needed.

The Financial Management of the CyberHubs project will be led by DIGITALEUROPE, strictly following the rules set in the EACEA Grant Agreement. A Consortium Agreement will be established among the project partners, setting the role of the coordinator (DE) and consortium partners and associated partners. This agreement will identify the responsible persons and bank account in each of the project partners, clearly indicating the amount of financial contribution allocated per partner, and when and how the contributions will be transferred.

The financial management will be performed through a set of tools and measures, including:

- In-depth presentation and discussion of all financial and administrative regulations in an extra workshop held during the kick-off meeting, focusing on the financial and administrative frameworks within the Grant Agreement. All information distributed to the partners will be confirmed in advance by the EACEA.
- DIGITALEUROPE will provide a set of templates to ease the reporting and administrative responsibilities of the partners.
- The core financial monitoring instruments are the annual reports. In a yearly basis, each partner will deliver a full financial report covering all expenditures during the last year. The reports will include all relevant documents and justifications (based on the common templates provided by DE), which might be asked by the EACEA or any auditing body. If needed, DE will perform closer monitoring, and it will organize more workshops (every two months) to ensure that partners' reporting is compliant with the Grant Agreement rules.

The financial management will be closely related to the activities implemented by the Quality Assurance Plan. A value-for-money-based approach considers it necessary that the financial flow is not only related to the performed activities but also to the delivered outputs and achieved results. Therefore, the financial management will be closely monitored to ensure that the project achieves its objectives in a cost-effective manner.

In conclusion, the financial management of the CyberHubs project will be conducted in a highly professional and efficient manner, using a range of tools and measures to ensure that the project budget is carefully controlled and monitored. DIGITALEUROPE's extensive experience in managing EU funded projects will be instrumental in ensuring the success of the project.

#\$FIN-MGT-FM\$# #@\$RSK-MGT-RM@#

## 2.1.5 Risk management

### Critical risks and risk management strategy

Describe critical risks, uncertainties or difficulties related to the implementation of your project, and your measures/strategy for addressing them.

Indicate for each risk (in the description) the impact and the likelihood that the risk will materialise (high, medium, low), even after taking into account the mitigating measures.

**Note:** Uncertainties and unexpected events occur in all organisations, even if very well-run. The risk analysis will help you to predict issues that could delay or hinder project activities. A good risk management strategy is essential for good project management.

#### 2.1.5.1 The risk management strategy

The risk management strategy for the project should be integrated into the project management plan and regularly reviewed to ensure its effectiveness. The Project Director should also communicate the risk management strategy to all partners and associated partners to ensure they are aware of potential risks and how they will be managed.

The risk management strategy for the project should include the following steps:

1. **Risk identification.** Identify and assess potential risks that may impact the project, including those related to cybersecurity, project delays, budget overruns, or changes in the project's scope.
2. **Risk analysis.** Analyse the potential impact of each identified risk and assess the likelihood of it occurring. This will help prioritize risks and determine which ones require immediate attention.
3. **Risk response planning.** Develop a plan to address each identified risk, including measures to mitigate, avoid, transfer, or accept the risk. This plan should be reviewed regularly and updated as necessary.
4. **Risk monitoring and control.** Monitor the project's progress and track potential risks to ensure they are effectively managed. Any changes in the project's scope, timeline, or budget should be monitored and assessed for their potential impact on the project's risk profile.
5. **Contingency planning.** Develop a contingency plan to address potential risks that may have a significant impact on the project's success. This plan should include measures to minimize the impact of the risk and ensure the project can continue despite the risk.

#### 2.1.5.1 List of potential critical risks affecting the project

The table includes a description of the risk, its potential impact, the likelihood of occurrence, and the proposed mitigation measures. By monitoring and addressing these risks throughout the project, the project team aims to ensure the successful completion of the CyberHubs project.

- "Impact" is understood as the impact of the risk on the project if it materialises.
- "Likelihood" is understood as the probability of this risk to materialise during the project lifetime.

Risk No	Description	WP No	Proposed risk-mitigation measures
1	<b>Delayed delivery of project outputs.</b> The project may experience delays in delivering its outputs, which could have a negative impact on the project timeline and budget. Impact: Medium Likelihood: Medium	1	The project consortium will establish a detailed project schedule with realistic timelines, monitor progress closely, and adjust the schedule as necessary to keep the project on track.
2	<b>Inadequate stakeholder engagement.</b> Failure to engage effectively with stakeholders could result in a lack of support or buy-in for the project, which could hinder its success. Impact: Medium Likelihood: Medium	1	The project consortium will establish a communication and dissemination plan (including stakeholder engagement tactics) and regularly communicate with stakeholders to keep them informed and involved throughout the project.

3	<b>Incomplete or inaccurate data.</b> If the project relies on data that is incomplete or inaccurate (the skills mismatches analysis at the national level), it may not be able to achieve its objectives or deliver its outputs. Impact: High Likelihood: Low	2	The Project consortium will establish data quality standards and procedures for data collection and analysis, and implement regular checks and audits to ensure data accuracy and completeness.
4	<b>Technological issues.</b> The project may encounter technological issues that could impact its ability to deliver its outputs or achieve its objectives (for example in the piloting of the EIT's Digital AI-assisted Skills Academy Platform (SAP) to match jobs and skills across the 7 CyberHubs). Impact: High Likelihood: Low	1, 4	The project consortium will establish a technology risk management plan and work with experts to identify and address potential issues early on. The Project Director has also a strong background in ICT and information management, that will facilitate the early identification of potential issues related to technology.
5	<b>Budget overrun.</b> If the project experiences unexpected costs or cost overruns, it could impact its ability to deliver its outputs and achieve its objectives. Impact: High Likelihood: Low	1	The Project Director and the Project Manager at DIGITALEUROPE will establish a detailed budget and regularly monitor expenses to ensure that the project stays on track financially.
6	<b>Inadequate team capacity.</b> If the project team within a partner or the whole project team working in a task lacks the necessary skills or resources to deliver its outputs, it could impact the project's success. Impact: Medium Likelihood: Low	1-5	The Project Director at DIGITALEUROPE will regularly assess team capacity and identify any gaps or areas for improvement, and provide training or additional resources as needed.
7	<b>Changes in policy or regulations.</b> Changes in EU policy or regulations on cybersecurity or skills management could impact the project's ability to deliver its outputs or to a certain extent, to achieve its objectives. Impact: Medium Likelihood: Low	1-5	The policy team at DIGITALEUROPE will regularly monitor relevant policies and regulations in the area and the Project Director and Project Manager will adjust the project plan as necessary to ensure compliance.
8	<b>Intellectual property issues.</b> The project may encounter issues related to intellectual property related to the background of the partners or ownership disputes regarding project outputs at country level. Impact: Medium Likelihood: Low	1, 4	The Project Director will establish an intellectual property policy and work with legal experts to identify and address potential issues early on. The Consortium Agreement will include a considerable number of clauses related to intellectual property and the availability of the project outcomes.
9	<b>Language and cultural barriers.</b> The project involves multiple partners from different countries, which could result in language and cultural barriers that impact communication and collaboration. Impact: Low Likelihood: Low	1	The Communication Manager in coordination with the Project Manager at DIGITALEUROPE will establish communication protocols and provide training to team members to ensure effective cross-cultural communication.
10	<b>Lack of interest or uptake from target audiences.</b> If the project outputs are not of interest or relevant to its target audiences, it could affect the impact and overall success of the project (for example lack of interest by national stakeholders in using AI-assisted Skills Academy Platform (SAP) to match jobs and skills in their context) Impact: High Likelihood: Low	1-5	The Project Director with the support and overall advice of the AB will conduct regular market research to ensure that the project outputs are meeting the needs of the target audience and adjust the project plan as necessary to ensure relevance and uptake.

#RSK-MGT-RM\$# #@CON-SOR-CS@#

## 2.2 PARTNERSHIP AND COOPERATION ARRANGEMENTS

### 2.2.1 Consortium set-up

Consortium cooperation and division of roles (if applicable)



Please address all guiding points presented in the Call document/Programme Guide under the award criterion 'Quality of the partnership and the cooperation arrangements'.

Describe the participants (Beneficiaries, Affiliated Entities, Associated Partners and others, 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.

### 2.2.1.1. Configuration of the consortium

The first and foremost guiding principle to identify project partners has been the quality and cost-effectiveness in reaching the project expected results. Among the several organisations approached during the consortium building, DIGITALEUROPE selected those that provided the higher quality, and innovative methodology in the different domains of the proposed project (educational methodology on HE and VET, Cybersecurity expertise both from the education and business side, and finally, experience in developing EU funded projects).

The CyberHubs Alliance for Education and Enterprises will strengthen the cybersecurity ecosystem in 7 European member states (Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain) by establishing reliable and sustainable relationships in the form of hubs. In each hub, at least one higher education provider institution involved in cybersecurity education and training and one national trade association of the ICT sector representing the labour market players will join forces. These key partners will ensure that a viral hub is established and carries out activities along a roadmap that the founding members and further associated stakeholders of the hubs agree upon in the 7 European countries. The consortium of the 7 hubs is supported by so called champion partners (Numeum in France representing the Campus Cyber and Munster Technological University in Ireland representing Cyber Ireland) who are excellence centres (hubs) in cybersecurity in their countries and in Europe and contribute to the future hubs' activities by knowledge and best practice transfer and capacity building activities. The perspectives of a VET provider are included in the Alliance's knowledge exchange activities and outputs via a well-known Italian VET provider, Adecco. Due to these 3 players, the knowledge exchange activities are supported by a HEI, a VET provider and a digital sector representing partner who bring sector specific views in the project, and also different cultural background which is expected to facilitate the adaptation of the best practices and the development of the hubs. The partnership is complemented also by two expert partners, who will lead and contribute to well defined key activities. Breyer Publico is expert in the field of cybersecurity skills and skills development frameworks, while EIT Digital is a European digital innovation ecosystem facilitator engaged deeply in the cybersecurity field.

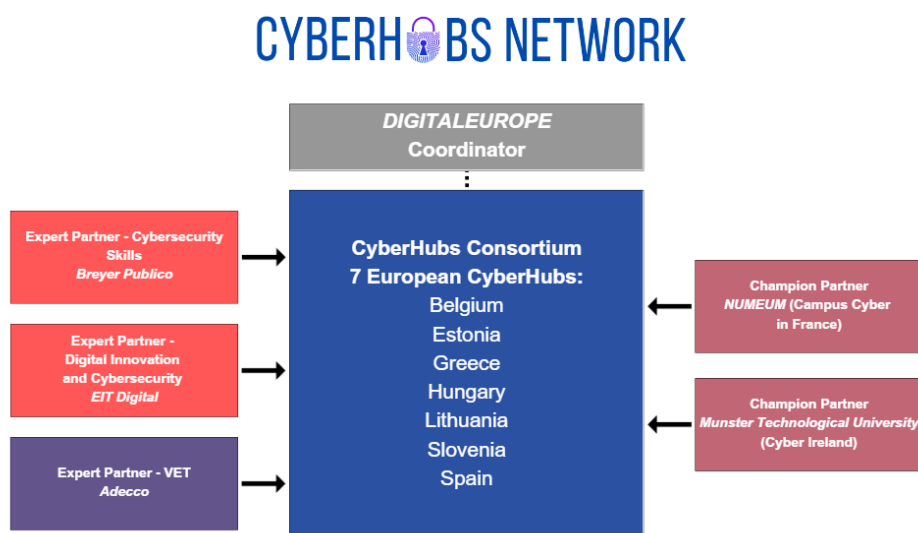


Figure 3: CyberHubs Network

The CyberHub transnational consortium consisting of 21 full partners (including the coordinator DIGITALEUROPE) and covering all together 11 European member states will work together towards the objectives of the project, namely to foster innovation, new skills and a sense of initiative and entrepreneurial mind-sets in cybersecurity that will be ensured via the 7 national cybersecurity hubs established as part of the CyberHubs project. Due to the associated partners joining the consortium, CyberHubs will ensure impact also in the Czech Republic and in Ukraine.

### 2.2.1.2. Description of the participants, collaborative work and complementarities

The participants in the CyberHubs project bring together a range of necessary expertise and complement each other in different ways.

The project is coordinated by **DIGITALEUROPE**, the European umbrella organisation of the digital industry, which proved its project management skills and competencies in the past years through the successful and effective coordination of several large Erasmus+ Sector Skills Alliance projects with the involvement of 15+ partners.

The project consortium includes **7 national trade associations**, who have a deep understanding of the needs and demands of the industry, including the skills and knowledge required for the cybersecurity workforce. These partners bring expertise in industry engagement, policy advocacy, and stakeholder management.

The **higher education institutions** involved in the project have expertise in cybersecurity education and training, curriculum development, and academic research. These partners bring knowledge of the latest trends and technologies in cybersecurity education, experience in designing innovative pedagogical approaches, and a strong network of academic professionals in the field.

The project includes **champion partners** such as MTU representing Cyber Ireland and Numeum representing Campus Cyber, who are excellence centers in cybersecurity in their countries and in Europe. These partners bring expertise and best practices in the establishment and development of cybersecurity hubs, as well as knowledge transfer and capacity building activities.

The project includes a well-known European **VET provider**, Adecco, who brings expertise in vocational education and training, including the design and delivery of training for the cybersecurity workforce.

The project includes expert partners such as Breyer Publico, who are experts in the field of cybersecurity skills and skills development frameworks, and EIT Digital, a European digital innovation ecosystem facilitator engaged deeply in the cybersecurity field. These partners bring a wealth of knowledge and expertise in cybersecurity education, training, and research, as well as policy development and industry engagement.

The participants in the CyberHubs project complement each other by bringing their unique expertise and knowledge to the project, enabling the consortium to achieve its objectives of fostering innovation, new skills, and a sense of initiative and entrepreneurial mindsets in cybersecurity. The diversity of expertise in the consortium ensures that the project outputs are of high quality, relevant, and tailored to the needs of the cybersecurity industry and workforce. In the following table a summary of the type of partners is provided.

Type of partners	Partners
Labour market actors - European Industry Umbrella Association	DIGITALEUROPE
Labour market actors - National Trade Associations	AGORIA, AMETIC, CCIS, Infobalt, ITL, IVSZ, SEPE
Higher Education Institutions	AUEB-RC, HOWEST, KTU, NKE, SBSEM, TalTech, UM, UNIR
Champion partners	MTU representing Cyber Ireland, Numeum representing Campus Cyber
VET provider	Adecco
European digital innovation ecosystem facilitator	EIT Digital
Cybersecurity skills expert	Breyer Publico
Associated partners	IT Ukraine, AAVIT, DTSL

### Full partners as beneficiaries

#### P1 - DIGITALEUROPE/DIGITALEUROPE (DE) – Belgium

DE is the leading trade association representing digitally transforming industries in Europe. Its mission is supporting regulatory environment that enables European businesses and citizens to prosper from digital technologies. Together with its members, DE shapes the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. DE membership represents over 35,000 businesses who operate and invest in Europe. It includes 87 corporations which are global leaders in their field of activity, as well as 38 national trade associations from across Europe. DE has an extensive experience in analysing the Digital Skills needs of the market, and engaging its members through its Working Groups, Communication campaigns and Events. Moreover, DE has an extensive expertise in managing EU funded projects, for example it coordinates the European Software Skills Alliance and the Artificial Intelligence Skills Alliance funded in 2020 and 2021 under the Sector Skills Alliance – Erasmus+ programme.

Role in the project: DE is the coordinator, it is in charge of WP1 Managing the Alliance for Innovation and WP5 Communication, dissemination and visibility. In addition, it takes task leader role in T2.1 and T3.3. It will take part in every professional task except T2.2 and T3.2.

#### P2 – AGORIA/AGORIA (AGORIA) – Belgium



Agoria is the Belgian federation of the technology industry that brings together more than 2000 technology companies and all those who are inspired by technology (digital and manufacturing sectors). Agoria's services and positions focus on digitalization, the manufacturing industry of tomorrow, talent management, policy and training, market developments, regulation, infrastructure, climate, environment and energy. Agoria has a business group called "Cybersecurity Made in Belgium". It is developing actions among others to increase the cybersecurity resilience and lobby to recognize the CS as critical sector, increase digital and cybersecurity skills. Agoria is closely involved in the training and education ecosystem in Belgium, contributes to the setting up of new Masters and is partner of the Belgian National Digital Skills and Jobs Coalition.

Role in the project: Agoria will be the key founder of the CyberHub in Belgium and accordingly it will take part in every activity of the project that contribute to the preparation, establishment and development of the hub. It will lead the national analysis of cybersecurity skills mismatches, the testing of the AI-assisted skills matching tool, get involved in competence development by learning from the champion partners and by organising training and ecosystem building events to hub members and stakeholders within the national cyberhub. It will take part in every professional task except T3.3 and T5.1.

### **P3 - Lifelong Learning of the Solvay Brussels School of Economics & Management (SBSEM)– Belgium**

SBSEM is a high-quality faculty dedicated to Economics and Management at the Université Libre de Bruxelles. Its main goals are to training leaders who aspire to the 'Homo Universalis' ideal, highlighting through its programmes the necessity of having a multi disciplinary perspective, and focusing on a quantitative and scientific approaches. SBSEM offered the first education in Digital trust in 2003. The executive education evolved to become in 2007 the "Postgraduate in IT Audit and Security" and in 2014 two executive education delivered the "Executive Programme in Cybersecurity" and the "Executive Master in Information Security Management". In 2016, the Belgian Cybersecurity Coalition was established by SBSEM. SBSEM launched also a project aiming at enabling cybersecurity professionals to assess their skills, identify upskilling alternatives, define career evolution models, and enable organisations to better manage Cybersecurity (as well as Digital skills). The tool/method is currently in use at the Belgian Public service.

Role in the project: Solvay being a HEI partner will contribute to the needs assessment activities in Belgium and the development of the cybersecurity skills strategy of the country. It will contribute to the establishment and competence development of the national CyberHub and participate in the services of the Hub. It will take part in every professional task except T3.3 and T5.1.

### **P4 - Hogeschool West-Vlaanderen/University of Applied Sciences (HOWEST) – Belgium**

Howest is an atypical, creative, innovative and enterprising institution. Howest coaches its students to become team-oriented, highly-skilled and directly employable professionals who are able to anticipate developments in our global society. Howest integrates socially relevant and competence-oriented education, valorisation-oriented research and services into its portfolio. Consequently, Howest is a strong "knowledge partner" working in close collaboration with and for the regional and international work field. It has a security and privacy research group that is active in four domains, namely cybersecurity, artificial intelligence, blockchain and innovative web platforms. One of the main objectives is to bridge the gap between the cutting-edge fundamental research in each of these domains and concrete applications that answer the needs and demands from enterprises both large and small and in government. It is partner in the EDIH Digitalis focusing on cybersecurity services for SMEs and PSOs. Howest is in Flanders the organizer of The Living Lab 'Innovative Cybersecurity for Industry and Logistics 4.0'

Role in the project: HOWEST being a HEI partner will contribute to the needs assessment activities in Belgium and the development of the cybersecurity skills strategy of the country. It will contribute to the establishment and competence development of the national CyberHub and participate in the services of the Hub. It will take part in every professional task except T3.3 and T5.1.

### **P5 - Eesti Infotehnoloogia Ja Telekommuniatiooni Liit/ Estonian Association of Information Technology and Telecommunications (ITL) – Estonia**

ITL is a non-governmental organisation having 124 members, whose primary objective is to unite the Estonian information technology and telecommunications companies and organisations, to promote their co-operation in Estonia's development towards information society, to represent and protect the interests of its member companies and to express their common positions. ITL speaks for the innovation of the digital society with vision of Smart Estonia and improves cooperation between the private and public sectors. ITL is the Legal body and cluster manager for Estonian ICT Cluster established in 2009. One of ITL's and also Estonia's strategic priorities is to widen SME's innovation and cybersecurity capabilities and through that increase the value added in other economic sectors. ITL is also an active member of the Information Security Council in Estonia, which is responsible for designing Estonia's cybersecurity policy.

Role in the project: ITL will be the key founder of the CyberHub in Estonia and accordingly it will take part in every activity of the project that contribute to the preparation, establishment and development of the hub. It will lead the national analysis of cybersecurity skills mismatches, the testing of the AI-assisted skills matching tool, get involved in competence development by learning from the champion partners and by organising training and ecosystem building events to hub members and stakeholders within the national cyberhub. It will take part in every professional task except T3.3.

#### **P6 - Tallinna Tehnikaülikool/Tallinn University of Technology (TalTech) – Estonia**

TalTech is the only technological university in Estonia. With its ca 9000 students and 1900 staff members, the university is an internationally recognized research institution that is actively responding to the rapidly developing society, tackling the challenges of the digital era. TalTech is cooperating with world-leading technology companies and universities and is in charge of nurturing the next generation of engineers and advancing the engineering culture in Estonia, contributing to the sustainable development of society and increasing national prosperity with its innovative services. The University has a Centre for Digital Forensics and Cybersecurity, the aim of which is raising capacity and competence of Estonian cybersecurity using educational, scientific and development activities. During the last few years, the centre has paid in addition to educational and scientific work more attention on prevention activities and working with the youth.

Role in the project: TalTech being a HEI partner will contribute to the needs assessment activities in Estonia and the development of the cybersecurity skills strategy of the country. It will contribute to the establishment and competence development of the national CyberHub and participate in the services of the Hub. It will take part in every professional task except T3.3 and T5.1.

#### **P7 - Gospodarska Zbornica Slovenije/Chamber of Commerce and Industry of Slovenia (CCIS) – Slovenia**

CCIS is a non-profit, non-governmental, independent business organization representing the interest of its members and is Slovenia's most influential business association. It has 5,200 member companies. One of its branch associations is the ICT association which is actively promoting digitalization and is involved in numerous national and international projects related to training and education for digital skills and is focused on attaining cross-sector multiplier impact that accelerates the development of the digital society and exploits opportunities for development of ICT, open data, data spaces artificial intelligence and cybersecurity. It is member of the EDIH in Slovenia and leads the Digital Skills and Jobs Platform's national activities and has taken coordinator, WP and task leader roles in large European skills alliance projects. Access to digitally skilled workers is already a key factor that sets successful companies apart from failing ones so closing the digital skills gap is at our highest priorities, so reskilling and upskilling employees is priority. One of the most active working groups in the association is the Cybersecurity work group.

Role in the project: CCIS will be the key founder of the CyberHub in Slovenia and accordingly it will take part in every activity of the project that contribute to the preparation, establishment and development of the hub. It will lead the national analysis of cybersecurity skills mismatches, the testing of the AI-assisted skills matching tool, get involved in competence development by learning from the champion partners and by organising training and ecosystem building events to hub members and stakeholders within the national cyberhub. CCIS is WP leader of WP3 National Cybersecurity Skills Hubs for Innovation and of T3.1 covering the establishment and development of the hubs. It will take part in every professional task except T5.1.

#### **P8 - Univerza v Mariboru/University of Maribor (UM) – Slovenia**

UM is the second largest (public) university in Slovenia with approximately 14,000 students and 17 faculties offering a full spectre of natural and social study programmes. UM is very entrepreneurially oriented and thus has strong partnerships established with businesses, governmental and non-governmental organizations and other institutions. UM is a founder and main operational entity of Digital Innovation Hub – DIH UM, as well as the coordinator for the EDIH DIGI-SI, which is 1 of the 2 Slovenian EDIHs. UM is member of many smart specialization clusters as well is actively involved in other regional activities. The Institute of Informatics hosts the CyberSec Lab:UM where the multidisciplinary team of researchers, developers and consultants who design, develop and evaluate cybersecurity solutions and services. UM was partner both in CONCORDIA and CyberSec4Europe that just recently ended and were funded as pilots for the European Cybersecurity Competence Centre (ECCC).

Role in the project: UM being a HEI partner will contribute to the needs assessment activities in Slovenia and the development of the cybersecurity skills strategy of the country. It will contribute to the establishment and competence development of the national CyberHub and participate in the services of the Hub. It will actively support the organisation of the European Cybersecurity Hackathon. It will take part in every professional task except T3.3 and T5.1.

#### **P9 - Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége/ICT Association of Hungary (IVSZ) – Hungary**

IVSZ is the joint platform of the information technology, telecommunications, and electronics sectors, representing the interest of the Hungarian information and communication technology sector for over 30 years with 350 members. IVSZ facilitates digitalisation of other sectors as well as the lawful operation of IT companies with various awareness raising activities & events. IVSZ is the key partner of the DigitalTech European Digital Innovation Hub in Hungary, offering services in key digital technology fields such as cybersecurity. In the EDIH. IVSZ is part of two European Skills Alliances where concrete curricula is developed and piloted at VET providers. The ESSA project focuses on Software development profiles while the ARISA project focuses on AI related job profiles. In addition IVSZ operates a cybersecurity working group where members interested in the field can gather and discuss relevant issues. IVSZ usually takes WP and task leader roles in European projects.

Role in the project: IVSZ will be the key founder of the CyberHub in Hungary and accordingly it will take part in every activity of the project that contribute to the preparation, establishment and development of the hub. It will lead the national analysis of cybersecurity skills mismatches, the testing of the AI-assisted skills matching tool, get involved in

competence development by learning from the champion partners and by organising training and ecosystem building events to hub members and stakeholders within the national CyberHub. IVSZ is WP leader of WP4 CyberHub Services and task leader of T4.1 focusing on competence development, awareness raising and ecosystem building activities of the hubs. It will take part in every professional task of the project.

#### **P10 - Nemzeti Közszoigálati Egyetem/University of Public Service (NKE) – Hungary**

NKE plays a key role in the education and research of the Hungarian public service. Its objective is to train professionals carrying out administrative, defence, disaster management and law enforcement activities, to provide the officer supply of the defence, disaster management and law enforcement bodies, and to create the interoperability of the unifying public service careers. The University has 5,000 students and cadets. It has 600 instructors. NKE as a public service university has an established connection to publicly owned enterprises (e.g., transportation, energy, water) and national authorities. The civilian cybersecurity activities at the University of Public Service happen in two entities: at the Department of Cybersecurity and the Institute of Cybersecurity. The first one is responsible for the educational activities, the latter one is for the research activities. Upon completion of the master's program, students get a Certified Cybersecurity Expert degree, which is a unique qualification in Hungarian higher education. The Institute coordinates relevant higher education, government, and international research links in the field and builds synergies with other entities and initiatives.

Role in the project: NKE being a HEI partner will contribute to the needs assessment activities in Hungary and the development of the cybersecurity skills strategy of the country. It will contribute to the establishment and competence development of the national CyberHub and participate in the services of the Hub. It will lead T4.2 and be the main organiser of the European Cybersecurity Hackathon. It will take part in every professional task except T3.3 and T5.1.

#### **P11 - Σύνδεσμος Επιχειρήσεων Πληροφορικής & Επικοινωνιών Ελλάδας/Federation of Hellenic Information Technology and Communication Enterprises (SEPE) – Greece**

SEPE, which represents the digital technology industry, aims to transform the Greek digital technology sector into a leading strategic industry that will: Stimulate Greek economy, encourage investment in research and technology, enhance digital literacy and at the same time, apply digital technology to address major social challenges. SEPE's work focuses on the areas of information dissemination, public affairs, and international presence. SEPE also monitors, analyses and responds to policies and regulatory developments that affect the digital technology industry; represents the industry to ensure the best possible regulatory and legislative environment. SEPE's efforts also focus on ensuring that Greece has the efficient number of ICT Specialists with the right knowledge and skills and citizens with ICT basic skills, to address the challenges to come.

It has extensive experience in skills-related projects and in providing training for upskilling and reskilling (incl also cybersecurity trainings). It organises every year the Digital Economy Forum, where cybersecurity is a key topic, and conducted recently a research that focused on ICT specialists' skills mismatch (incl also cybersecurity).

Role in the project: SEPE will be the key founder of the CyberHub in Greece and accordingly it will take part in every activity of the project that contribute to the preparation, establishment and development of the hub. It will lead the national analysis of cybersecurity skills mismatches, the testing of the AI-assisted skills matching tool, get involved in competence development by learning from the champion partners and by organising training and ecosystem building events to hub members and stakeholders within the national cyberhub. It will take part in every professional task except T3.3.

#### **P12 - Ειδικός Λογαριασμός Κονδυλίων Έρευνας του Οικονομικού Πανεπιστημίου Αθηνών/Athens University of Economics and Business (AUEB-RC) – Greece**

AUEB-RC is the leading academic institution in Greece in the areas of Cybersecurity and Resilience - Critical Infrastructure Protection. Its mission is to undertake, manage, promote and support research projects, consulting, innovation, and training activities on various topics - including cybersecurity - funded by private and public organizations and on both, a national and international level. AUEB-RC priorities focus on the promotion and adoption of the best available technologies and practices, and the strengthening of the cooperation between the government and the industry, in the fields of cybersecurity, data protection and resilience. It not only offers various training courses in cybersecurity but also develops new curricula and training meeting the needs of the market.

Role in the project: AUEB -RC being a HEI partner will contribute to the needs assessment activities in Greece and the development of the cybersecurity skills strategy of the country. It will contribute to the establishment and competence development of the national CyberHub and participate in the services of the Hub. It will take part in every professional task except T3.3 and T5.1.

#### **P13 - Asociacija Infobalt/ DigiTech Sector Association (Infobalt) – Lithuania**

INFOBALT is a national association of the DigiTech sector, that aims to create the best conditions for the growth of the DigiTech market. It has over 180 Lithuanian information and communication technology companies, related research and study institutions and other participants of the digital economy. The association represents the interests of its members in the public sector, organizes export missions for the members, solves DigiTech specialists supply problems, does a variety of research in relation to DigiTech and more. It operates several working groups of which the

cybersecurity and the human efforts are the most relevant for this project. Infobalt was member of the REWIRE project (See above in chapter 1.3) and organises the national Cybersecurity Forum every year in Lithuania.

Role in the project: Infobalt will be the key founder of the CyberHub in Lithuania and accordingly it will take part in every activity of the project that contribute to the preparation, establishment and development of the hub. It will lead the national analysis of cybersecurity skills mismatches, the testing of the AI-assisted skills matching tool, get involved in competence development by learning from the champion partners and by organising training and ecosystem building events to hub members and stakeholders within the national cyberhub. Infobalt is the main organiser of the European Cybersecurity Conference, the final event of CyberHubs. It will take part in every professional task except T3.3 and T5.1.

#### **P14 - Kauno Technologijos Universitetas/Kaunas University of Technology (KTU) – Lithuania**

KTU is the largest and oldest technological university in Lithuania. By integrating education, research and business, KTU focuses its activities on the enhancement of the quality of human life, and the acceleration of statehood development. One of KTU's key priorities is to maintain a synergy with local businesses in security area. It offers specialised training courses at 3 levels in cybersecurity. KTU participates in international and national projects aimed at developing digital skills, including cybersecurity, at all levels of society. KTU also conducts research in the field of cybersecurity. Since 2016, KTU, together with the National Cyber Security Center (NCSC) under the Ministry of National Defense, has been organizing and conducting large-scale cybersecurity exercises "Cybersecurity Shield"

Role in the project: KTU being a HEI partner will contribute to the needs assessment activities in Lithuania and the development of the cybersecurity skills strategy of the country. It will contribute to the establishment and competence development of the national CyberHub and participate in the services of the Hub. KTU is the WP leader of WP2 Cybersecurity skills intelligence, forecast, and strategy and Task 2.3 focusing on the national cybersecurity skills strategies. It will take part in every professional task except T5.1.

#### **P15 - Asociacion Multisectorial de Empresas de la Electronica, las Tecnologias de la Informacion y la Comunicacion, de las Telecomunicaciones y de los Contenidos Digitales/ Association of the digital industry sector in Spain (AMETIC) – Spain**

AMETIC represents the interest of the digital industry sector in Spain. Its members are enterprises and also regional associations of the sector and technology parks. In addition, it supports the internationalization of the members and their export activities to international markets. AMETIC operates 21 commissions and 12 working groups. It has a Commission focusing on Cybersecurity involving member representatives, universities, research centres and consultancy companies. Skills development and talent issues are heavily discussed in AMETIC and accordingly a specific Commission deals with the development of digital talent. AMETIC leads the Spanish chapter of the European Digital Skills and Jobs Coalition Platform and participates in the ESSA skills alliance too.

Role in the project: AMETIC will be the key founder of the CyberHub in Spain and accordingly it will take part in every activity of the project that contribute to the preparation, establishment and development of the hub. It will lead the national analysis of cybersecurity skills mismatches, the testing of the AI-assisted skills matching tool, get involved in competence development by learning from the champion partners and by organising training and ecosystem building events to hub members and stakeholders within the national cyberhub. It will take part in every professional task except T3.3 and T5.1.

#### **P16 - Universidad Internacional de la Rioja/ University of La Rioja (UNIR) – Spain**

UNIR is a 100% online university, which facilitates an exclusive, innovative, and high-quality virtual model of higher education, leant on a personalized, pro-active, and collaborative distance learning method of instruction. UNIR provides more than 400 academic degrees, and also private, non-official programmes, e.g. to companies' staff and professionals based on the industry requirements. Student enrolment is over 130.000. Foreign students at UNIR stands for the 40%, learning from over 100 different countries. UNIR works on selected scientific and humanistic fields of study with particular focus on ICT. The Software Engineering and Cybersecurity Group of UNIR has expertise in different cybersecurity fields.

Role in the project: UNIR being a HEI partner will contribute to the needs assessment activities in Spain and the development of the cybersecurity skills strategy of the country. It will contribute to the establishment and competence development of the national CyberHub and participate in the services of the Hub. It will take part in every professional task except T3.3 and T5.1.

#### **P17 - Numeum/Nauseum (Numeum) – France**

Numeum is the leading voice of the digital sector in France, representing more than 2500 companies of all sizes from high-growth tech start-ups to the largest groups operating in the digital sector, generating 85% of the sector's total turnover. Numeum represent the interest of its members, creates a dynamic digital ecosystem to promote synergies and innovation. One of its ambitions is to support France in the generalization and democratization of digital training. Numeum is shareholder and key member of „Campus Cyber“ a unique hub dedicated to cybersecurity in France. The Campus hosts many training institutes and allows them to be in regular contact with the relevant companies. Numeum



participates in all actions related to the attractiveness and diversity of digital technology organised by any ecosystem player, taking care to include cybersecurity.

Role in the project: Numeum is a champion partner of CyberHubs who brings its experience and knowledge in the project and supports the knowledge exchange activities (Task 3.2), the elaboration of the sustainability and exploitation strategy of the Alliance (T3.3) and contribute to the capacity building of the Hubs and the Hackathon in WP4. It is the leader of T3.2.

#### **P18 - Munster Technological University/Munster Technological University (MTU)**

MTU is a public technological university established in 2021, consisting of six campuses. Cyber Ireland is the national cybersecurity cluster organisation of Ireland, launched in 2019 to bring together industry, academia and government to represent the needs of the cybersecurity ecosystem and support its growth. The cluster is industry-led, hosted at Munster Technological University, and is supported by the government through the National Cybersecurity Centre. The cluster has over 150 member organisations nationwide, with 40 MNCs and 90 SMEs, as well as 15 Knowledge Providers including the education and training providers who supply the skills required by industry. Cyber Ireland aims at strengthening productivity and competitiveness in companies through cooperation on innovation and the transfer of knowledge between companies, knowledge institutions and other support actors in the cluster.

Role in the project: MTU is a champion partner of CyberHubs who brings its experience and knowledge in the project and supports the knowledge exchange activities (Task 3.2) and the elaboration of the sustainability and exploitation strategy of the Alliance (T3.3) and contribute to the capacity building of the Hubs and the Hackathon in WP4.

#### **P19 - Breyer Publico/Breyer Publico (Breyer) – Spain**

Breyer Publico is an independent consultancy firm, whose team combines in-depth experience in the area of cybersecurity skills as articulated by the European Cybersecurity Skills Framework (ECSF) that was launched by ENISA and in skills and competence performance in the IT professional full domain with practical know-how in the educational field on all levels, ensuring high-quality services provision to CVET and HE providers. Among the key areas of expertise are making best use of European IT Professional and digital skills and competence frameworks, multi-stakeholder collaboration, designing and executing domain-related research, as for skills needs analysis and forecast scenarios.

Role in the project: Breyer being a cybersecurity skills expert will take the leadership of T2.2 focusing on cybersecurity skills forecasting. It will be the key contributor of T2.1 too where the cybersecurity skills mismatches will be analysed and of T4.3 the piloting of National AI-assisted system to match skills and jobs. It will contribute to T3.3 too.

#### **P20 - EIT Digital/EIT Digital (EIT Digital) – Belgium**

EIT Digital is a pan-European ecosystem of top European corporations, SMEs, start-ups, universities, and research institutes that supports entrepreneurial education and skill through the development of Master Programs, Summer Schools and Professional courses. EIT Digital embodies the future of innovation by mobilizing a pan-European multi-stakeholder open-innovation ecosystem. It is running a Master program in Cybersecurity, in cooperation with several European Universities. In addition to that, it was partner in the CONCORDIA project, an EU-funded project in which a methodology for designing and deploying online courses was developed and successfully piloted together with a detailed scheme for offering certifications in the field of Cybersecurity. In addition to that, EIT Digital is co-leading several activities whitening the Deep Tech Talent Initiative for which it is developing a skills platform that will help to match job-positions and profiles, profiles and learning content, and mapping skills.

Role in the project: EIT Digital will be involved in the skills matching activities. It will be key contributor of T2.1 where the matching tool will be developed. In T4.3 EIT Digital will lead the testing of the AI-assisted matching system.

#### **P21 - Adecco Formazione/Adecco (Adecco) - Italy**

Adecco is one of the largest Italian training providers. It offers a comprehensive service of orientation, higher and continuing education, acting as a reference point for analysis, advice, and implementation of growth projects, using a methodological approach based on innovation, where the participant is placed at the heart of the training experience and makes them responsible for their own skills development.

Adecco participates in several European transnational projects focused on the development of advanced digital skills such as cybersecurity, AI, data space, cloud, IoT and so forth. where it contributes to the development and implementation of innovative curricula and training programs.

Role in the project: Adecco being a VET provider will primarily get involved in the knowledge exchange activities in T3.2 and will lead the twinning sub-activity in it and support the competence building activities in T4.1 and the organisation of the European Cybersecurity Hackathon in T4.2. Due to its role in the project it will be key contributor of T3.3 too.

#### **Associated partners**

#### **P22 - Asociace pro aplikovany vyzkum v IT, z.s./Association for Applied Research in IT (AAVIT) – Czech Republic**

AAVIT advocates and supports all interests of stakeholders involved in applied IT research and support activities connected with the digitalization of the public sector, creation and retention of jobs within the IT sector, and creation of GDP through applied research.

Role in the project: AAVIT will support get involved in the project primarily via the Advisory Board (T1.4). In addition, its volunteer participation in capacity development and strategy elaboration activities will be a valuable contribution, similarly to the communication activities to promote the project, its activities and results.

#### **P23 - Digital Technology Skills Limited (DTSL) – Ireland**

DTLS is the national agency dedicated to the promotion and facilitation of workforce learning in Ireland. Its mission is to facilitate increased participation in enterprise training and workforce learning within Ireland's small and medium enterprises (SME). DTLS has an extensive experience in developing VET programme on ICT for upskilling and reskilling the workforce.

Role in the project: DTSL will support get involved in the project primarily via the Advisory Board (T1.4). In addition, its volunteer participation in capacity development and strategy elaboration activities will be a valuable contribution, similarly to the communication activities to promote the project, its activities and results.

#### **P24 - Association "IT Ukraine" (IT Ukraine) - Ukraine**

IT Ukraine unites the interests of business, the state and international partners for the development of the IT industry in Ukraine. Together with its members, IT clusters and partners, it protects the interests of business and promote the brand of Ukraine as a leading technological nation.

Role in the project: IT Ukraine will support get involved in the project primarily via the Advisory Board (T1.4). In addition, its volunteer participation in capacity development and strategy elaboration activities will be a valuable contribution, similarly to the communication activities to promote the project, its activities and results.

### **2.2.2 Consortium management and decision-making**

#### **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.

##### **2.2.2.1. Consortium management structure**

The consortium management structure of the CyberHubs project has been designed to ensure full transparency and control of the project in terms of time, resources, and cost-planning. To achieve this, two levels of management have been defined: the Project Steering Committee and the Project Management Team.

- **The Project Steering Committee** will be led by DIGITALEUROPE and will include the leaders and co-leads of each Work Package, representatives from each partner company who wish to participate, and experts from the Associated Partners. This committee will ensure a good balance of representation across the partnership and facilitate the inclusion of senior experts from different types of organizations. It will be responsible for overseeing the project and making strategic decisions related to its implementation.
- The **Project Management Team**, on the other hand, will be responsible for the day-to-day management of the project. This team will be led by DIGITALEUROPE and will include a Project Director, WP Leaders, and Task Leaders. They will work closely together to ensure that the project is delivered on time, within budget, and to the required quality standards. The Project Director will be responsible for coordinating the work of the WP and Task Leaders, ensuring that the project runs smoothly, and addressing any issues or concerns that may arise.

Cooperation between partners is essential for the success of the project. The management structure of the partnership is set up to facilitate a shared but rapid decision-making process. The lead partner, DIGITALEUROPE, was selected as a coordinator thanks to its extensive experience of project management within multi-stakeholder grant-funded programs. At an early stage of the project, DIGITALEUROPE will define a detailed work plan for the three-year project along with a risk analysis that details potential project risks within each Work Package and proposes corrective measures should these risks occur. The detailed Work Plan will also identify the leaders and co-leaders of each Work Package and clearly present their responsibilities.

Overall, the consortium management structure of the CyberHubs project is designed to ensure effective project delivery, foster cooperation between partners, and facilitate decision-making. With DIGITALEUROPE leading the way, the partnership is well-equipped to achieve its goals and deliver on its promises.

#### 2.2.2.2. Decision-making mechanisms within the consortium

Decision-making mechanisms within the consortium will be established to ensure effective communication, coordination, and decision-making among partners. The decision-making process will be transparent and inclusive to ensure that all partners have equal opportunity to participate in the decision-making process.

**The Project Steering Committee (PSC)** will serve as the primary decision-making body for the project. The PSC will consist of representatives from each partner company who wish to participate, the leaders and co-leads of each work package, and experts from the Associated Partners. DIGITALEUROPE will lead the PSC, and it will meet on a regular basis to review project progress, discuss any issues or challenges that may arise, and make decisions related to the project.

**Work Package leader and co-leader.** In addition to the PSC, each work package will have a leader and a co-leader responsible for decision-making related to their respective work package. The leaders and co-leaders will work closely with the PSC to ensure that decisions related to their work package align with the overall project goals and objectives.

All decisions made by the PSC and work package leaders and co-leaders will be documented and communicated to all partners in a timely and transparent manner. If necessary, partners will have the opportunity to provide feedback or input on decisions before they are finalized.

To ensure that decisions are made in a timely manner, a clear decision-making process will be established at the start of the project. This process will outline the roles and responsibilities of each partner in the decision-making process and specify timelines for decision-making. The decision-making process will also outline the steps to be taken if partners are unable to reach a consensus on a particular decision.

In general terms, the decision-making mechanisms within the consortium will be designed to ensure that decisions are made in a transparent, inclusive, and timely manner, with the ultimate goal of achieving the project's objectives and delivering high-quality results.

#### 2.2.2.3. Regular and effective communication within the consortium

The CyberHubs consortium will establish internal communication processes to ensure that all partners are informed and updated on project activities, progress, and issues.

Communication within the consortium will take place through various channels, including virtual meetings, email correspondence (mailing lists and bilateral emails), and an online collaboration platform (Microsoft Teams). Virtual meetings will be held regularly, with at least one meeting per month. During these meetings, project updates and progress reports will be discussed, and any issues or challenges will be addressed. The online collaboration platform will serve as a central repository for sharing project-related documents and information, as well as for communicating with other partners.

The consortium will also establish a clear and concise reporting system to ensure that all partners are aware of project progress and are kept up to date on any issues or challenges. Reports will be generated on a regular basis, with specific deadlines established for each report. These reports will include updates on project activities, progress, and issues, as well as any changes to the project plan or budget.

To ensure effective communication, the consortium will also establish clear lines of responsibility and authority. Each partner will be responsible for communicating with their team members and ensuring that information is shared in a timely and effective manner. The project coordinator, DIGITALEUROPE, will be responsible for ensuring that all partners are aware of project progress and are kept up to date on any issues or challenges.

The internal communication processes will work in harmony with the quality assurance plan, including provisions for addressing any conflicts or issues that may arise during the project. A conflict resolution process will be established, with clear steps for addressing and resolving any conflicts. This will include regular check-ins and communication between partners, as well as mediation or escalation procedures if necessary.

#\$CON-SOR-CSS# #SQUA-LIT-QL\$# #IMP-ACT-IA@#

### 3. IMPACT

#### 3.1 Impact and ambition

##### Impact and ambition

Please address each guiding points presented in the Call document/Programme Guide under the award criterion 'Impact'.

Define the expected short, medium and long-term effects of the project. Who are the target groups? How will the target groups benefit concretely from the project and what would change for them?



**3.1.1. Expected short, medium, and long-term effects of the project**

This section outlines the expected impact of the CyberHubs project in terms of economic, social, and environmental benefits. The impact foreseen is categorised into short-term, medium-term, and long-term effects to provide a comprehensive understanding of the project's contribution to the cybersecurity industry, society, and the broader socio-economic environment.

Timeline	Effects
<b>Short term (1-3 years)</b>	<ul style="list-style-type: none"> <li>Increased understanding of European and country-specific needs for current cybersecurity skills and roles/professionals.</li> <li>Increased awareness and understanding of cybersecurity threats and the need for digital resilience and workforce transition.</li> <li>Improved structured collaboration of cybersecurity skills stakeholders including higher education, vocational education and training, and industry at both the national and EU level via the CyberHubs and its network.</li> <li>Improved knowledge transfer mechanisms between all CyberHubs actors and alignment with European frameworks and standards such as ENISA's ECSF.</li> <li>Increased provision of capacity-building activities and stakeholder engagement in the field of cybersecurity.</li> <li>Improved relevance and quality of cybersecurity education in the EU.</li> <li>Increased participation of underrepresented groups in cybersecurity-related activities.</li> <li>Improved cybersecurity skills matching through the piloting of the EIT's Digital Skills Academy Platform to match skills and jobs.</li> <li>Increased visibility and brand recognition of the CyberHub concept.</li> </ul>
<b>Medium term (4-6 years)</b>	<ul style="list-style-type: none"> <li>Increased understanding of European and country-specific needs for future cybersecurity skills and roles/professionals.</li> <li>Increased number of cybersecurity professionals in the EU.</li> <li>Improved entrepreneurial mindset as well as diversity and inclusion in the field of cybersecurity.</li> <li>Improved cybersecurity resilience of EU citizens and businesses.</li> <li>Increased EU-wide uptake of the project's outputs by the project's target groups.</li> <li>Strengthening of the European network of Cybersecurity Skills Hubs with the addition of new CyberHubs.</li> <li>Improved EU-wide exchange of good practices for cybersecurity resilience and alignment with European frameworks and policies in the field of skills.</li> </ul>
<b>Long term (7+ years)</b>	<ul style="list-style-type: none"> <li>Increased Europe competitiveness and innovation capacity in the field of cybersecurity.</li> <li>Improved cybersecurity skills forecasting and matching to meet the demand of the dynamic cybersecurity landscape.</li> <li>Increased availability of diverse and inclusive cybersecurity talents in the EU.</li> <li>Improved overall cybersecurity resilience of the EU.</li> </ul>

**3.1.2. Target groups and how the project engage and support them**

The project aims to address the challenges faced by the cybersecurity industry in the European Union, specifically the shortage of skilled professionals and the need to increase cybersecurity resilience. To achieve these objectives, the project has identified five target groups including industry players, learning providers, public organisations and social partners, youth and professionals, and policymakers. Each target group has specific needs and requirements that the project aims to address through its various activities and deliverables. This section provides an overview of each target group and how the project plans to engage and support them.

Target group	Stakeholder	Description and project engagement and support
Industry Players	<b>Companies</b>	This includes businesses of various sizes, from large corporations to small and medium-sized enterprises (SMEs). Companies are important target groups as they are major employers of cybersecurity professionals and are responsible for protecting their own and their clients' data and assets.
	<b>Start-ups</b>	Start-ups are businesses in their early stage of development, often with innovative products or services. The project aims to support start-ups in the cybersecurity sector, as they can contribute to the development of new and creative solutions to cybersecurity challenges.
	<b>Business associations</b>	These are organisations that represent the interests of businesses in a particular industry or sector. Business associations are important target groups as they

		can play a role in promoting cybersecurity awareness and best practices among their members (especially SMEs).
	<b>Business owners</b>	Small business owners, in particular, may have limited knowledge or resources to address cybersecurity challenges. The project aims to support them in building their capacity and awareness in this area.
	<b>Higher education institutions</b>	These are universities and colleges that offer bachelor's, master's, and doctoral degrees in cybersecurity and related fields. Higher education institutions are important target groups as they are responsible for training the next generation of cybersecurity professionals.
Learning providers	<b>VET providers</b>	These are organisations that offer vocational training programmes in cybersecurity and related fields. Vocational Education and Training (VET) providers are important target groups as they can provide practical and job-oriented training to individuals seeking to enter the cybersecurity workforce.
	<b>Private training providers</b>	These are organisations that offer training courses in cybersecurity and related fields outside of traditional higher education or VET settings. Private training providers are important target groups as they can provide flexible and customised training options to individuals and companies.
	<b>Public organisations</b>	This includes government agencies, such as ministries or departments responsible for cybersecurity policies and regulations as well as employment services. Public organisations are important target groups as they play a crucial role in shaping national cybersecurity and employment strategies and policies.
Public, NGOs, CSOs, and other social partners	<b>NGOs and CSOs</b>	These are organisations that work towards social or environmental causes. Non-Governmental Organisations (NGOs) and Civil Society Organisations (CSOs) are important target groups as they can raise awareness about cybersecurity among the general public and advocate for policies and practices that promote cybersecurity.
	<b>Other social partners</b>	This includes organisations such as trade unions, professional associations, and community groups. Other social partners are important target groups as they can contribute to building awareness and capacity in cybersecurity among their members and the communities they serve.
	<b>Youth and students</b>	This includes individuals under the age of 25 who are in school or university. The project aims to engage youth and students in cybersecurity awareness and capacity-building activities to encourage them to pursue careers in this field.
Youth, students, professionals, and NEETs	<b>Professionals</b>	This includes individuals currently working in cybersecurity or related fields. The project aims to support professionals in building their capacity and keeping their skills up to date through networking opportunities and an AI-assisted tool to match skills and jobs in the cybersecurity arena.
	<b>NEETs</b>	NEET stands for Not in Employment, Education, or Training. This includes individuals who are currently not employed, enrolled in education or training programmes, or actively seeking employment. The project aims to provide NEETs with opportunities to gain knowledge and skills in cybersecurity and enter the cybersecurity workforce.
	<b>National policymakers</b>	These are government officials responsible for developing and implementing national cybersecurity, skills, and employment policies and regulations. The project aims to provide policymakers with insights to shape national cybersecurity skills strategies.
Policymakers	<b>EU policymakers</b>	These are European policy makers responsible for developing and supporting the implementation of European policies related to education and training, employment, skills and cybersecurity. The project aims to provide concrete insights into the current and future cybersecurity skills demand and supply at the EU level as well as replicable good practices for knowledge transfer and capacity-building in the field of cybersecurity.

### 3.1.3. Impact and benefits of the project results on each target group

The following table summarises the expected impact and benefits of the CyberHub project on its five main target groups during the duration of the project (3 years). The impact and benefits listed in the table are based on the project's activities, expected results, and outputs.

Target groups	Expected impact and benefits	Related outputs
---------------	------------------------------	-----------------

<b>Industry Players</b>	<ul style="list-style-type: none"> <li>• Access to the CyberHubs as a one-stop-shop for cybersecurity skills information and awareness, capacity-building, and networking opportunities.</li> <li>• Improved cybersecurity resilience through better knowledge, awareness, and skills.</li> <li>• Increased trust and confidence among customers and partners through better cybersecurity practices and skills.</li> <li>• Access to new collaboration and business opportunities through cross-sectoral cooperation and innovation fostered by the national CyberHubs.</li> <li>• Strengthened cooperation, knowledge exchange, and innovation capacity among learning providers, industry, and other stakeholders through the CyberHubs and its European network.</li> <li>• Access to a pool of young cybersecurity talents.</li> </ul>	<ul style="list-style-type: none"> <li>• D2.1 Cyber skills mismatches analysis</li> <li>• D2.2 Cyber skills forecasting model</li> <li>• D2.3 Country-specific cyber skills strategies</li> <li>• D3.1 National CyberHub governance and sustainability strategies</li> <li>• D3.2 CyberHub country delegation visits</li> <li>• D3.3 CyberHub twinning programme</li> <li>• D3.4 Alliance sustainability and exploitation strategy</li> <li>• D4.1 Cybersecurity workshops impact assessment</li> <li>• D4.2 European Cyber Hackathon</li> <li>• D4.3 Skills Academy Platform's User Manual and capacity-building</li> <li>• D5.2 Project website and other communication tools</li> <li>• D5.3 European Cybersecurity Fest</li> </ul>
<b>Learning Providers</b>	<ul style="list-style-type: none"> <li>• Enhanced quality and relevance of cybersecurity education and training programmes through cybersecurity skills intelligence, forecast, and strategy.</li> <li>• Access to updated and relevant cybersecurity knowledge, good practices, and other relevant education and training programmes via the CyberHubs.</li> <li>• Improved capacity to upskill and reskill cybersecurity professionals at all levels considering the market needs and European frameworks.</li> <li>• Increased attractiveness and relevance of cybersecurity education and training programmes across Europe through mapping and matching to the labour market skills needs.</li> <li>• Strengthened cooperation, knowledge exchange, and innovation capacity among learning providers, industry, and other stakeholders through the CyberHubs and its European network.</li> </ul>	<ul style="list-style-type: none"> <li>• D2.1 Cyber skills mismatches analysis</li> <li>• D2.2 Cyber skills forecasting model</li> <li>• D2.3 Country-specific cyber skills strategies</li> <li>• D3.1 National CyberHub governance and sustainability strategies</li> <li>• D3.2 CyberHub country delegation visits</li> <li>• D3.3 CyberHub twinning programme</li> <li>• D3.4 Alliance sustainability and exploitation strategy</li> <li>• D4.1 Cybersecurity workshops impact assessment</li> <li>• D4.2 European Cyber Hackathon</li> <li>• D4.3 Skills Academy Platform's User Manual and capacity-building</li> <li>• D5.2 Project website and other communication tools</li> <li>• D5.3 European Cybersecurity Fest</li> </ul>
<b>Public organisations, NGOs, CSOs, and other social partners</b>	<ul style="list-style-type: none"> <li>• Improved capacity to design, implement, and monitor cybersecurity policies and initiatives at the national and European level.</li> <li>• Increased awareness and understanding of the importance of cybersecurity skills in the digital society and economy.</li> <li>• Improved cooperation and coordination among different actors involved in cybersecurity skills policies and initiatives at the national and European level.</li> <li>• Access to new cybersecurity tools, good practices, and standards for public services and citizens.</li> </ul>	<ul style="list-style-type: none"> <li>• D2.1 Cyber skills mismatches analysis</li> <li>• D2.2 Cyber skills forecasting model</li> <li>• D2.3 Country-specific cyber skills strategies</li> <li>• D3.1 National CyberHub governance and sustainability strategies</li> <li>• D3.4 Alliance sustainability and exploitation strategy</li> <li>• D5.2 Project website and other communication tools</li> <li>• D5.3 European Cybersecurity Fest</li> </ul>
<b>Youth, Students, Professionals, and NEETs</b>	<ul style="list-style-type: none"> <li>• Increased awareness and knowledge of cybersecurity risks, threats, and good practices on the safe use of cyberspace.</li> <li>• Improved access to cybersecurity learning and job opportunities through the EIT Digital's Skills Academy Platform.</li> </ul>	<ul style="list-style-type: none"> <li>• D2.1 Cyber skills mismatches analysis</li> <li>• D2.2 Cyber skills forecasting model</li> <li>• D3.1 National CyberHub governance and sustainability strategies</li> <li>• D3.4 Alliance sustainability and exploitation strategy</li> </ul>

	<ul style="list-style-type: none"> <li>Increased employability and career prospects in the cybersecurity field.</li> <li>Access to mentoring and networking opportunities with industry and other stakeholders.</li> <li>Improved digital literacy and citizenship skills for a safer and more secure online environment.</li> <li>Improved access to opportunities to contribute to the development of solutions to tackle today's cybersecurity challenges.</li> </ul>	<ul style="list-style-type: none"> <li>D4.1 Cybersecurity workshops impact assessment</li> <li>D4.2 European Cyber Hackathon</li> <li>D4.3 Skills Academy Platform's User Manual and capacity-building</li> <li>D5.2 Project website and other communication tools</li> <li>D5.3 European Cybersecurity Fest</li> </ul>
<b>National and EU Policymakers</b>	<ul style="list-style-type: none"> <li>Enhanced evidence-based and strategic recommendations for cybersecurity skills policies and initiatives.</li> <li>Improved understanding of the cybersecurity skills needs and related challenges of different stakeholders at the national and EU level.</li> <li>Access to a European network of experts and stakeholders for knowledge exchange and cooperation in the cybersecurity field.</li> </ul>	<ul style="list-style-type: none"> <li>D2.1 Cyber skills mismatches analysis</li> <li>D2.2 Cyber skills forecasting model</li> <li>D2.3 Country-specific cyber skills strategies</li> <li>D3.1 National CyberHub governance and sustainability strategies</li> <li>D3.2 CyberHub country delegation visits</li> <li>D3.3 CyberHub twinning programme</li> <li>D3.4 Alliance sustainability and exploitation strategy</li> <li>D5.2 Project website and other communication tools</li> <li>D5.3 European Cybersecurity Fest</li> </ul>

### 3.1.4. Key Performance Indicators (KPIs) to monitor progress and assess the expected impact

The following table presents a list of Key Performance Indicators (KPIs) that will be used to monitor the progress and assess impact of the CyberHubs project. Each KPI has a specific target value and a corresponding metric that will be used to measure progress towards that target. Additionally, a column has been added to assess the expected impact of each KPI, quantifying the benefits of achieving the target value. These KPIs have been selected to ensure that the project objectives are met and that the desired impact is achieved for the target groups.

NOTE: A more task-oriented and output-oriented list of KPIs is also provided in section 1.2.3. **CyberHubs project's specific objectives.**

Key Performance Indicators	Target value	Expected impact in target groups
Number of CyberHubs established during the project lifetime	7	Increase access to relevant cybersecurity skills training and learning opportunities across the EU by all target groups. Improve the coordination and integration of existing cybersecurity skills initiatives. Strengthen higher education, vocational education and training, business collaboration.
Number of new collaboration agreements established with representatives of the target groups (for the whole network)	30	Strengthen the cybersecurity skills ecosystem through cross-sectoral collaborations and knowledge-sharing.
Number of policymakers engaged with CyberHubs activities	35	Increase awareness and understanding of the importance of cybersecurity skills. Inform policy and decision-making in the field.
Number of industry players engaged through the CyberHubs activities	150	Increase awareness and understanding of the importance of cybersecurity skills. Foster collaboration and knowledge-sharing between industry and learning providers.
Number of learning providers engaged through the CyberHubs activities	150	Increase access to high-quality cybersecurity skills training and learning opportunities. Foster collaboration and knowledge-sharing between learning providers and industry.
Number of youth and NEETs engaged through the CyberHubs activities	100	Increase awareness and interest in cybersecurity skills as a career path. Provide opportunities for skills development and career advancement.

Number of professionals engaged through the CyberHubs activities	175	Increase awareness of the importance of upskilling and reskilling in cybersecurity. Provide opportunities for professional development and career advancement.
Number of public organisations and CSOs engaged through the CyberHubs activities	35	Increase awareness and understanding of the importance of cybersecurity skills. Foster collaboration and knowledge-sharing between public organizations, CSOs, and other social partners.
Number of participants in twinning activities	14	Increase awareness and knowledge-sharing among CyberHubs partners and stakeholders. Build capacity and skills through peer-to-peer learning.
Number of participants in the European Cybersecurity Hackathon event	50	Increase awareness and interest in cybersecurity skills among students, professionals, and NEETs. Foster innovative solutions and ideas in the field.
Number of participants in the country delegation visits	30	Increased transnational knowledge exchange and sharing of best practices in the cybersecurity skills field.
Number of active users on the AI Cybersecurity Skills Academy Platform (SAP)	140	Increased access to career path and job opportunities and forecasting tools, leading to better alignment of cybersecurity skills with industry demand.
Percentage increase in the number of students enrolled in cybersecurity-related courses through the SAP	10%	Increased awareness and interest in cybersecurity skills development among students and future professionals

#\$IMP-ACT-IA\$# #@\$COM-DIS-VIS-CDV@#

### 3.2 Communication, dissemination and visibility

#### Communication, dissemination and visibility of funding

*Describe the communication and dissemination activities which are planned in order to promote the activities/results and maximise the impact (to whom, which format, how many, etc.). 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.*

##### 3.2.1. Communication and dissemination activities

The communication and dissemination activities of the project, led by DE, aim at ensuring the project results and outputs reach the relevant target groups, as widely as possible, by selecting the appropriate communication channels and tools, and developing engaging promotional campaigns that will be timely implemented. The project adopts a two-fold approach consisting of ensuring the CyberHubs visibility and impact at the national and EU level — leveraging each of the 7 CyberHub ecosystems and ensuring a common voice for the European Network of Cybersecurity Skills Hubs.

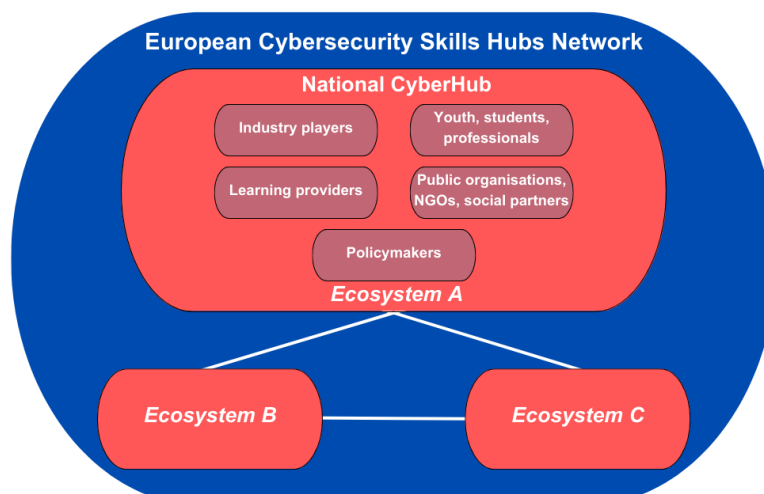


Figure 4: National CyberHubs connected at European level

To this end, the communication and dissemination plan (D5.1) will be key to not only further define the dissemination objectives (see WP5) but also ensure the target groups and tools and channels presented in this section are valid. It will set the direction of the communications by giving a recognisable, unique, strong voice to the CyberHubs and defining a strategy for EU-wide outreach. Key Performance Indicators (KPIs) will help to gauge the project communications' impact and inform the periodical consolidation of the communication strategy. The communication and dissemination



strategy will be translated into promotional actions and campaigns and implemented by the project communication channels and those of consortium partners.

The table below presents the main target groups of the project, related communication and dissemination activities, and their involvement in the project overall tasks and outputs. In addition to the below actions, it is to be noted that all partners will leverage their own ecosystems and networks throughout the project lifetime to complement the actions and further boost the impact of the dissemination efforts; be pro-active and support the WP5 leader DE by localising materials and linking their activities to relevant initiatives and projects at the local level.

The communications and dissemination activities foreseen include, but are not limited to:

- **Act 1** – Communication campaigns to raise awareness about cybersecurity threats, cybersecurity resilience, and safe use of cyberspace. (WP4 and WP5)
- **Act 2** – E-mailing campaigns for the CyberHubs partnership development and visibility (WP3 and WP5)
- **Act 3** – A series of CyberHubs capacity-building, awareness-raising and stakeholder engagement workshops (WP4)
- **Act 4** – Series of blog articles, opinion pieces, and interviews with relevant actors to discuss the need for cybersecurity skills and professionals (WP2 and WP5)
- **Act 5** – European Cybersecurity Hackathon to enhance cybersecurity young talents across European and connect high potentials with industry leading organisations (WP4)
- **Act 6** – Communication campaigns to promote the CyberHub SAP tool and pilots (WP4)
- **Act 7** – Representation of the CyberHubs at national and EU conferences to showcase the project results/outputs (WP5)
- **Act 8** – European Cybersecurity Fest to boost the uptake of the CyberHubs results and attract new CyberHub candidates (WP5)
- **Act 9** – Press releases on the good practices from the knowledge transfer activities including the promotion of the delegation visits and twinning programme results (WP3)
- **Act 10** – An EU-wide campaign to promote cybersecurity jobs and skills, attracting new talents in the cybersecurity, in particular people from underrepresented groups in the ICT field, e.g., women and girls (WP2)
- **Act 11** – National conferences to discuss topical issues related to cybersecurity relevant to education, training, policy, and the market (WP5)

Target groups	Communication and dissemination activities	Main involvement
<b>Industry players</b>	Act 1, Act 2, Act 3, Act 4, Act 5, Act 6, Act 7, Act 8, Act 9, Act 10, Act 11	<ul style="list-style-type: none"> <li>• Provide contributions, expertise, opinions, and data to feed the cybersecurity skills mismatches analysis</li> <li>• Exchange knowledge and good practices</li> <li>• Join/Support the national CyberHubs</li> <li>• Participate in the CyberHubs workshops (as participant or contributor)</li> <li>• Sponsor the European Cybersecurity Hackathon and/or propose real-world challenges</li> <li>• Take part in the European Cybersecurity Fest</li> <li>• Use the project results, especially the SAP and Cybersecurity Skills Strategies</li> <li>• Become a multiplier</li> </ul>
<b>Learning providers</b>	Act 2, Act 3, Act 4, Act 5, Act 7, Act 8, Act 9, Act 10, Act 11	<ul style="list-style-type: none"> <li>• Provide contributions, expertise, opinions, and data to feed the cybersecurity skills mismatches analysis</li> <li>• Join/Support the national CyberHubs</li> <li>• Exchange knowledge and good practices</li> <li>• Participate in the CyberHubs workshops (as participant or contributor)</li> <li>• Sponsor/Participate in the European Cybersecurity Hackathon</li> <li>• Take part in the European Cybersecurity Fest</li> <li>• Use the project results, especially the Cybersecurity Skills Strategies</li> <li>• Become a multiplier</li> </ul>
<b>Public organisations, NGOs, CSOs, and other social partners</b>	Act 1, Act 2, Act 4, Act 7, Act 8, Act 9, Act 10, Act 11	<ul style="list-style-type: none"> <li>• Join/Support the national CyberHubs</li> <li>• Exchange knowledge and good practices</li> </ul>

		<ul style="list-style-type: none"> <li>Sponsor/Participate in the European Cybersecurity Hackathon</li> <li>Take part in the European Cybersecurity Fest</li> <li>Use the project results, especially the Cybersecurity Skills Strategies</li> <li>Become a multiplier</li> </ul>
<b>Youth, students, professionals, and NEETs</b>	Act 1, Act 3, Act 4, Act 5, Act 6, Act 7, Act 10, Act 11	<ul style="list-style-type: none"> <li>Support the validation of the CyberHubs action plans</li> <li>Join/Support the national CyberHubs</li> <li>Participate in the CyberHubs workshops (as participant)</li> <li>Compete in the European Cybersecurity Hackathon</li> <li>Take part in the European Cybersecurity Fest</li> <li>Use the project results, especially the SAP</li> <li>Become a cybersecurity ambassador towards other students</li> </ul>
<b>National and EU policymakers</b>	Act 7, Act 8, Act 9, Act 11	<ul style="list-style-type: none"> <li>Support the implementation of the cybersecurity skills strategies</li> <li>Support the national CyberHubs</li> <li>Promote the European Cybersecurity Hackathon</li> <li>Take part in the European Cybersecurity Fest</li> <li>Become a cybersecurity ambassador towards other policymakers</li> </ul>

### 3.2.2. Dissemination channels

The following chosen dissemination channels will be used to maximise the impact of the project communication and dissemination activities. Each target group has its own preferred tools and channels — where they are the most active — those will be leveraged in priority. In addition, these dissemination channels enable us to personalise the communications with our target groups — which is beneficial to the project's success.

Channel/Tool	Best for	Characteristic of communication
<b>Project website</b>	All target groups	Official, informative, welcoming
<b>Social media</b>	<ul style="list-style-type: none"> <li>Industry players</li> <li>Learning providers</li> <li>Youth, students, professionals</li> </ul>	Professional, informative, visual, engaging, interactive
<b>Mass e-mailing</b>	All target groups	Professional, informative, narrative, promotional
<b>Direct e-mailing/messaging</b>	<ul style="list-style-type: none"> <li>Industry players</li> <li>Learning providers</li> <li>Public organisations, NGOs, CSOs, and other social partners</li> <li>Policymakers</li> </ul>	Professional, inviting, promotional
<b>Press articles</b>	All target groups	Official, informative, storytelling
<b>Press releases</b>	<ul style="list-style-type: none"> <li>Industry players</li> <li>Learning providers</li> <li>Public organisations, NGOs, CSOs, and other social partners</li> <li>Policymakers</li> </ul>	Official, informative, storytelling
<b>Events (online/ on-site)</b>	All target groups	Official, informative, storytelling, promotional

### 3.2.3. Marketing and promotional campaigns: how to reach to relevant stakeholders

The marketing and promotional strategy relies on an approach aiming to Reach, Act toward, Convert, and Engage (RACE) each of the target groups, thus creating widespread awareness and interest in the project. Based on these tactics, promotional actions and campaigns will be built to reach the relevant audiences. The promotional content and visuals will be packaged (into Communication Packs) and distributed to the CyberHubs partners for action. The RACE specific actions include but are not limited to:



**1) Reach — building brand awareness, increasing online visibility, growing an audience cross-channel:** launch of the CyberHubs website and social media; creation of stakeholder mapping at the EU and national levels; organisation of stakeholder meetings with relevant organisations, initiatives, and projects; direct emailing; deployment of a cybersecurity awareness-raising campaign; organic and sponsored social media content, SEO, attending/participating in third-party topical events to present the project, project-specific hashtags (e.g., #CyberHubs).

**2) Act — prompting interactions, increasing the positive sentiment towards the project and outputs:** creation of value-added content, direct emailing, developing engaging visual assets, creation and deployment of promotional campaigns on recent outputs with clear calls-to-action, activate Comms packs for partners, organic and sponsored social media content, attending/participating in third-party events to present the project.

**3) Convert — persuading key stakeholders to uptake project results, increasing trust:** highlighting supporters' viewpoint, organising calls with relevant initiatives and stakeholders, direct emailing, networking, cold-calling/meetings, organising events.

**4) Engage — boosting the multiplier effect, involving supporters, activating the European Cybersecurity Skills Hubs Network:** organising consultation meetings/roundtables, delivering media and communication kits, interacting with online communities, re-purposing engaging content.

In collaboration with the consortium partners and other EU and national stakeholders, we will design and execute coordinated EU-wide campaigns to ensure maximum dissemination and impact, as well as national-level campaigns in each of the CyberHub countries.

- **Launch campaign:** the focus is to raise awareness about the project and build a database of interested stakeholders/ potential multipliers. The campaign will begin with the launch of the CyberHubs' website and social media channels to introduce the project to the public. The key measures will be the no. visitors on the project's website, no. actions per user including, no. likes, comments, and shares on social media.
- **National CyberHubs expansion campaigns:** in each of the CyberHub countries, we will organise a campaign to increase the interest in the project and expand the database of interested stakeholders, with the possibility of a further expansion of the CyberHub at the national level. These campaigns will raise awareness about cybersecurity threats and the importance of cybersecurity skills among the project's target groups.

### 3.2.4. Visibility of the EU Funding

The visibility of the EU funding will be ensured in the following ways:

- The EU emblem will be clearly visible on all the visual assets produced (e.g., web banners, promotional videos, roll up banner, leaflets, etc.).
- All projects' written deliverables (e.g., reports, manuals, toolkits, etc.) — printed and/or online versions — will include the EU emblem and appropriate disclaimer.
- The website will display the EU emblem and appropriate disclaimer in its footer so it can be seen at any moment and on any pages. Beyond this, the website will have a dedicated section that acknowledges the EU's support for the development of the project and will clearly state the type of funding received. The project website will be advertised on social media posts and invite the stakeholders to discover it. Driving traffic to the website will ensure that the EU funding will be seen.
- The promotional videos that will be produced will display the EU emblem and acknowledge the financial support of the EU. This video will be widely disseminated through the promotional campaigns on social media and other channels.

#§COM-DIS-VIS-CDV\$# # @SUS-CON-SC@#

## 3.3 Sustainability and continuation

### Sustainability, long-term impact and continuation

*Describe the follow-up of the project after the EU funding ends. How will the project impact be ensured and sustained?*

*What will need to be done? Which parts of the project should be continued or maintained? How will this be achieved? Which resources will be necessary to continue the project? How will the results be used?*

*Are there any possible synergies/complementarities with other (EU funded) activities that can build on the project results?*

#### 3.3.1. Continuation and sustainability of the project

After the project funding period, the partners will continue to work together to ensure the sustainability of the project results and their long-term impact. The follow-up of the project will be ensured through a comprehensive sustainability and exploitation strategy (D3.4) developed during the project lifetime. The plan will outline specific actions and measures to be taken by each partner to ensure the continued use, exploitation and dissemination of project results beyond the project duration.

One of the key elements of the sustainability plan will be the development of a self-sustainable business model for the AI-assisted Cybersecurity Skills Academy Platform. This will involve identifying potential revenue streams, such as licensing fees, subscription fees, and sales of premium content, as well as exploring partnerships with relevant stakeholders to ensure the continued use and development of this platform or an equivalent one. This work strand will be aligned with the project Data Space for Skills, led by DIGITALEUROPE, with a number of use cases and solutions to match skills and jobs and to forecast future skills needs. Therefore, each national CyberHubs will have the possibility to implement a sustainable data space application for the country, using local providers but following the model tested during the project.

To ensure the sustainability of the CyberHubs, the partners will work on building strong partnerships with relevant stakeholders, such as national and regional authorities, the civil society, industry associations, and educational institutions. The partners will also explore opportunities for securing additional funding from national and private sources, as well as from EU programmes and initiatives that support cybersecurity education and training. For example, DIGITALEUROPE has already created an organisation-wide Roadmap for EU projects related to Cybersecurity skills for the period 2023-2024. In this respect, some of the envisaged project proposals will be oriented to the extension of the European Network of Cybersecurity Skills Hubs to more EU countries and the provision of more diverse innovative services.

To sustain the project impact, the partners will engage in dissemination and awareness-raising activities beyond the project duration including for example the organisation of national and EU-level events, the publishing of articles and reports, and leveraging existing networks and platforms to reach wider audiences. The partners will also work to ensure that the project results are integrated into relevant policies and strategies at the national and EU level, such as the European Skills Agenda, EU Cybersecurity Strategy, and with the recently launched Cybersecurity Skills Academy.

### 3.3.2. Specific actions to ensure sustainability and long-term impact of the key project results.

Specific actions should be taken to ensure the sustainability and long-term impact of the key project results, including the CyberHubs network and associated activities, the CyberHubs brand concept and main communication channels, the partnerships and collaboration established throughout the project, the country mappings of education and training programmes, the national cybersecurity skills strategies, the results of the Hackathon, and the results of the twinnings. By taking these actions, the project partners can continue to build upon the successes of the CyberHubs project and contribute to the development of the cybersecurity skills ecosystem at the national and EU level while leveraging other funding opportunities.

**The network of Cybersecurity Skills Hubs and associated activities.** The CyberHubs network and associated activities developed during the project should be maintained and expanded to further develop the cybersecurity skills ecosystem at the national and EU level. This will require continued engagement with the CyberHubs partners and relevant stakeholders, as well as the allocation of resources and funding. To ensure the long-term sustainability of the CyberHubs, the partners will develop a strategic plan (D3.1 National CyberHub governance and sustainability strategies) that includes measures to ensure financial sustainability, such as seeking funding from other sources or developing revenue-generating activities. In addition, the CyberHubs should continue to collaborate with other cybersecurity initiatives, such as the European Cybersecurity Organisation (ECISO) and the Cybersecurity Skills Academy initiative to create meaningful synergies and avoid duplication of efforts. Additionally, DIGITALEUROPE as coordinator will seek to extend the European Network of Cybersecurity Skills Hubs to other EU Member States and beyond, taking advantage of the presence of its member National Trade Associations in all EU Member States. These opportunities will be thoroughly considered when developing the Alliance sustainability and exploitation strategy (D3.4) which will be updated each year during the project's lifetime.

**The project's brand concept and main communication channels,** including the project website, the specific #CyberHubs hashtag and other promotional materials. The project's CyberHubs brand concept and specific hashtag should be maintained while expanding the network of Cybersecurity Skills Hubs to other Member States. The idea is to unify all initial and new Hubs under one banner (a.k.a. brand concept and visual identity). To this end, the visual identity, logotype, and communication guidelines will be kept up-to-date and will be integrated in a welcome package of each new CyberHubs. The project website, as the main, centralised tool for communicating around the project, will be maintained and updated by DE.

**The partnerships and collaboration established through the project,** including those with industry players, learning providers, public organisations, and policymakers. The partnerships and collaboration established through the project should be maintained and further developed to ensure the continued impact of the project outcomes. This includes engaging with industry players, learning providers, public organisations, and policymakers to promote the CyberHubs network activities, as well as seeking opportunities for collaboration and partnership on new initiatives, e.g., joint research or education projects.

**The country mappings of cybersecurity education and training programmes.** To ensure the continuity and sustainability of the country mappings of the cybersecurity education and training offering beyond the project duration, the project partners will collaborate with relevant stakeholders to create a database at the national level and potentially make relevant links and help feed the CyberHead tool of ENISA, the EIT Digital's Skills Academy Platform and other tools that could contribute to making it easier for individuals to find relevant and market-oriented educational offers.

**The national cybersecurity skills strategies and forecasting model.** The national cybersecurity skills strategies developed by the CyberHubs will be maintained and updated by the relevant national authorities in each country, and shared with the national cybersecurity skills ecosystem, fostering lobby activities and overall awareness raising of the strategy. In addition, the specific elements of the forecasting model tested and validated over the project lifetime (T4.3) will, in the long-term, be promoted for the widest possible use by CyberHubs consortium members (foreseen as part of the Alliance sustainability and exploitation strategy (D3.4)) to produce their country-specific cybersecurity skills forecasts on a regular basis.

**The results of the Hackathon.** The results of the Hackathon will be shared widely with the cybersecurity community through various channels, such as cybersecurity conferences and social media. The winning teams and their solutions will be highlighted, and the CyberHubs project will provide support to help the teams turn their ideas into marketable products or services in the long term. To ensure the continuity and sustainability of the Hackathon, the project will encourage the organisation of similar events at the national level and provide guidance and support to interested organisations or institutions.

**The results of the twinnings.** The results of the twinnings will be disseminated widely through various channels, such as the project website, CyberHubs channels, and cybersecurity-related events. The project will encourage the continuation of the twinnings beyond the project duration, and will provide guidance and support to interested organisations, including the management of virtual twinnings for knowledge exchange (building in the successful experiences of several projects during the Covid19 pandemic).

### 3.3.3 Measures and financial resources oriented to sustainability and long-term impact

To ensure that the results and benefits of the CyberHubs project are sustained beyond the funding period, it is crucial to have a clear understanding of the necessary resources for its continuation. This section outlines the measures and financial resources needed for the successful roll-out of the project's outcomes, and the steps needed to ensure its long-term impact. Specifically, it covers the available EU and national funding programs that can be leveraged to continue the project, financial resources from national and private sources, and continued support from industry players, learning providers, public organizations, and policymakers to maintain and build upon the partnerships and collaborations established through the project. By utilising these resources effectively, the CyberHubs project can continue to thrive and make a lasting impact on the cybersecurity skills shortage landscape in Europe.

One relevant EU funding programme is the **Digital Europe Programme (DEP)**, which is the EU's funding instrument to support the digital transformation of Europe's society and economy. DEP has several calls for proposals that could be of interest for the continuation of the CyberHubs project, such as the call for proposals on "Cybersecurity competence centres, including a European cybersecurity competence centre", or the call for proposals on "Advanced digital skills for the workforce".

Another relevant potential funding scheme is the **Erasmus+ programme**, which provides opportunities for education and training projects, including those related to cybersecurity skills. The program offers various calls for proposals, such as "Strategic Partnerships for vocational education and training" and "Cooperation Partnerships for Digital Education Readiness," among others.

Another funding program that may be of interest is **Horizon Europe**, the EU's research and innovation framework program. The program aims to support research and innovation activities in various fields, including cybersecurity, to address societal challenges and generate economic growth. Calls for proposals related to cybersecurity under Horizon Europe include "Cybersecurity for Digital Infrastructures" and "Cybersecurity Competence Centers," among others.

In addition to EU funding, there are also **national funding programmes** that can be used to sustain the CyberHubs project results. For example, in several EU Member States, there are national funding programmes to support the development of cybersecurity skills and the digital transformation of businesses. Partners could explore these funding opportunities to further develop the CyberHubs network and associated activities, as well as the national cybersecurity skills strategy developed as part of the project.

Moreover, partners could also use the partnerships and collaborations established through the project to leverage **additional funding opportunities**. For example, partners could collaborate on future projects or initiatives that align with the goals and objectives of the CyberHubs project, and use the network and relationships developed through the project to secure funding from other sources. Financial resources from national and private sources will be crucial to continue the CyberHubs network and associated activities beyond the project's duration. Partners can explore various national funding programs such as those aimed at promoting digital skills, supporting SMEs, or cybersecurity research and development. They can also seek financial support from private sources such as corporate sponsors, investors, or philanthropic organizations that share the project's goals and vision.

Partners can leverage the relationships and networks built during the project to further develop joint initiatives, exchange good practices and resources, and explore new avenues for cooperation. Furthermore, partners can engage with relevant stakeholders and decision-makers to promote the project's outcomes, advocate for its goals, and generate interest and support for future related initiatives.



#@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)).

**CYBERHUBS**

**WP1 Managing the Alliance for Innovation**

**WP2 Cyber skills  
intelligence, forecast,  
and strategy**

**WP3 National  
Cybersecurity Skills  
Hubs for Innovation**

**WP4 CyberHub Services**

**WP5 Communication, dissemination, visibility, and impact**

### 4.2 Work packages, activities, resources and timing

## WORK PACKAGES


### Work packages

*This section concerns a detailed description of the project activities.*


Group your activities into work packages. **A work package means a major sub-division of the project.** For each work package, enter an objective (expected outcome) and list the activities, milestones and deliverables that belong to it. The grouping should be logical and guided by identifiable deliverables/outputs.

Projects should normally have a minimum of 2 work packages. WP1 should cover the management and coordination activities (meetings, coordination, project monitoring and evaluation, financial management, progress reports, etc.) and all the activities which are cross-cutting and therefore difficult to assign to another specific work package (do not try splitting these activities across different work packages). WP2 and further WPs should be used for the other project activities. You can create as many work packages as needed by copying WP1. The last WP should be dedicated to Impact and dissemination

Please refer to the Call document/Programme Guide for specific requirements concerning the number and the typology of work packages.

Work packages covering financial support to third parties () only allowed if authorised in the Call document/Programme Guide) must describe the conditions for implementing the support (for grants: max amounts per third party; criteria for calculating the exact amounts, types of activity that qualify (closed list), persons/categories of persons to be supported and criteria and procedures for giving support; for prizes: eligibility and award criteria, amount of the prize and payment arrangements).

 Enter each activity/milestone/output/outcome/deliverable only once (under one work package).

 Ensure consistence with the detailed budget table/calculator (if applicable). (n/a for prefixed Lump Sum Grants)

### Objectives

*List the specific objectives to which the work package is linked.*

### Activities and division of work (WP description)

*Provide a concise overview of the work (planned tasks). Be specific and give a short name and number for each task.*

*Show who is participating in each task: Coordinator (COO), and if applicable Beneficiaries (BEN), Affiliated Entities (AE), Associated Partners (AP) and others, indicating **in bold** the task leader.*

*Add information on other participants' involvement in the project e.g. subcontractors, in-kind contributions.*

#### Note:

*In-kind contributions: In-kind contributions for free are cost-neutral, i.e. cannot be declared as cost. Please indicate the in-kind contributions that are provided in the context of the work package.*

*The Coordinator remains fully responsible for the coordination tasks, even if they are delegated to someone else. Coordinator tasks cannot be subcontracted.*

*If there is subcontracting, please also complete the table below.*

### Milestones and deliverables (outputs/outcomes)

**Milestones** are control points in the project that help to chart progress (e.g. completion of a key deliverable allowing the next phase of the work to begin). Use them only for major outputs in complex projects, otherwise leave the section empty. Please limit the number of milestones by work package.

Means of verification are how you intend to prove that a milestone has been reached. If appropriate, you can also refer to indicators.

**Deliverables** are project outputs which are submitted to show project progress (any format). Refer only to major outputs. Do not include minor sub-items, internal working papers, meeting minutes, etc. It is recommended to limit the number of deliverables to max 10-15 for the entire project. You may be asked to further reduce the number during grant preparation.

For deliverables such as meetings, events, seminars, trainings, workshops, webinars, conferences, etc., enter each deliverable separately and provide the following in the 'Description' field: invitation, agenda, signed presence list, target group, number of estimated participants, duration of the event, report of the event, training material package, presentations, evaluation report, feedback questionnaire. @

For deliverables such as manuals, toolkits, guides, reports, leaflets, brochures, training materials etc., add in the 'Description' field: format (electronic or printed), language(s), approximate number of pages and estimated number of copies of publications (if any).

For each deliverable you will have to indicate a due month by when you commit to upload it in the Portal. The due month of the deliverable cannot be outside the duration of the work package and must be in line with the timeline provided below. Month 1 marks the start of the project and all deadlines should be related to this starting date.

The labels used mean:

Public — fully open (🚩 automatically posted online on the Project Results platforms)

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](#). For items classified under other rules (e.g. national or international organisation), please select the equivalent EU classification level.

## Work Package 1

### Work Package 1: Managing the Alliance for Innovation

**Duration:**

M1- M36

**Lead Beneficiary:**

DIGITALEUROPE (DE)

### Objectives

SO1: to create a long-term, sustainable partnership of key European stakeholders within the cybersecurity sector who will cooperate to develop and implement new strategic approach to address the cybersecurity skills mismatches.

More specific sub-objectives include:

- To ensure the overall management and effective monitoring of the project activities in administrative, technical, and financial terms
- To foster smooth collaboration among partners, preventing and managing potential risks and misunderstandings



- To guarantee quality content and ensure effective progress, synergies, and coherence during the implementation of the activities
- To coordinate the involvement of the experts of the project Advisory Board in different project activities

**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	Administrative and financial management	This task covers the overall administrative and financial management of the project. DE, as project coordinator, will ensure the efficient consortium partner management and coordination, financial allocation and instalments, and budget monitoring aligned with the Grant Agreement (GA).	DE	COO	No
T1.2	Project coordination and risk mitigation	This task covers several activities related to project management and risk mitigation. DE, as project coordinator, will ensure the coordination of the annual work plan in close collaboration with the work package leaders (WPL). It also includes knowledge transfer and technical assistance to WP activities, risk mitigation actions in collaboration with the project Steering Committee (SC), the implementation of efficient internal communication processes and tools to facilitate collaboration, as well as the organisation of transnational project meetings (TPM) online and in-person.	DE KTU, CCIS, IVSZ	COO BEN	No
T1.3	Reporting and quality assurance	This task covers the reporting and quality assurance activities of the project. It includes the periodical internal reporting cycles and contractual periodic reporting (progress, final) of the project. DE, as coordinator, will be liaising with EACEA and coordinating the production of the reports. A quality assurance (QA) plan with clear key performance indicators (KPI) and appropriate evaluation and monitoring measures, tools, and processes will be put in place. The results of the periodical QA assessments will be considered to continuously enhance the quality and impact of the project. All partners contribute by providing the necessary information and supporting documents to the coordinator (DE) for the proper completion of the reporting.	DE All full partners	COO BEN	No

T1.4	Advisory Board coordination	This task covers the management and coordination of the Advisory Board (AB) of the project. It includes the organisation of bi-annual online meetings and the coordination of the involvement of AB members in project activities such as the reviewing of outputs according to their expertise. Yearly, AB members will be invited to provide recommendations on project activities and share their expertise on specific aspects to improve the project's value proposition and impact.				DE  All associated partners	COO  AP	No
<b>Milestones and deliverables (outputs/outcomes)</b>								
Milestone No <small>(continuous numbering not linked to WP)</small>	Milestone Name	Work Package No	Lead Beneficiary	Description		Due Date <small>(month number)</small>	Means of Verification	
MS1	Transnational project meetings (TPM)	1	DE	Organisation of 4 in-person TPMs (including kick-off and final meeting) gathering representatives from each full partner organisations to take stock of the project progress and co-design/discuss activities.		Multiple: M1, M12, M24, M34	Minutes of the meetings	
Deliverable No <small>(continuous numbering linked to WP)</small>	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date <small>(month number)</small>	Description <small>(including format and language)</small>	
D1.1	Annual work plan	1	DE	R	SEN	Multiple: M1, M12, M24	Annual, operational work plans produced by DE and WPLs to present the active WP tasks, sub-tasks, and activities of the year ahead. They help to visualise and coordinate the work among involved partners including KPIs and timelines. // Electronic format, 10 pages, EN.	
D1.2	Annual project collaboration and risk management report	1	DE	R	SEN	Multiple: M12, M24, M36	Annual reports produced by DE with input from the SC and AB to present the main outcomes of TPMs and elaborate on the risk mitigation actions	

							and decisions taken, as well as their potential impact on the work plan and implemented/foreseen adaptations. // Electronic format, 10 pages, EN.
D1.3	Quality assurance plan	1	DE	R	SEN	M2	The quality assurance (QA) plan to present the QA and impact assessment procedures of the project. It will serve as a basis to periodically evaluate and further improve the overall impact of the project's results, outcomes, and outputs. // Electronic format, 25 pages, EN.

Estimated budget — Resources <i>(n/a for prefixed Lump Sum Grants)</i>														
Participant	Costs													
	A. Personnel		B. Subcontracting	C.1a Travel			C.1b Accommodation	C.1c Subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		E. Indirect costs	Total costs
[name]	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X grants	X EUR	X EUR	X EUR
[name]	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X prizes	X EUR	X EUR	X EUR
Total	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X grants X prizes	X EUR	X EUR	X EUR]

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

## Work Package 2

Work Package 2: Cybersecurity skills intelligence, forecast, and strategy					
<b>Duration:</b>	M1 - M12	<b>Lead Beneficiary:</b>	Kaunas University of Technology (KTU)		
<b>Objectives</b>					
<p>SO2: to improve the quality and relevance of cybersecurity education and training programmes through the identification of country-specific cyber skills mismatches and providing innovative skills need anticipation methodology (market/educational offering) in Belgium, Estonia, Slovenia, Hungary, Greece, Lithuania, and Spain.</p> <p>More specific sub-objectives include:</p> <ul style="list-style-type: none"> <li>To develop well-rounded, country-specific cybersecurity skills mismatches analysis uncovering the critical gaps between the market needs and education and training offering, using a common skills framework and research methodology to ensure scalability, quality, and comparability of the results across the EU</li> <li>To provide a solid, innovative cybersecurity skills forecasting model supporting labour market and education and training actors to make informed decisions and reduce the risk of future mismatches and cybersecurity professional shortages</li> <li>To elaborate country-specific cybersecurity skills strategies to reduce the cybersecurity skills mismatches in the short, medium, and long-term</li> </ul>					
<b>Activities and division of work (WP description)</b>					
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)	
T2.1	Country-specific cybersecurity skills mismatches analysis (M1-M9)	This task covers the development of country-specific reports on the cybersecurity skills mismatches in Belgium, Estonia, Slovenia, Hungary, Greece, Lithuania, and Spain. All the CyberHubs will follow a common research methodology, produced by Breyer Publico, based on a multi-method approach (both quantitative and	DE  Breyer Publico  EIT Digital	COO  BEN  BEN  BEN	No

		<p>qualitative) including surveys, job vacancies scrapping (powered by the EIT Digital's Skills Academy Platform (SAP)), desk research, and expert focus groups. The mapping of skills and roles from the job vacancies and education and training programmes will follow the ENISA European Cybersecurity Skills Framework (ECSF). The country analysis will uncover the critical market needs in terms of cybersecurity skills and professional roles demand and the education and training programmes gaps. The reports will give an accurate picture of the country cybersecurity skills ecosystem maturity, opportunities, and peculiarities. This task also ensures that EIT Digital will be able to populate the tool with existing cybersecurity education and training programmes into the platform to anticipate the piloting of the SAP at the national level in T4.3.</p>	<p>All CyberHub partners: AGORIA, SBSEM, Howest, ITL, TalTech, CCIS, UM, IVSZ, NKE, SEPE, AUEB-RC, Infobalt, KTU, AMETIC, UNIR</p>		
T2.2	Cybersecurity skills forecasting model (M3-M12)	<p>This task aims to deliver a cybersecurity skills and roles forecasting model for long-term implementation. It will be a method for the anticipation of future cybersecurity professional skills and roles demand and supply to mitigate possible and labour market imbalances. It supports the education and training providers and labour market actors in making informed decisions. Breyer Publico will lead on the development of the forecasting model. The data to forecast cybersecurity skills demand and supply will come from a number of sources such as trends in job vacancy analysis, CEDEFOP occupational forecasts, other forecasts of market trends and expert groups. The ECSF adoption within the forecasting model will significantly benefit the comprehensiveness of the results and subsequent actions to be taken. All CyberHub partners contribute to its development to ensure that all relevant aspects, also on a national level, will be considered in the model.</p>	<p><b>Breyer Publico</b></p> <p>All CyberHub partners: AGORIA, SBSEM, Howest, ITL, TalTech, CCIS, UM, IVSZ, NKE, SEPE, AUEB-RC, Infobalt, KTU, AMETIC, UNIR</p>	<p><b>BEN</b></p> <p>BEN</p>	No

		The specific elements of the forecasting model will be tested and validated over the project lifetime (T4.3). In the long-term, the forecasting model can be used by the CyberHub consortium members and EU-wide as a whole (foreseen as part of the sustainability and exploitation plan) to produce their country-specific cybersecurity skills forecasts on a regular basis.				
T2.3	Country-specific cybersecurity skills strategy (M9-M12)	<p>This task covers the elaboration of country-specific cybersecurity skills strategies to reduce the cybersecurity skills mismatches in the short, medium, and long-term. It will build on the results of the cybersecurity skills mismatches analysis of T2.1, the already existing documentation and studies (e.g., the European Cybersecurity Skills Strategy of the blueprint project REWIRE, and the cybersecurity skills forecast model (T2.2) to define specific approaches that are country relevant and viable, and involve the essential ecosystem players (mapping of national actors active in the cybersecurity field) to drive efficient, innovative, systemic cybersecurity upskilling and reskilling in the country.</p> <p>KTU will benchmark the existing documentation and studies on cybersecurity skills development at the EU level and coordinate the alignment actions with regards to relevant European frameworks and tools such as the ENISA's European Cybersecurity Skills Framework (ECSF), ESCO, and Europass opportunities. All CyberHubs will produce a country strategy following guidance provided by KTU, Breyer Publico, and DE.</p>	<b>KTU</b>  Breyer Publico  DE  All CyberHub partners: AGORIA, SBSEM, Howest, ITL, TalTech, CCIS, UM, IVSZ, NKE, SEPE, AUEB-RC, Infobalt, AMETIC, UNIR	<b>BEN</b>  BEN  COO  BEN	No	
Milestones and deliverables (outputs/outcomes)						
Milestone No  (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description	Due Date  (month number)	Means of Verification

MS2	Research methodology	2	Breyer Publico	Elaboration of a common research methodology to identify country-specific cybersecurity skills mismatches using different methods. The methodology will be followed by all CyberHubs to ensure quality and comparability of results at EU level.			M3	Timely delivery
Deliverable No (continuous numbering linked to WP)	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month number)	Description (including format and language)	
D2.1	Cybersecurity skills mismatches analysis	2	DE	R	PU	M9	7 country reports on the cybersecurity skills mismatches in Belgium, Estonia, Slovenia, Hungary, Greece, Lithuania, and Spain based on a common research methodological approach. // Electronic format, 30 pages, EN and local languages.	
D2.2	Cybersecurity skills Forecasting model	2	Breyer Publico	R	PU	M12	Report to propose a novel methodological framework for forecasting demand for cybersecurity skills across EU countries and matching this against the educational offer. // Electronic format, 30 pages, EN	
D2.3	Country-specific cybersecurity skills strategies	2	KTU	R	PU	M12	7 country-specific strategies to address the cybersecurity skills mismatches in the short, medium and long-term. // Electronic format, 20 pages, EN and local languages.	

Estimated budget — Resources <i>(n/a for prefixed Lump Sum Grants)</i>										
Participant	Costs									
	A. Personnel	B. Subcontracting	C.1a Travel	C.1b Accommodation	C.1c Subsistence	C.2 Equipment	C.3 Other goods, works	D.1 Financial support to third parties	E. Indirect costs	Total costs



										and services				
[name]	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X grants	X EUR	X EUR	X EUR
[name]	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X prizes	X EUR	X EUR	X EUR
Total	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X grants X prizes	X EUR	X EUR	X EUR]

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

### Work Package 3

<b>Work Package 3: National Cybersecurity Skills Hubs for Innovation</b>			
<b>Duration:</b>	M9 – M36	<b>Lead Beneficiary:</b>	Chamber of Commerce and Industry of Slovenia (CCIS)
<b>Objectives</b>			
<p>SO1: to create a long-term, sustainable partnership of key European stakeholders within the cybersecurity sector who will cooperate to develop and implement new strategic approach to address the cybersecurity skills mismatches.</p> <p>SO3: to foster the development of national cyber skills incubators (i.e., the “CyberHubs”) across the EU, promoting cyber skills development, innovation, and entrepreneurship.</p> <p>SO4: to facilitate knowledge transfer, the exchange of good practices and information between higher education institutions, vocational education and training, and the business sector in the field of cybersecurity.</p> <p>More specific sub-objectives include:</p> <ul style="list-style-type: none"> <li>To establish national cybersecurity incubators (i.e., the “CyberHubs”) across the EU, promoting cybersecurity skills development, innovation, and entrepreneurship</li> </ul>			

- To improve knowledge transfer and accelerate the exchange of good practices between education, industry, and the public actors in the field of cybersecurity
- To ensure the EU-wide exploitation of the project results, develop a financial sustainability approach for the CyberHubs, and develop relevant collaboration avenues with existing projects, initiatives, and actors in the cybersecurity field

**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	Setting up, developing, and sustaining National CyberHubs (M9-M15)	<p>This task covers the establishment and sustainable development of solid innovation ecosystems focused on skills in the cybersecurity field — the CyberHubs — in 7 countries (Belgium, Estonia, Slovenia, Hungary, Greece, Lithuania, and Spain). All CyberHubs (industry-education pairs) will collaborate to define their CyberHub modus operandi including:</p> <ul style="list-style-type: none"> <li>• Developing the <b>CyberHub collaboration processes and structure</b> at the national level (inc. the organisation of CyberHub quarterly meetings)</li> <li>• Establishing the <b>governance of the CyberHub</b> including a <b>sustainability and exploitation strategy</b> (inc. mapping of national and EU funding opportunities, invitations to key actors identified within T2.3)</li> <li>• Developing <b>an action plan</b> for the delivery of the CyberHub services (inc. KPIs) stemming from the national cybersecurity skills strategies (D2.2).</li> </ul> <p>It is to be noted that CyberHubs will consult students and student entrepreneurs to validate their needs and action plans and ensure the CyberHub can answer to their needs. DE will support the task to ensure an</p>	<b>CCIS</b>  DE  All CyberHub partners: AGORIA, SBSEM, Howest, ITL, TalTech, UM, IVSZ, NKE, SEPE, AUEB-RC, Infobalt, AMETIC, UNIR	<b>BEN</b>  COO  BEN	No

		overall coherence between the CyberHubs and at the EU level.			
T3.2	Knowledge transfer activities (M9-M18)	<p>This task aims to ensure efficient knowledge transfer and the exchange of innovative practices between the CyberHubs so they can support each other's development and considerably reduce the learning curve. This task builds on the expertise of the two cybersecurity champion industry partners — Numeum and MTU (representing Cyber Ireland) who both have already well-established collaboration at the national level (France and Ireland) with industry, academia, start-ups, and government in the field of cybersecurity and Adecco which has longstanding expertise in VET and employment services. The knowledge transfer activities foreseen include:</p> <ul style="list-style-type: none"> <li>• <b>CyberHub country delegation visits</b> to Champion partners. The 7 delegations will be composed of two representatives from the CyberHub partners (1 industry and 1 education representative). The visits will aim to present the functioning of the Campus Cyber (Numeum) and Cyber Ireland's cluster (MTU). The detailed scope of the delegation visits will be developed and prepared by Numeum, in collaboration with Cyber Ireland.</li> <li>• A <b>CyberHub Twinning programme</b> to support the actual implementation and adoption of practices/services under WP4. The twinning will focus on practices which have organically been developed as a good practice in a specific organisation/region/country (originator) within and beyond the partnership and are then being transferred to another (adopter) a.k.a. the CyberHubs. All CyberHubs (7 twinings) will be able to take part in the twinning programme with the aim to strengthen transnational cooperation for cybersecurity skills development, create synergies and fostering capacity to develop educational projects in higher education and VET, drive</li> </ul>	<p><b>Numeum</b></p> <p>MTU</p> <p>Adecco</p> <p>All CyberHub partners: AGORIA, SBSEM, Howest, ITL, TalTech, CCIS, UM, IVSZ, NKE, SEPE, AUEB-RC, Infobalt, AMETIC, UNIR</p>	<p><b>BEN</b></p> <p>BEN</p> <p>BEN</p> <p>BEN</p>	No

		innovation and sustainable development in the cybersecurity field.						
T3.3	Alliance sustainability and exploitation strategy (M9-M36)	This task covers the design of a solid sustainability and exploitation strategy for the CyberHub Alliance for Innovation. DE, together with the WPLs, cybersecurity champion partners, Adecco, and Breyer Publico will develop a report including the identification of key exploitable results (KER) and ways to exploit them in the long-term, the investigation of funding opportunities at the local and EU level to ensure financial sustainability, a proposed model for expansion and other sustainability measures. The proposed strategy will be further reviewed and validated throughout the project duration and according to the input provided by the CyberHubs in their national CyberHub Governance and Sustainability strategies (D3.1). This task also includes the definition and implementation of collaboration avenues with relevant organisations, projects, and initiatives — such as ENISA, ECCC, ECCO, the Cybersecurity Skills Academy, EDHIs, DSJP, NCCs, ECSO, the REWIRE project, and more — to increase the relevance and impact of the project results and outputs.			DE  KTU, CCIS, IVSZ, Numeum, MTU, Breyer Publico, Adecco		COO  BEN	No
Milestones and deliverables (outputs/outcomes)								
Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description		Due Date (month number)	Means of Verification	
MS3	National CyberHub action plans	3	CCIS	Strategic design of the actions, services, and practices of the 7 CyberHubs.		M15	CyberHub education and industry partners as well as student entrepreneurs validate the action plans.	
Deliverable No (continuous numbering	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month number)	Description (including format and language)	

linked to WP)							
D3.1	National CyberHub governance and sustainability strategies	3	CCIS	R	SEN	M12	7 CyberHub-specific reports detailing the collaboration processes and structure, governance and sustainability and exploitation strategy. They will define the modus operandi of each CyberHub. // Electronic format, 20 pages, EN
D3.2	CyberHub country delegation visits	3	Numeum	R	PU	M18	Report on the results and learnings of the CyberHub country delegation visits to the two cybersecurity champion partners. // Electronic format, 10 pages, EN.
D3.3	CyberHub Twinning Programme	3	ADECCO	R	PU	M18	Report on the results and learnings of the 7 CyberHub twinings. // Electronic format, 10 pages, EN.
D3.4	Alliance sustainability and exploitation strategy	3	DE	R	SEN	Multiple: M12, M24, M36	Report (updated each year) to define the sustainability and exploitation strategy of the Alliance. // Electronic format, 10 pages, EN.

Estimated budget — Resources <i>(n/a for prefixed Lump Sum Grants)</i>														
Participant	Costs													
	A. Personnel		B. Subcontracting	C.1a Travel			C.1b Accommodation	C.1c Subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		E. Indirect costs	Total costs
[name]	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X grants	X EUR	X EUR	X EUR

[name]	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X prizes	X EUR	X EUR	X EUR
Total	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X grants X prizes	X EUR	X EUR	X EUR
For certain Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see <a href="#">Portal Reference Documents</a> ).														

#### Work Package 4

Work Package 4: CyberHub Services			
<b>Duration:</b>	M12 - M36	<b>Lead Beneficiary:</b>	ICT Association of Hungary (IVSZ)
Objectives			
<p>SO5: to increase the number of cybersecurity professionals in Europe by matching skills supply and job demand, engaging key players at the national and EU level, and attracting and retaining more talents in the cybersecurity field in Europe.</p> <p>SO6: to promote an entrepreneurial mindset as well as diversity and inclusion in the field of cybersecurity by engaging youth and addressing underrepresented groups in the ICT industry in Europe.</p> <p>SO7: to increase awareness and understanding of cybersecurity threats and good practices for cyber resilience among the general public.</p> <p>More specific sub-objectives include:</p> <ul style="list-style-type: none"> <li>To build the capacity in and raise awareness about cybersecurity with the aim to increase the number of cybersecurity professionals, and attract and retain EU talents</li> <li>To foster an entrepreneurial mindset as well as ensure diversity and inclusion in the field of cybersecurity through the engagement of youth and underrepresented groups in relevant activities</li> <li>To pilot a cutting edge platform aiming to match EU citizens' skills with jobs in the cybersecurity field</li> </ul>			

Activities and division of work (WP description)					
Task No <small>(continuous numbering linked to WP)</small>	Task Name	Description	Participants		In-kind Contributions and Subcontracting <small>(Yes/No and which)</small>
			Name	Role <small>(COO, BEN, AE, AP, OTHER)</small>	
T4.1	Cybersecurity skills awareness raising, stakeholder engagement, and capacity-building activities (M15-M36)	<p>This task aims to implement awareness raising, stakeholder engagement, and capacity-building activities/workshops. The design of the activities aims to strengthen the impact of and work in synergy with the actions and services mapped in CyberHub action plan (MS5), while considering the country perspective (D.2.3). The awareness raising and capacity-building activities will be designed to offer value added to a wide range of individuals from cybersecurity professionals to C-level workers, to SMEs, to academic staff and student entrepreneurs. They will aim to have an inclusive reach towards underrepresented groups in the cybersecurity field such as women and girls. The activities (online, in-person, or hybrid) will be delivered in a multimodal way, when possible, to widen participation and increase flexibility. All CyberHubs will choose whether to offer the workshops in the national language or in English. Examples of the type of activities foreseen include but are not limited to:</p> <ul style="list-style-type: none"> <li>• (Joint) talks and workshops by education and industry players</li> <li>• Cybersecurity readiness sessions and awareness raising</li> <li>• Design thinking workshops and/or coaching</li> <li>• Career fairs</li> <li>• Tandem meetings for a practical sharing of experience and skills in the sector</li> </ul> <p>The task also includes stakeholder engagement activities such as organising roundtables with relevant actors at the national level to discuss cybersecurity employment trends, skills and jobs, innovation cafés to gather education and training and industry representatives to discuss talent retention, skills mismatches and public-private partnerships, etc.</p>	<b>IVSZ</b>  Adecco MTU Numeum  All CyberHub partners: AGORIA, SBSEM, Howest, ITL, TalTech, CCIS, UM, NKE, SEPE, AUEB-RC, Infobalt, AMETIC, UNIR	<b>BEN</b>  BEN BEN BEN  BEN	No



		IVSZ is leading the task and develop processes to log and evaluate the performance of the activities. Adecco will ensure the VET perspective is taken into account when designing activities and MTU and Numeum will provide their expertise. All CyberHubs will implement a set of 10 activities throughout the duration of this task.			
T4.2	European Cybersecurity Hackathon (M9-M23)	<p>This task covers the preparations and organisation of an online European Cybersecurity Hackathon (during the month of October—"European Cybersecurity Month") to gather student entrepreneurs and students from a wide range of fields, e.g., engineering, economics, social sciences, who are interested in cybersecurity to solve real-world problems. The challenges will be proposed and sponsored by organisations and the CyberHub ecosystems under various pillars. The competitors will be able to deepen their understanding of today's cybersecurity challenges and contribute with their ideas to the development of solutions that can be brought to life in the medium to long-term.</p> <p>Groups of 3 to 5 participants will be given a real problem to solve in real time, working together in an international team. Clear, inclusive, transparent selection and awarding criteria will be elaborated. The challenges will be relevant to the persons expertise allowing them to combine their complementary background and interests.</p> <p>NKE, supported by UM, Adecco, will coordinate the conceptualisation of the Hackathon and manage the organisational and logistical aspects. The task involves the establishment of the jury, composed of experts and financial investors in the field of cybersecurity supported by MTU and Numeum. NKE will create a team of mentors, who will provide the competitor teams with guidance on how to take their ideas further during and after the competition.</p>	<p><b>NKE</b></p> <p>UM</p> <p>Adecco</p> <p>MTU</p> <p>Numeum</p> <p>All CyberHub partners: AGORIA, SBSEM, Howest, ITL, TalTech, CCIS, IVSZ, SEPE, AUEB-RC, Infobalt, AMETIC, UNIR</p>	<p><b>BEN</b></p> <p>BEN</p> <p>BEN</p> <p>BEN</p> <p>BEN</p>	No
T4.3	Piloting of a national AI-assisted system to match skills and jobs and forecasting model testing (M12-M36)	This task covers the testing of the cybersecurity skills forecasting model and piloting of the EIT Digital SAP — an AI-assisted tool designed to match skills and jobs — in the 7 countries represented by the CyberHubs. The platform will be piloted with 140 users (20 per CyberHub). The rationale is for the CyberHubs to be able to offer a fully researched service to match the individuals' skills with cybersecurity jobs as well as to be able to anticipate the cybersecurity skills and roles demand in their country.	<p><b>EIT Digital</b></p> <p>Breyer Publico</p> <p>All CyberHub partners: AGORIA, SBSEM, Howest, ITL, TalTech,</p>	<p><b>BEN</b></p> <p>BEN</p> <p>BEN</p>	No

		<p>The anonymised skills-matching solution enables a candidate to be discovered in a skills-first job and career-matching process that supports inclusivity. The candidates will be able to proactively apply for any great matches. This element will help (future) professionals to identify the most suitable career path based on their current skills and interests as well as the skills they will upskill or reskill. Equally, the recruiters will see anonymised skills-based matches and on that basis, they can decide to invite the candidate into the process bypassing any subconscious hiring bias, and in turn, supporting diversity and inclusion. SAP supports, in an innovative way, a student-centred learning approach offering personalised learning recommendations over 100+ learning and development programmes integrated and further populated in T2.1. The platform provides a seamless medium to measure the current skills in supply and an opportunity for the students to upskill or reskill for a desired role or position in the cybersecurity field.</p> <p>EIT Digital will provide the technical and operational assistance to all CyberHubs.</p> <p>Within this task, the CyberHubs will also test and validate specific elements of the cybersecurity skills forecasting model (D2.2) with the guidance of Breyer Publico. These elements include trends in the job vacancy analysis and input from reports, but also a test on how expert groups can contribute to improving the forecasting results of the model. Near the end of year 2 and year 3 it will be evaluated if the model is predicting the right trend based on the results of year 1 and year 2. The result of this sub-task will be a refined cybersecurity skills forecasting model.</p>	CCIS, UM, IVSZ, NKE, SEPE, AUEB-RC, Infobalt, AMETIC, UNIR			
Milestones and deliverables (outputs/outcomes)						
Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description	Due Date (month number)	Means of Verification
MS4	Completed piloting of the EIT Digital's Skills Academy Platform (SAP)	4	EIT Digital	The 7 CyberHubs have completed the piloting of the SAP in their country.	M36	140 users (20 per CyberHub) on the SAP.

Deliverable No (continuous numbering linked to WP)	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month number)	Description (including format and language)
D4.1	Cybersecurity workshops impact assessment	4	IVSZ	R	PU	Multiple: M24, M36	Yearly impact assessment report on the awareness raising, stakeholder engagement, and capacity-building activities across the 7 CyberHubs. // Electronic format, 10 pages, EN.
D4.2	European Cybersecurity Hackathon	4	NKE	OTHER (event)	PU	M22	Online European Cybersecurity Hackathon gathering pan-European, multi-disciplinary teams to solve real-world problems in the cybersecurity field.
D4.3	Skills Academy Platform's User Manual and capacity-building	4	EIT Digital	R	PU	M13	User Manual detailing how to use the functionalities and navigate the EIT Digital's Skills Academy Platform and capacity building to the CyberHubs. // Electronic format, 15 pages, EN.

Estimated budget — Resources <i>(n/a for prefixed Lump Sum Grants)</i>										
Participant	Costs									
	A. Personnel	B. Subcontracting	C.1a Travel	C.1b Accommodation	C.1c Subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties	E. Indirect costs	Total costs

[name]	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X grants	X EUR	X EUR	X EUR
[name]	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X prizes	X EUR	X EUR	X EUR
Total	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X grants X prizes	X EUR	X EUR	X EUR
For certain Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see <a href="#">Portal Reference Documents</a> ).														

### Work Package 5

Work Package 5: Communication, dissemination, visibility and impact			
Duration	M1 - M36	Lead Beneficiary:	DIGITALEUROPE (DE)
Objectives			
<p>SO4: to facilitate knowledge transfer, the exchange of good practices and information between higher education institutions, vocational education and training, and the business sector in the field of cybersecurity.</p> <p>SO6: to promote an entrepreneurial mindset as well as diversity and inclusion in the field of cybersecurity by engaging youth and addressing underrepresented groups in the ICT industry in Europe.</p> <p>SO7: to increase awareness and understanding of cybersecurity threats and good practices for cyber resilience among the general public.</p> <p>More specific sub-objectives include:</p> <ul style="list-style-type: none"> <li>To ensure the widespread dissemination of the project outputs and results during the project's lifetime</li> <li>To increase the impact of the project activities and EU-wide uptake of the outputs by the project's target groups</li> </ul>			

<ul style="list-style-type: none"> <li>To ensure high visibility for the CyberHubs at the EU and national level</li> <li>To raise awareness about cybersecurity and further the exchange of good practices for cybersecurity resilience</li> </ul>					
Activities and division of work (WP description)					
Task No <small>(continuous numbering linked to WP)</small>	Task Name	Description	Participants		In-kind Contributions and Subcontracting <small>(Yes/No and which)</small>
			Name	Role <small>(COO, BEN, AE, AP, OTHER)</small>	
T5.1	Alliance communication and dissemination coordination (M1-M36)	<p>This task covers all the aspects related to the communication and dissemination of the project including:</p> <ul style="list-style-type: none"> <li>Defining and developing the <b>CyberHub brand</b> concept, strategy, and visual identity.</li> <li>Developing a <b>communication and dissemination plan</b> including audience segmentation, key messages, promotional strategy, communication tools.</li> <li>Setting up <b>key performance indicators</b> (KPIs) and internal dissemination processes for implementation and reporting.</li> <li>Setting up and management of the <b>external project communication channels</b> including the project website.</li> <li>Delivering <b>communication packages and visual templates</b> for the CyberHubs to facilitate efficient communication activities.</li> <li>Supporting WPs where needed for optimal delivery and publication of the outputs/results.</li> </ul>	DE	COO	No
T5.2	CyberHubs visibility and impact at the national and EU level (M1-M36)	<p>This task aims at ensuring the widespread visibility and impact of the CyberHubs at the national and EU level. At the national level, CyberHubs, in particular business associations, will coordinate and implement communication and dissemination activities in the local language to reach the local communities and ensure impact. It includes, but is not limited to, regular <b>publishing of information</b> about the</p>	<p>DE</p> <p>All CyberHub partners: AGORIA, SBSEM, Howest, ITL,</p>	<p>COO</p> <p>BEN</p>	No

		<p>CyberHubs and their activities on different platforms including their own websites and social media channels (using the common CyberHub branding), <b>leveraging the relevant, established national channels of communication</b> such as the National Coalition for Digital Skills and Jobs platforms in each represented countries (where CCIS, IVSZ, and AMETIC are already leading their respective coalitions), <b>linking their activities with the work of the national nodes of the European Digital Innovation Hubs</b> (especially those focused on cybersecurity in Spain, Slovenia, Lithuania, Hungary, Belgium, and Greece), <b>running communication campaigns</b> to raise awareness about cybersecurity, <b>sending regular briefs to engaged stakeholders</b> on the CyberHub activities, and <b>organising a national conference</b> (1 per CyberHub) to gather the key players in the cybersecurity field to discuss topical issues related to education and cybersecurity policies, and industry-education cooperation in the field of cybersecurity.</p> <p>At the EU level, a large-scale “<b>European Cybersecurity Fest</b>” will be organised by Infobalt (final conference) to showcase and discuss the CyberHubs’ achievements and key benefits for member states and society at large with EU key players including policymakers, and industry and education representatives. DE will ensure representation to relevant third-party conferences such as the annual European Cybersecurity Conference where the <b>learnings and strategic dimensions will be highlighted and transferred</b> to ensure other actors can benefits from the project in the long-term — this activity will be linked to the long-term sustainability and exploitation strategy of the Alliance under WP3.</p>	TalTech, CCIS, UM, IVSZ, NKE, SEPE, AUEB-RC, Infobalt, AMETIC, UNIR			
Milestones and deliverables (outputs/outcomes)						
Milestone No (continuous numbering not linked to WP)	Milestone Name	Work Package No	Lead Beneficiary	Description	Due Date (month number)	Means of Verification
MS5	Communication Performance analysis reports	5	DE	Annual reporting consisting of measuring and analysing the marketing results of the communication activities (at the	Multiple: M12, 24, 36	All CyberHub have filled in the reporting tool in time to perform the analysis.

				national and EU level). It will inform the further development and adaptations of activities.			
Deliverable No (continuous numbering linked to WP)	Deliverable Name	Work Package No	Lead Beneficiary	Type	Dissemination Level	Due Date (month number)	Description (including format and language)
D5.1	Project communication and dissemination plan	5	DE	R	PU	M5	The communication and dissemination plan sets a clear framework that ensures consistent and coherent communication and dissemination activities throughout the project's lifetime. // Electronic format, 20 pages, EN
D5.2	Project website and other communication tools	5	DE	R	PU	M8	The project website and other communication tools and channels (e.g., social media, videos...) will serve the project dissemination and outreach activities during the project's lifetime. // Electronic format, EN
D5.3	European Cybersecurity Fest	5	Infobalt	OTHER (event)	PU	M34	The European Cybersecurity Fest will serve as the final conference of the project and will be organised during October 2026 ("European Cybersecurity Month"). // EN

**Estimated budget — Resources** *(n/a for prefixed Lump Sum Grants)*



Participant	Costs													
	A. Personnel		B. Subcontracting	C.1a Travel			C.1b Accommodation	C.1c Subsistence	C.2 Equipment	C.3 Other goods, works and services	D.1 Financial support to third parties		E. Indirect costs	Total costs
	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X grants	X EUR	X EUR	X EUR
	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X prizes	X EUR	X EUR	X EUR
Total	X person months	X EUR	X EUR	X travels	X persons travelling	X EUR	X EUR	X EUR	X EUR	X EUR	X grants X prizes	X EUR	X EUR	X EUR]
For certain Lump Sum Grants, see detailed budget table/calculator (annex 1 to Part B; see <a href="#">Portal Reference Documents</a> ).														

Staff effort (n/a for Lump Sum Grants)

Staff effort per work package						
Fill in the summary on work package information and effort per work package.						
Work Package No	Work Package Title	Lead Participant No	Lead Participant Short Name	Start Month	End Month	Person-Months
1	Managing the Alliance for Innovation	P1	DE	M1	M36	48

2	Cybersecurity skills intelligence, forecast, and strategy	P14	KTU	M1	M12	55
3	National Cybersecurity Skills Hubs for Innovation	P7	CCIS	M9	M36	73
4	CyberHub Services	P9	IVSZ	M9	M36	98
5	Communication, dissemination, visibility and impact	P1	DE	M1	M36	36
					Total Months      Person-	310

**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	WP1	WP2	WP3	WP4	WP5	Total Person-Months
DE	13	5	6	2	9	35
AGORIA	2	2	2	3	2	11

SBSEM	1	1	2	2	1	7
HOWEST	1	1	2	2	1	7
ITL	2	3	5	8	3	21
TalTech	1	2	3	3	1	10
CCIS	2	2	8	5	2	19
UM	2	2	3	5	1	13
IVSZ	3	3	6	15	3	30
NKE	2	3	4	14	1	24
SEPE	2	4	4	5	3	18
AUEB-RC	2	3	4	5	1	15
Infobalt	2	3	4	5	4	18
KTU	3	4	3	3	1	14
AMETIC	2	3	4	5	2	16
UNIR	2	2	2	2	1	9
Numeum	1	0	4	1	0	6
MTU	1	0	3	3	0	7
Breyer Publico	2	8	1	1	0	12

Adecco	1	4	0	6	0	11
Total Person-Months	48	55	73	98	36	310

### 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 to have sufficient operational capacity to implement the project activities themselves. Subcontracting should therefore be exceptional.

Include only subcontracts that comply with the rules (i.e. best value for money and no conflict of interest; no subcontracting of project coordination 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?)
N/A	N/A	N/A	N/A	N/A	N/A	N/A
Other issues: <i>If subcontracting for the project goes beyond 30% of the total eligible costs, give specific reasons.</i>			N/A			

### Events meetings and mobility

#### Events meetings and mobility

This table is to be completed for events meetings and mobility that have been mentioned as part of the activities in the work packages above

Give more details on the type, location, number of persons attending, etc.

Event No (continuous numbering linked to WP)	Participant	Description					Attendees
		Name	Type	Area	Location	Duration (days)	Number
E1.1	Organiser: DE Attendees: All	Kick-off meeting	Transnational project meeting	Meeting to manage the implementation of the project.	Brussels, Belgium	1	22
E1.2	Organiser: CCIS Attendees: All partners	1 <sup>st</sup> Progress meeting	Transnational project meeting	Meeting to manage the implementation of the project.	Ljubljana, Slovenia	1	22
E1.3	Organiser: IVSZ Attendees: All partners	2 <sup>nd</sup> Progress meeting	Transnational project meeting	Meeting to manage the implementation of the project.	Budapest, Hungary	1	22
E1.4	Organiser: KTU Attendees: All partners	3 <sup>rd</sup> Progress meeting linked to final event	Transnational project meeting	Meeting to manage the implementation of the project. IT will be linked to the European Cybersecurity Fest. 2 days including the Fest.	Vilnius, Lithuania	1	22
E3.1	Organiser: Agoria, ITL, CCIS, IVSZ, SEPE, Infobalt, AMETIC Attendees: SBSEM, Howest, TalTech, UM, NKE, AUEB-RC, KTU, UNIR	CyberHubs' operative meetings	National quarterly meetings of the established CyberHubs	Regular meetings to launch and to operate the CyberHubs	Belgium, Estonia, Slovenia, Hungary, Greece, Lithuania and Spain.	0,5 days each	5-10 per country, per meeting
E3.2	Hosts: Numeum, MTU Attendees: Agoria, ITL, CCIS, IVSZ, SEPE, Infobalt, AMETIC SBSEM, Howest, TalTech, UM, NKE, AUEB-RC, KTU, UNIR	Country delegation visits	Knowledge exchange events	Meetings to understand the operation of the champion hubs and to develop capacity of the future hubs.	Cork, Ireland and Paris, France	2	at least 2 attendees/visit, at least 30 attendees in total

E3.3	Agoria, ITL, CCIS, IVSZ, SEPE, Infobalt, AMETIC SBSEM, Howest, TalTech, UM, NKE, AUEB-RC, KTU, UNIR	Twinning events	Knowledge Exchange events	Meetings to learn in detail about good practices and discuss their transferability potential.	CyberHub partners' locations, TBC in detail, exact location of each trip depends on the identified practices	1-2 days each	at least 2 attendees/twinning, at least 30 attendees in total
E4.1	Organiser: Agoria, ITL, CCIS, IVSZ, SEPE, Infobalt, AMETIC Contributors: DE, SBSEM, Howest, TalTech, UM, NKE, AUEB-RC, KTU, UNIR, Adecco	CyberHub events (10 per Hub)	National (hub) level capacity building, awareness raising and stakeholder engagement events	Events to fulfil the action plan of the CyberHubs, strengthen cooperation with stakeholders, offer capacity building for different target groups and awareness raising.	Belgium, Estonia, Slovenia, Hungary, Greece, Lithuania and Spain (online, in-person, and/or hybrid).	0,5-1 days each	10-50 participants per event // in total min 490 participants
E4.2	Organiser: NKE Contributors: DE, Agoria, ITL, CCIS, IVSZ, SEPE, Infobalt, AMETIC SBSEM, Howest, TalTech, UM, NKE, AUEB-RC, KTU, UNIR, Adecco	European Cybersecurity Hackathon	European CyberHubs Network joint event	European level online hackathon to solve real-world problems related to cybersecurity.	Online event	1-2 days	50-70 participants
E5.1	Organiser: Agoria, ITL, CCIS, IVSZ, SEPE, Infobalt, AMETIC Contributors: DE, SBSEM, Howest, TalTech, UM, NKE, AUEB-RC, KTU, UNIR, Adecco	National Cybersecurity Conference	National dissemination events	National events to discuss topical issues related to education and cybersecurity policies, and industry-education cooperation in the field of cybersecurity	Belgium, Estonia, Slovenia, Hungary, Greece, Lithuania and Spain.	1 day each	50 participants each // in total 350 participants
E5.2	Organiser: Infobalt Contributors: DE, Agoria, ITL, CCIS, IVSZ, SEPE, Infobalt, AMETIC, SBSEM, Howest, TalTech, UM,	European Cybersecurity Fest	European dissemination event	Final event to showcase and discuss the CyberHubs' achievements and key benefits for	Vilnius, Lithuania	1	150 participants

	NKE, AUEB-RC, KTU, UNIR			member states and society at large with EU key players. It will be linked to the final progress meeting. 2 days with the last progress meeting.			
--	-------------------------	--	--	---	--	--	--

*Timetable***Timetable (projects of more than 2 years)**

Fill in cells in beige to show the duration of activities. Repeat lines/columns as necessary.

**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	YEAR 1				YEAR 2				YEAR 3			
	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4	Q 1	Q 2	Q 3	Q 4
T1.1 - Administrative and financial management												
T1.2 - Project coordination and risk mitigation												
T1.3 - Reporting and quality assurance												
T1.4 - Advisory Board coordination												
T2.1 - Country-specific cybersecurity skills mismatches analysis												



T2.2. - Cybersecurity skills forecasting model												
T2.3 - Country-specific cybersecurity skills strategy												
T3.1 - Setting up, developing, and sustaining National CyberHubs												
T3.2 - Knowledge transfer activities												
T3.3 - Alliance sustainability and exploitation strategy												
T4.1 - Cybersecurity skills awareness raising, stakeholder engagement and capacity building activities												
T4.2 - European Cybersecurity Hackathon												
T4.3 - Piloting of National AI-assisted system to match skills and jobs and forecasting model testing												
T5.1 - Alliance communication and dissemination coordination												
T5.2 - CyberHubs visibility and impact at the national and EU level												

#\$WRK-PLA-WP\$#

#@ETH-ICS-EI@#

## 5. OTHER

### 5.1 Ethics

#### Ethics (if applicable)

*If the Call document/Programme Guide contains a section on ethics, describe ethics issues that may arise during the project implementation and the measures you intend to take to solve/avoid them.*

*Describe how you will ensure gender mainstreaming and children's rights in the project activities.*

##### 5.1.1. Potential ethics issues during the project implementation

As with any project that involves the collection, storage, and processing of data, there are potential ethics issues that may arise during the implementation of the CyberHubs project.

**Privacy concerns.** The project will involve the collection of personal data from participants in various activities such as the Hackathon, country delegation visits, and the AI Cybersecurity Skills Academy Platform. The project will need to ensure that the privacy of participants is protected and that their data is only used for the intended purposes of the project.

**Bias in data collection and analysis.** There is a risk of bias in the collection and analysis of data that could result in unfair or discriminatory outcomes. The project will need to ensure that data collection is unbiased and that any potential biases in data analysis are identified and addressed.

**Ethical considerations in AI.** The project will involve the development of an AI platform for cybersecurity skills management. There are ethical considerations in the development and deployment of AI, such as ensuring that the AI is transparent, accountable, and fair. The project will need to ensure that these ethical considerations are addressed in the development and deployment of the AI platform.

##### 5.1.2. Measures to address ethical issues in the project

To address these potential ethics issues, the CyberHubs project will take several measures, including:

1. Developing a privacy policy: the project will develop a privacy policy that outlines the types of data that will be collected, how the data will be used, and how it will be protected.
2. Establishing a code of ethics: the project will establish a code of ethics that outlines the ethical principles that will guide the project's activities.
3. Ensuring data collection and analysis are unbiased: the project will use best practices to ensure that data collection and analysis are unbiased, such as ensuring that data collection methods are standardized and that the analysis is conducted by qualified professionals.
4. Addressing ethical considerations in AI: the project will ensure that ethical considerations in the development and deployment of the AI platform are addressed by engaging with experts in the field and following established best practices.
5. Ensuring transparency and accountability: the project will ensure that its activities are transparent and accountable by regularly reporting on progress, engaging with stakeholders, and conducting evaluations of its activities.

##### 5.1.3. Ethical approach of the AI tool (high risk)

The platform ensures that ethical issues are managed through its anonymised skills-matching solution, which supports inclusivity and eliminates any subconscious hiring bias. This solution allows a candidate to be discovered in a skills-first job and career-matching process, enabling them to identify the most suitable career path based on their current skills, interests, and upskilling or reskilling goals and not revealing the personal identifiers to the recruiters until the interview process. The platform also ensures to provide a match is completely based on a candidate's competencies including both hard and human skills and working preferences with a 50% fit, allowing them to proactively apply for the best matches. Additionally, employers will only see anonymised skills-based matches, enabling them to make unbiased hiring decisions and support diversity and inclusion in their hiring processes. Overall, the platform's focus on skills-matching and inclusivity ensures that ethical issues are appropriately managed, creating a fair and equal opportunity for all.

As such, the platform conducts adequate risk assessment and mitigation systems before putting the solution on the market. The datasets feeding the system are of high quality to minimise risks and discriminatory outcomes. Logging of activity is done on a regular basis to ensure traceability of results, and detailed

documentation is provided with all necessary information on the system and its purpose for authorities to assess its compliance. Clear and adequate information is provided to all users, and they have access to request and download copies of their personal data at any time, and appropriate human oversight measures are in place to minimise risk. The system is of high robustness, security, and accuracy.

**5.1.4. Gender mainstreaming in the project activities**

Gender mainstreaming is a crucial aspect of the project, and the project team is committed to ensuring that gender equality is integrated throughout all project activities. The following measures will be taken to ensure gender mainstreaming in the project:

**Gender-disaggregated data collection.** The project team will collect gender-disaggregated data in all aspects of the project, including participant demographics, stakeholder engagement, and training activities. This data will be used to identify any gender gaps and ensure that the project is meeting the needs of all participants.

**Gender-sensitive communication.** The project team will use gender-sensitive language and imagery in all project communication and dissemination materials, including the project website, social media accounts, and promotional materials.

**Gender balance in project activities.** The project team will strive to ensure a gender balance in all project activities, including events, workshops, and meetings. This will be achieved by actively seeking the participation of women in all project activities and ensuring that all participants have equal opportunities to contribute.

**Gender-specific training.** The project team will develop gender-specific training materials, where appropriate, to address the specific needs and challenges faced by women in the cybersecurity sector. This may include training on topics such as work-life balance, career development, and overcoming gender biases.

**Gender-responsive monitoring and evaluation.** The project team will use a gender-responsive monitoring and evaluation framework to ensure that gender equality is integrated throughout the project cycle. This will involve regularly assessing the gender impact of project activities and making adjustments as needed to ensure that gender mainstreaming is being effectively implemented.

#§ETH-ICS-EI§# #@SEC-URI-SU@#

**5.2 Security**

Security
Not applicable.

#§SEC-URI-SU§# #@DEC-LAR-DL@#

**6. DECLARATIONS**

Double funding	
Information concerning other EU grants for this project	YES/NO
 Please note that there is a strict prohibition of double funding from the EU budget (except under EU Synergies actions).	
We confirm that to our best knowledge neither the project as a whole nor any parts of it have benefitted from any other EU grant (including EU funding managed by authorities in EU Member States or other funding bodies, e.g. Erasmus, EU Regional Funds, EU Agricultural Funds, etc). If NO, explain and provide details.	YES
We confirm that to our best knowledge neither the project as a whole nor any parts of it 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. Erasmus, EU Regional Funds, EU Agricultural Funds, etc). If NO, explain and provide details.	YES

<b>Financial support to third parties (if applicable)</b> <i>If your project requires a higher maximum amount per third party than the threshold amount set in the Call document/Programme Guide, justify and explain why this is necessary in order to fulfil your project's objectives.</i>
Not applicable.

<b>Seal of Excellence (if applicable)</b> <i>If provided in the Call document, proposals that pass the evaluation but are below the budget threshold (i.e. pass the minimum thresholds but are not ranked high enough to receive funding) will be awarded a Seal of Excellence.</i> <i>In this context we may share information about your proposal with other EU or national funding bodies through the Erasmus+ National Agencies.</i>	
Do you agree that your proposal (including proposal data and documentation) is shared with other EU and national funding bodies to find funding under other schemes?	YES

#§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](#)).





ANNEX 2

ESTIMATED BUDGET (LUMP SUM BREAKDOWN) FOR THE ACTION

Forms of funding	Estimated EU contribution					
	Estimated eligible lump sum contributions (per work package)					Maximum grant amount <sup>1</sup>
	WP1 Managing the Alliance for Innovation	WP2 Cybersecurity skills intelligence, forecast, and strategy	WP3 National Cybersecurity Skills Hubs for Innovation	WP4 CyberHub Services	WP5 Communication, dissemination, visibility and impact	
	Lump sum contribution	Lump sum contribution	Lump sum contribution	Lump sum contribution	Lump sum contribution	
	a	b	c	d	e	f = a + b + c + d + e
1 - DE	60 378.00	23 214.00	26 958.00	7 489.00	56 377.00	174 416.00
2 - AGORIA	15 704.00	15 405.00	16 916.00	26 488.00	16 218.00	90 731.00
3 - SBSEM	7 556.00	5 503.00	12 517.00	11 006.00	5 503.00	42 085.00
4 - HOWEST	7 556.00	5 503.00	12 517.00	11 006.00	5 503.00	42 085.00
5 - ITL	9 201.00	10 590.00	18 627.00	32 307.00	12 624.00	83 349.00
6 - TalTech	7 575.00	9 799.00	16 209.00	14 698.00	4 900.00	53 181.00
7 - CCIS	12 960.00	10 049.00	44 091.00	27 629.00	9 988.00	104 717.00
8 - UM	7 446.00	6 504.00	11 267.00	15 148.00	3 252.00	43 617.00
9 - IVSZ	9 816.00	7 857.00	16 273.00	47 729.00	9 474.00	91 149.00
10 - NKE	4 781.00	4 647.00	7 334.00	25 071.00	1 549.00	43 382.00
11 - SEPE	10 035.00	15 918.00	17 429.00	25 332.00	14 207.00	82 921.00
12 - AUEB-RC	6 603.00	6 650.00	10 377.00	11 083.00	2 216.00	36 929.00
13 - INFOBALT	9 503.00	12 555.00	16 667.00	24 476.00	28 978.00	92 179.00
14 - KTU	16 068.00	20 026.00	16 659.00	14 207.00	5 049.00	72 009.00
15 - AMETIC	10 200.00	15 161.00	19 145.00	27 823.00	10 095.00	82 424.00
16 - UNIR	11 700.00	11 502.00	11 502.00	13 012.00	5 751.00	53 467.00
17 - Numeum	9 522.00	0.00	29 097.00	6 846.00	0.00	45 465.00
18 - MTU	6 988.00	0.00	14 651.00	12 940.00	0.00	34 579.00
19 - Breyer Publico	11 977.00	56 381.00	6 239.00	6 239.00	0.00	80 836.00
20 - EIT DIGITAL	5 212.00	33 257.00	0.00	87 259.00	0.00	125 728.00
21 - ADECCO	5 829.00	0.00	9 461.00	9 461.00	0.00	24 751.00
22 - AAVIT						
23 - DTSL						
24 - IT Ukraine						
Σ consortium	246 610.00	270 521.00	333 936.00	457 249.00	191 684.00	1 500 000.00

<sup>1</sup> The 'maximum grant amount' is the maximum grant amount fixed in the grant agreement (on the basis of the sum of the beneficiaries' lump sum shares for the work packages).

**ANNEX 3**

**ACCESSION FORM FOR BENEFICIARIES**

**AGORIA ASBL (AGORIA)**, PIC 998981079, established in A REYERS 80 DIAMANT BUILDING, BRUXELLES 1030, Belgium,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**SOLVAY BRUSSELS SCHOOL LIFELONG LEARNING (SBSEM)**, PIC 882074448,  
established in AVENUE FRANKLIN ROOSEVELT 42 CP114/01, BRUXELLES 1050, Belgium,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**HOGESCHOOL WEST-VLAANDEREN HOWEST (HOWEST)**, PIC 998686684, established in MARKSESTEENWEG 58, KORTRIJK 8500, Belgium,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**EESTI INFOTEHNOLOOGIA JA TELEKOMMUNIKATSIOONI LIIT (ITL), PIC 935207556**, established in LOOTSA 6, TALLINN 11415, Estonia,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**TALLINNA TEHNIKAÜLIKOOL (TalTech)**, PIC 999842536, established in EHITAJATE TEE 5, TALLINN 19086, Estonia,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**GOSPODARSKA ZBORNICA SLOVENIJE (CCIS)**, PIC 999780165, established in DIMICEVA ULICA 13, LJUBLJANA 1000, Slovenia,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**UNIVERZA V MARIBORU (UM)**, PIC 999903646, established in SLOMSKOV TRG 15, MARIBOR 2000, Slovenia,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**IVSZ - DIGITALIS VALLALKOZASOK SZOVETSEGE (IVSZ)**, PIC 999794230, established in TINODI U 1-3. FSZT 2., BUDAPEST 1095, Hungary,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**NEMZETI KOZSZOLGALATI EGYETEM (NKE)**, PIC 943340812, established in LUDOVIKATER 2, BUDAPEST 1083, Hungary,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**FEDERATION OF HELLENIC INFORMATION TECHNOLOGY AND COMMUNICATION ENTREPRISES (SEPE)**, PIC 997352546, established in FRANTZI 19, ATHINA 117 43, Greece,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER (AUEB-RC)**, PIC 999896856, established in KEFALLINIAS STREET 46, ATHENS 11251, Greece,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**ASOCIACIJA INFOBALT (INFOBALT)**, PIC 970234450, established in GOSTAUTO STR. 8-313, VILNIUS LT-01108, Lithuania,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**KAUNO TECHNOLOGIJOS UNIVERSITETAS (KTU)**, PIC 999844961, established in K  
DONELAICIO 73, KAUNAS LT-44029, Lithuania,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**ASOCIACION MULTISECTORIAL DE EMPRESAS DE LA ELECTRONICA, LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACION, DE LAS TELECOMUNICACIONES Y DE LOS CONTENIDOS DIGITALES (AMETIC)**, PIC 968769750, established in CALLE PRINCIPE DE VERGARA 74, MADRID 28006, Spain,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA (UNIR)**, PIC 956152281, established in AVENIDA DE LA PAZ 137, LOGRONO 26006, Spain,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**NUMEUM (Numeum)**, PIC 882036618, established in 148 BD HAUSSMANN, PARIS 75008, France,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**MUNSTER TECHNOLOGICAL UNIVERSITY (MTU)**, PIC 892106673, established in ROSSA AVENUE BISHOPSTOWN, CORK T12 P928, Ireland,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**BREYER PUBLICO S.L. (Breyer Publico)**, PIC 881967554, established in C VERDAGUER 2, BARCELONA 08198, Spain,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**EIT DIGITAL (EIT DIGITAL)**, PIC 954616286, established in GUIMARDSTRAAT 7, BRUSSEL 1040, Belgium,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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**

**ADECCO FORMAZIONE SRL (ADECCO)**, PIC 919579789, established in VIA TOLMEZZO 15, MILANO 20132, Italy,

**hereby agrees**

**to become beneficiary**

**in Agreement No 101140030 — CyberHubs** ('the Agreement')

**between DIGITALEUROPE AISBL\* (DE) and the European Education and Culture Executive Agency (EACEA)** ('EU executive agency' or '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

FINANCIAL STATEMENT FOR THE ACTION FOR REPORTING PERIOD [NUMBER]

EU contribution												
Eligible lump sum contributions (per work package)												Requested EU contribution
	WP1 [name]	WP2 [name]	WP3 [name]	WP4 [name]	WP5 [name]	WP6 [name]	WP7 [name]	WP8 [name]	WP9 [name]	WP10 [name]	WP [XX]	
Forms of funding	[ Lump sum contribution// Financing not linked to costs]	[ Lump sum contribution// Financing not linked to costs]	[ Lump sum contribution// Financing not linked to costs]	[ Lump sum contribution// Financing not linked to costs]	[ Lump sum contribution// Financing not linked to costs]	[ Lump sum contribution// Financing not linked to costs]	[ Lump sum contribution// Financing not linked to costs]	[ Lump sum contribution// Financing not linked to costs]	[ Lump sum contribution// Financing not linked to costs]	[ Lump sum contribution// Financing not linked to costs]	[ Lump sum contribution// Financing not linked to costs]	
Status of completion	COMPLETED	COMPLETED	COMPLETED	COMPLETED	COMPLETED	COMPLETED	COMPLETED	PARTIALLY COMPLETED	PARTIALLY COMPLETED	COMPLETED	NOT COMPLETED	
	a	b	c	d	e	f	g	h	i	j	k	$l = a + b + c + d + e + f + g + h + i + j + k$
1 – [short name beneficiary]												
1.1 – [short name affiliated entity]												
2 – [short name beneficiary]												
2.1 – [short name affiliated entity]												
X – [short name associated partner]												
Total consortium												

The consortium hereby confirms that:

The information provided is complete, reliable and true.

The lump sum contributions declared are eligible (in particular, the work packages have been completed and the work has been properly implemented and/or the results were achieved; see Article 6).

The proper implementation of the action/achievement of the results 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, 21 and 25).



## **ANNEX 5**

### **SPECIFIC RULES**

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

##### **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, EU institutions, bodies, offices or agencies and national authorities 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.

The access rights also extend to national authorities of EU Member States or associated countries, for developing, implementing and monitoring their policies or programmes in this area. In this case, access is subject to a bilateral agreement to define specific conditions ensuring that:

- the access will be used only for the intended purpose and
- appropriate confidentiality obligations are in place.

Moreover, the requesting national authority or EU institution, body, office or agency (including the granting authority) must inform all other national authorities of such a request.

### **Access rights for third parties to ensure continuity and interoperability**

Where the call conditions impose continuity or interoperability obligations, the beneficiaries must make the materials, documents and information and results produced in the framework of the action available to the public (freely accessible on the Internet under open licences or open source licences).

## **COMMUNICATION, DISSEMINATION AND VISIBILITY (— ARTICLE 17)**

### **Additional communication and dissemination activities**

The beneficiaries must engage in the following additional communication and dissemination activities:

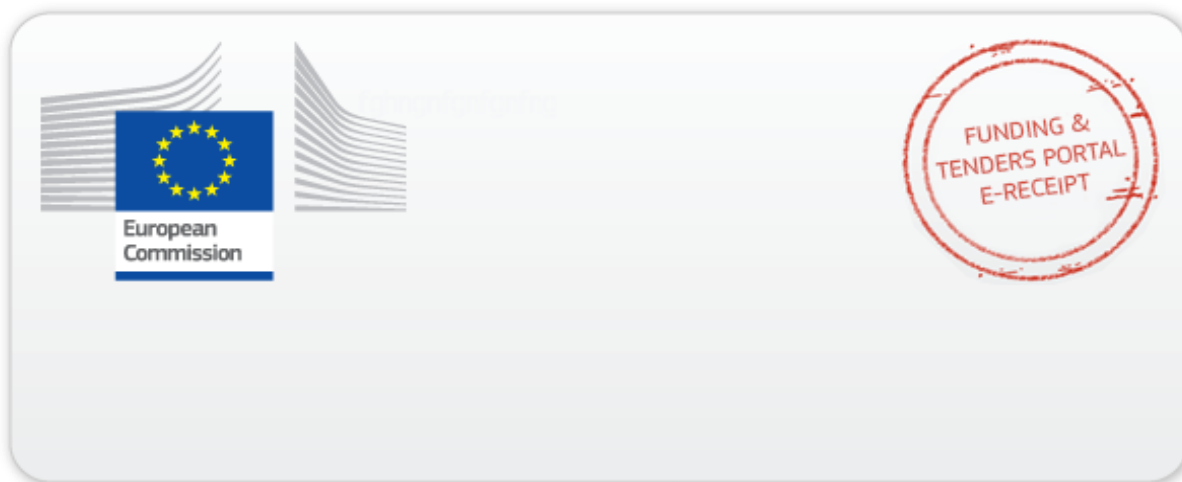
- **present the project** (including project summary, coordinator contact details, list of participants, European flag and funding statement and project results) on the beneficiaries' **websites** or **social media accounts**
- for actions involving public **events**, display signs and posters mentioning the action and the European flag and funding statement
- upload the public **project results** to the Erasmus+ Project Results platform, available through the Funding & Tenders Portal.

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

### **EU restrictive measures**

The beneficiaries must ensure that the EU grant does not benefit any affiliated entities, associated partners, subcontractors or recipients of financial support to third parties that are

subject to restrictive measures adopted under Article 29 of the Treaty on the European Union or Article 215 of the Treaty on the Functioning of the EU (TFEU).



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>)