



Council of the European Union  
General Secretariat

---

---

**Interinstitutional files:  
2018/0328(COD)**

---

---

**Brussels, 13 February 2019**

**WK 2142/2019 INIT**

**LIMITE**

**CYBER  
TELECOM  
CODEC  
COPEN  
COPS  
COSI  
CSC  
CSCI  
IND  
JAI  
RECH  
ESPACE**

### WORKING PAPER

*This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.*

### **WORKING DOCUMENT**

From:	The Swedish delegation
To:	Horizontal Working Party on Cyber Issues
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres - Comments from the Swedish delegation

Delegations will find in Annex comments from the Swedish delegation on the above mentioned proposal.

2018/0328 (COD)

Proposal for a

**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres**

*A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018*

**Commented [A1]:** SE is still hesitant towards the establishment of a new eu-body to fulfill the tasks of CCCN, both in terms of scale and scope. CCCN should be able to be incorporated by other existing eu-bodies as for example enisa. The main purpose of CCCN should be to coordinate and facilitate cyber security within the EU.

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,  
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 173(3) and the first paragraph of Article 188 thereof,

Having regard to the proposal from the European Commission,

Having regard to the opinion of the European Economic and Social Committee<sup>1</sup>,

Having regard to the opinion of the Committee of the Regions<sup>2</sup>,

Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) Our daily lives and economies become increasingly dependent on digital technologies, citizens become more and more exposed to serious cyber incidents. Future security depends, among others, on enhancing technological and industrial ability to protect the Union against cyber threats, as both civilian infrastructure and military capacities rely on secure digital systems.

---

<sup>1</sup> OJ C , , p. .

<sup>2</sup> OJ C , , p. .

- PUBLIC
- (2) The Union has steadily increased its activities to address growing cybersecurity challenges following the 2013 Cybersecurity Strategy<sup>3</sup> aimed to foster a reliable, safe, and open cyber ecosystem. In 2016 the Union adopted the first measures in the area of cybersecurity through Directive (EU) 2016/1148 of the European Parliament and of the Council<sup>4</sup> on security of network and information systems.
  - (3) In September 2017, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a Joint Communication<sup>5</sup> on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" to further reinforce the Union's resilience, deterrence and response to cyber-attacks.
  - (4) The Heads of State and Government at the Tallinn Digital Summit, in September 2017, called for the Union to become "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."
  - (5) Substantial disruption of network and information systems can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market. At the moment, the Union depends on non-European cybersecurity providers. However, it is in the Union's strategic interest to ensure that it retains and develops essential cybersecurity technological capacities to secure its Digital Single Market, and in particular to protect critical networks and information systems and to provide key cybersecurity services.
  - (6) A wealth of expertise and experience in cybersecurity research, technology and industrial development exists in the Union but the efforts of industrial and research communities are fragmented, lacking alignment and a common mission, which hinders competitiveness in this domain. These efforts and expertise need to be pooled, given support as a strategic asset and the possibilities to grow and gain competitiveness through supported networking and allocation of funds networked and by this used in an efficient manner to reinforce and complement existing research, technology and industrial capacities at Union and national levels.
  - (7) The Council Conclusions adopted in November 2017 called on the Commission to provide rapidly an impact assessment on the possible options to create a network of cybersecurity competence centres with the European Research and Competence Centre and propose by mid-2018 the relevant legal instrument.

**Commented [A2]:** A vast majority of this expertise and these efforts are today pooled and allocated to projects in the private sector that is being privately funded. Therefore, this is resources that cannot (easily) be "pooled". Neither can these private businesses and projects easily be subject to steering, coordination or forms of controlled planning. What is to be regarded as "Efficient manner" is today mainly decided on an open market. EU Strategic efforts for reinforcing research, technology and industrial capabilities should initially be allocated to create reciprocity towards foreign markets and by common rules and regulations supporting market demands and at the same time strengthening the security within the EU.

<sup>3</sup> Joint Communication to the European Parliament and the Council: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final.

<sup>4</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

<sup>5</sup> Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017) 450 final.

(7a) The decision regarding the seat of the Centre will be taken within the framework of Decision (2004/97/EC, Euratom) by common agreement between the Representatives of the Member States, meeting at Head of State or Government level<sup>6</sup>. It is imperative for the proper and efficient performance of its tasks, for staff recruitment and retention and for enhancing the efficiency of networking activities that the Centre be based in an appropriate location, among other things providing appropriate transport connections and facilities for spouses and children accompanying members of staff of the Centre. The necessary arrangements should be laid down in an agreement between the Centre and the host Member State concluded after obtaining the approval of the Governing Board of the Centre.

(8) The ~~Competence~~ Centre ~~should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with the Cybersecurity Competence Network. It should deliver cybersecurity-related financial support from the Horizon Europe and Digital Europe programmes, and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to cybersecurity research, innovation, technology and industrial development and avoiding duplication.~~

**Commented [A3]:** To align the text with the tasks of the Centre.

**Commented [A4]:** This should be done with utmost care as not to create an unbalanced competition and by that hurting new technologies and companies. Many of the markets "unicorns" emerge from ideas and technologies initially shunned. Many such efforts are not well suited for or have the capabilities for seeking research funds or assistance from large national EU-institutions and might be misfavoured.

(8a) The implementation of the present initiative will be informed by the results of four projects launched in early 2019 under Horizon 2020. These projects will be informative in particular with regard to the content of research and innovation roadmaps and with regard to concrete ways of interaction within the Network and Community.

**Commented [A5]:** Could the Presidency explain this? What is meant by "be informed"?

(8b) Entities from all Member States will be eligible for Union financial support from the Digital Europe and Horizon Europe programmes. This will be regardless whether or not a given entity is located in a Member State which is a contributing Member State.

(9) ~~Taking into account that the objectives of this initiative can be best achieved if all Member States or as many Member States as possible participate, and as an incentive for Member States to take part, only Member States who contribute financially to the administrative and operational costs of the Competence Centre should hold voting rights.~~

(10) ~~The participating Member States' financial participation should be commensurate to the Union's financial contribution to this initiative.~~

(11) The ~~Competence~~ Centre should facilitate and help coordinate the work of the Cybersecurity Competence Network ("the Network"), made up of National Coordination Centres in each Member State. National Coordination Centres should receive direct Union financial support, including grants awarded without a call for proposals, in order to carry out activities related to this Regulation.

<sup>6</sup> Decision (2004/97/EC, Euratom) taken by common agreement between the Representatives of the Member States, meeting at Head of State or Government level, of 13 December 2003 on the location of the seats of certain offices and agencies of the European Union (L 29, 3.2.2004, p. 15).

- (12) National Coordination Centres should be selected by Member States. In addition to the necessary administrative capacity, Centres should either possess or have direct access to cybersecurity technological expertise in cybersecurity, ~~notably in domains such as cryptography, ICT security services, intrusion detection, system security, network security, software and application security, or human and societal aspects of security and privacy.~~ They should also have the capacity to effectively engage and coordinate with the industry, the public sector, including authorities designated pursuant to the Directive (EU) 2016/1148 of the European Parliament and of the Council<sup>7</sup>, and the research community.

**Commented [A6]:** This should be deleted to bring the recital in line with article 6.4, which it the article that sets the requirements for the national node.

~~(12a) The function of National Coordination Centre in a given Member State can be carried out by the same entity also fulfilling other functions created under European law, such as that of a national competent authority and/or single point of contact in the meaning of Article 8 of the NIS Directive or digital innovation hub in the meaning of the Digital Europe Programme.~~

**Commented [A7]:** Unnecessary in relation to recital 12. It can be other solutions as well so why specify these options?

- (13) Where financial support is provided to National Coordination Centres in order to support third parties at the national level, this shall be passed on to relevant stakeholders through cascading grant agreements.

- (14) Emerging technologies such as artificial intelligence, Internet of Things, high-performance computing (HPC) and quantum computing, blockchain and concepts such as secure digital identities create at the same time new challenges for cybersecurity as well as offer solutions. Assessing and validating the robustness of existing or future ICT systems will require testing security solutions against attacks run on HPC and quantum machines. The **Competence** Centre, the Network and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity solutions. ~~At the same time the Competence Centre and the Network should be at the service of promote activities supporting developers and operators in critical sectors such as transport, energy, health, financial, government, telecom, manufacturing, defence, and space in order to achieve security by design and to help them solve their cybersecurity challenges.~~

**Commented [A8]:** MS competence, especially when it comes to National security

- (15) The **Competence** Centre should have several key functions. First, ~~the Competence Centre~~ **it** should facilitate and help coordinate the work of the European Cybersecurity Competence Network and nurture the Cybersecurity Competence Community. The Centre should ~~drive the~~ **promote** a cybersecurity technological agenda **in accordance with its multi-annual strategic plan** and facilitate access to the expertise gathered in the Network and the Cybersecurity Competence Community. Secondly, it should implement relevant parts of Digital Europe and Horizon Europe programmes by allocating grants, typically following a competitive call for proposals. Thirdly, the **Competence** Centre should facilitate joint investment by the Union, Member States and/or industry.

**Formatted:** English (United States)

**Commented [A9]:** EU should primarily concentrate on giving business, innovation and academia the motivation to pursue a common agenda. This is primarily done through market incentives and regulation (not unusually the same).

<sup>7</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

- (16) The ~~Competence~~ Centre should stimulate and support the cooperation and coordination of the activities of the Cybersecurity Competence Community, which would involve a large, open, and diverse group of actors involved in cybersecurity technology. That Community should include in particular research entities, supply-side industries, demand side industries, civil society groups in the area of cybersecurity and the public sector. The Cybersecurity Competence Community should provide input to the activities and work plan of the ~~Competence~~ Centre and it should also benefit from the community-building activities of the ~~Competence~~ Centre and the Network, but otherwise should not be privileged with regard to calls for proposals or calls for tender.
- (17) In order to respond to the needs of both demand and supply side industries, the ~~Competence~~ Centre's task to provide access to cybersecurity knowledge and technical assistance to industries should refer to both ICT products and services and all other industrial and technological products and solutions in which cybersecurity is to be embedded.
- (18) Whereas the ~~Competence~~ Centre and the Network should strive to achieve synergies and coordination between the cybersecurity civilian and defence spheres, projects financed by the Horizon Europe Programme will be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe shall have a focus on civil applications.
- (18a) This initiative could not utilise resources from Horizon Europe or Digital Europe to fund projects which have a focus on defence applications.**
- (18b) The enhancement of dual use application of cybersecurity technologies for cybersecurity purposes is without prejudice to the civilian nature of this Regulation and should therefore reflect specificities of Member States in cases when cybersecurity policy is pursued by civil-military or military authorities, and ensure complementarity but not overlap to the cyber defence related funding instruments.**
- (19) In order to ensure structured and sustainable collaboration, the relation between the ~~Competence~~ Centre and the National Coordination Centres should be based on a contractual agreement.
- (20) Appropriate provisions should be made to guarantee the liability and transparency of the ~~Competence~~ Centre.
- (21) In view of their respective expertise in cybersecurity, the Joint Research Centre of the Commission as well as the European ~~Union Network and Information Security~~ Agency for Cybersecurity (ENISA) should play an active part in the Cybersecurity Competence Community and the Industrial and Scientific Advisory Board.
- (22) Where they receive a financial contribution is received from the general budget of the Union, the National Coordination Centres and the entities which are part of the Cybersecurity Competence Community should publicise the fact that the respective activities are undertaken in the context of the present initiative.

**Commented [A10]:** This is, somewhat depending on definitions, soon to be most consumer electronics. The scope of work would be enormous. How would the Centre prioritize in this?

**Commented [A11]:** SE does not fully understand what these agreements shall include. The COM are invited to explain further.

**Commented [A12]:** Who are "they"? SE suggests this wording instead to clarify.

- ~~(23) The Union contribution to the Competence Centre should finance half of the costs arising from the establishment, administrative and coordination activities of the Competence Centre. In order to avoid double funding, those activities should not benefit simultaneously from a contribution from other Union programmes.~~
- (24) The Governing Board of the **Competence** Centre, composed of the Member States and the Commission, should define the general direction of the **Competence** Centre's operations, and ensure that it carries out its tasks in accordance with this Regulation. The Governing Board should be entrusted with the powers necessary to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the **Competence** Centre, adopt the **Competence** Centre's work plan and multiannual strategic plan reflecting the priorities in achieving the objectives and tasks of the **Competence** Centre, adopt its rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof.
- (25) In order for the **Competence** Centre to function properly and effectively, the Commission and the Member States should ensure that persons to be appointed to the Governing Board have appropriate professional expertise and experience in functional areas. The Commission and the Member States should also make efforts to limit the turnover of their respective Representatives on the Governing Board in order to ensure continuity in its work.
- (26) The smooth functioning of the **Competence** Centre requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for cybersecurity, and that the duties of the Executive Director be carried out with complete independence.
- (27) The **Competence** Centre should have an Industrial and Scientific Advisory Board as an advisory body to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The Industrial and Scientific Advisory Board should focus on issues relevant to stakeholders and bring them to the attention of the **Competence** Centre's Governing Board. The composition of the Industrial and Scientific Advisory Board and the tasks assigned to it, such as being consulted regarding the work plan, should ensure sufficient representation of stakeholders in the work of the **Competence** Centre.
- (28) The **Competence** Centre should benefit from the particular expertise and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity during the duration of Horizon 2020, through its Industrial and Scientific Advisory Board.

- (29) The **Competence** Centre should have in place rules regarding the prevention and the management of conflict of interest. The **Competence** Centre should also apply the relevant Union provisions concerning public access to documents as set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council<sup>8</sup>. Processing of personal data by the **Competence** Centre will be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council. The **Competence** Centre should comply with the provisions applicable to the Union institutions, and with national legislation regarding the handling of information, in particular sensitive non classified information and EU classified information.
- (30) The financial interests of the Union and of the Member States should be protected by proportionate measures throughout the expenditure cycle, including the prevention, detection and investigation of irregularities, the recovery of lost, wrongly paid or incorrectly used funds and, where appropriate, the application of administrative and financial penalties in accordance with Regulation XXX (EU, Euratom) of the European Parliament and of the Council<sup>9</sup> [the Financial Regulation].
- (31) The **Competence** Centre should operate in an open and transparent way providing all relevant information in a timely manner as well as promoting its activities, including information and dissemination activities to the wider public. The rules of procedure of the bodies of the **Competence** Centre should be made publicly available.
- (32) The Commission's internal auditor should exercise the same powers over the **Competence** Centre as those exercised in respect of the Commission.
- (33) The Commission, the **Competence** Centre, the Court of Auditors and the European Anti-Fraud Office should get access to all necessary information and the premises to conduct audits and investigations on the grants, contracts and agreement signed by the **Competence** Centre.
- (34) Since the objectives of this Regulation, namely retaining and developing Union's cybersecurity technological and industrial capacities, increasing the competitiveness of the Union's cybersecurity industry and turning cybersecurity into a competitive advantage of other Union industries, cannot be sufficiently achieved by the Member States due the fact that existing, limited resources are dispersed as well as due to the scale of the investment necessary, but can rather by reason of avoiding unnecessary duplication of these efforts, helping to achieve critical mass of investment and ensuring that public financing is used in an optimal way be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

[This Regulation shall be without prejudice to the sole responsibility of the Member States for national security, as provided for in Article 4\(2\) TEU, and to the right of the Member States to protect their essential security interests in accordance with Article 346 TFEU.](#)

**Commented [A13]:** This fundamental and essential principle should be expressed in the recitals and in the regulation itself.

HAVE ADOPTED THIS REGULATION:

<sup>8</sup> Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

<sup>9</sup> [add title and OJ reference]



## CHAPTER I

### GENERAL PROVISIONS AND PRINCIPLES OF THE COMPETENCE CENTRE AND THE NETWORK

#### *Article 1*

##### **Subject matter**

1. This Regulation establishes the European Cybersecurity Industrial, Technology and Research ~~Competence~~ Centre (the '~~Competence~~Centre'), as well as the Network of National Coordination Centres (the "Network"), and lays down rules for the nomination of National Coordination Centres as well as for the establishment of the Cybersecurity Competence Community (the "Community").
2. The ~~Competence~~ Centre shall contribute to the implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] thereof and of the Horizon Europe Programme established by Regulation No XXX and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme].
3. ~~The seat of the Competence Centre shall be located in [XXXBrussels, Belgium]<sup>140</sup>.~~
4. The ~~Competence~~ Centre shall have legal personality. In each Member State, it shall enjoy the most extensive legal capacity accorded to legal persons under the laws of that Member State. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings.
5. **This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the state in areas of criminal law.**

*Article 2*  
**Definitions**

For the purpose of this Regulation, the following definitions shall apply:

- (1) 'cybersecurity' means ~~the protection of~~ **all the activities necessary to protect** network and information systems, ~~their users of such systems, and other persons affected by other affected persons against~~ **cyber threats**;
- (1a) 'network and information system' means a network and information system as defined in point (1) of Article 4 of Directive (EU) 2016/1148";**
- (2) 'cybersecurity products and solutions' means ICT products, services or process with the specific purpose of protecting network and information systems, their users and affected persons from cyber threats;
- (3) 'public authority' means any government or other public administration, including public advisory bodies, at national, regional or local level or any natural or legal person performing public administrative functions under national law, including specific duties;
- (4) ~~'participating Member State contributing Member State'~~ **means a Member State which voluntarily contributes financially to the administrative and operational costs of the Competence Centre.**

*Article 3*  
**Mission of the ~~Competence~~ Centre and the Network**

1. The ~~Competence~~ Centre and the Network shall help the Union to:
- (a.1.a) retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market;
  - (a.1.b) increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into competitive advantage of other Union industries.
2. The ~~Competence~~ Centre shall undertake its tasks, where appropriate, in collaboration with the Network of National Coordination Centres and a Cybersecurity Competence Community.
- (2a) This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the state in areas of criminal law.**

**Commented [A14]:** We still believes this is better placed in article 4 a where the tasks of the centre is described, since art 3 regulates the mission of both the centre and the Network.

*Article 4*  
**Objectives and Tasks of the Centre**  
**of the Centre**

The **Competence** Centre shall have the following objectives and related tasks: -;

1. ~~facilitate~~**facilitating** and ~~help~~**helping** coordinate the work of the National Coordination Centres Network (~~‘the Network’~~) referred to in Article 6 and the and the Community as an ecosystem of all stakeholders whose involvement is required in order to achieve the mission stated in Article 3;
2. ~~stimulating~~ **and steering** cybersecurity research, development and ~~standardization~~ **standardization, based on a common, continuously evaluated and improved multiannual strategic, industrial, technology and research agenda; thereby coordinating research and development priorities between Member States and the Union and contributing to the effectiveness of public support by avoiding unnecessary duplication and fragmentation of efforts;**
3. ~~enhancing and supporting the availability of cybersecurity capabilities, knowledge and infrastructures, in particular for use by industries, the public sector and research communities;~~
6. ~~contribute supporting cybersecurity start-ups and SMEs in Europe to connect to potential markets and to attract investment;~~
8. ~~enhancing cooperation and coordination between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, including in relation to the European Defence Fund.~~

**Commented [A15]:** The center should concentrate on stimulating (rather than steering), fostering and promoting.

**Commented [A16]:** The goals for financial support are already regulated in DEP and Horizon and should therefore not be repeated here, in order to avoid goal conflicts. Articles 4 and 4a should therefore only include objectives and tasks that the Centre in Brussels will perform beyond those specified in the programs. SE still considers that the objectives set out in Art. 4.3, 4.4. and 4.6, are objectives for MS to implement, or they are already regulated in the respective program.

In the same way, we believe that the board should NOT have the task of promoting the centre globally becoming a world-leading player for excellence in cyber security as stated in article 13.3.1. It cannot be a task for a centre that we believe should primarily have a coordinating tasks. In line with this, SE cannot support the addition of the last sentence on financial support in 4.a.1. SE maintains the previous line that the funds are targeted by the respective framework programs.

**Commented [A17]:** Unclear what is intended here. The only possibility indicated in the EDF is a optional option from the MS to appoint a project manager that theoretically could be the CCCN. Nothing more is indicated in the EDF, at this moment. Regardless the CCCN proposal does not at this point include an appropriate level of security from any cyber defence issues

#### Article 4a

##### Tasks of the Center-Centre

**In order to fulfill the mission laid out in Article 3 and the objectives laid out in Article 4, the tasks of the Competence Centre shall include have the following tasks:**

1. ~~contributing to the~~ implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX<sup>11</sup> and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] and of the Horizon Europe Programme established by Regulation No XXX<sup>12</sup> and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme]. and of other Union programmes when provided for in legal acts of the Union]. This shall be done in particular by providing financial support to beneficiaries, including to cybersecurity start-ups and SMEs
3. ~~enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities, by carrying out the following tasks:~~
  - (a) ~~having regard to the state of the art cybersecurity industrial and research infrastructures and related services , acquiring, upgrading, operating and making available such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community;~~
  - (b) ~~having regard to the state of the art cybersecurity industrial and research infrastructures and related services, providing support to other entities, including financially, to acquiring, upgrading, operating and making available such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community;~~
  - (c) ~~providing cybersecurity knowledge and technical assistance to industry and public authorities, in particular by supporting actions aimed at facilitating access to the expertise available in the Network and the Cybersecurity Competence Community;~~

**Commented [A18]:** SE prefers the previous wording of this task: contributing to the implementation of" since it is a task in cooperation with the other actors and this stronger wording is therefore misleading.

**Commented [A19]:** See comment to article 4 above.

<sup>11</sup> [add full title and OJ reference]

<sup>12</sup> [add full title and OJ reference]

- ~~4. contribute to the wide deployment of state of the art cyber security products and solutions across the economy, by carrying out the following tasks:~~
- ~~(a) stimulating cybersecurity research, development and the uptake of Union cybersecurity products and solutions by public authorities and user industries;~~
  - ~~(b) assisting public authorities, demand side industries and other users in adopting and integrating the latest cyber security solutions;~~
  - ~~(c) supporting in particular public authorities in organising their public procurement, or carrying out procurement of state of the art cybersecurity products and solutions on behalf of public authorities;~~
  - ~~(d) providing financial support and technical assistance to cybersecurity start-ups and SMEs to connect to potential markets and to attract investment;~~
- ~~5. improve the understanding of cybersecurity and contribute to reducing skills gaps in the Union related to cybersecurity by carrying out the following tasks:~~
- ~~(a) supporting further development of cybersecurity skills, where appropriate together with relevant EU agencies and bodies including ENISA.~~
- ~~6. contribute to the reinforcement of cybersecurity research and development in the Union by:~~
- 2. providing financial support to cybersecurity research efforts to stakeholders, based on a common, continuously evaluated and improved multiannual strategic, industrial, technology and research agenda.**
- ~~(a) support large scale research and demonstration projects in next generation cybersecurity technological capabilities, in collaboration with the industry and the Network;~~
  - ~~(b) bringing together stakeholders, to foster synergies between civil and defence cyber security research and markets;~~
- ~~8. enhance synergies between the civil and defence dimensions of cybersecurity in relation to the European Defence Fund by carrying out the following tasks:~~

32. having regard to the state-of-the-art, carrying out or facilitating the acquisition of cybersecurity capabilities and infrastructures- at the service of industries, the public sector and research communities, based on in accordance with the conditions defined in the Work Plan.

~~at European level, where relevant with financial contributions from Member States or industry.~~

4. ~~Specifying rules governing the operation of a capability or infrastructure supported pursuant paragraph (6) including where relevant selection of a hosting entity based on criteria that the Competence Centre shall define and rules governing access to and use of an infrastructure or capability.~~

5. ~~having regard to the state-of-the-art, providing support, including financially, to the acquisition or upgrading of cybersecurity capabilities and infrastructures by industries, the public sector and research communities.~~

6. ~~ensuring European value added of the investments made pursuant paragraph (8).~~

73. facilitating collaboration and the provision of advice the sharing of expertise among relevant stakeholders, in particular members of the Community and including defence stakeholders; this may include and providing financial support to public authorities, demand side industries and other users in adopting and integrating the best fit for purpose cyber security solutions.

8. ~~providing targeted support, including financially, to cybersecurity start ups and SMEs.~~

9. ~~together with National Coordination Centres and where appropriate together with relevant EU agencies and bodies including ENISA, provide support, including financially, to actions aiming to increase capacity, transparency, alignment and quality in cybersecurity education and professional training.~~

10. ~~enhancing the coordination between the civilian and military spheres of cybersecurity, in particular by:~~

a. ~~providing advice, sharing expertise and facilitating collaboration among relevant stakeholders, including members of the Community; supporting education, training and exercises;~~

b4. managing multinational cyber defence projects, when requested by Member States, and thus acting as a project manager within the meaning of Regulation XXX [Regulation establishing the European Defence Fund].

**Commented [A20]:** If the centre shall carry out acquisition of infrastructure on an EU-level shall it not only be based on the conditions defined in the work plan but be in accordance with the conditions.

**Commented [A21]:** Unnecessary specifications. It shall be up to the parties to decide what to cooperate about.

**Commented [A22]:** Pending on negotiation in EDF, and the capability of the CCCN to manage these task. Not possible at this point

#### Article 5

##### **Investment in and use of infrastructures, capabilities, products or solutions**

1. ~~Where the Competence Centre provides funding for infrastructures, capabilities, products or solutions pursuant to Article 4(3) and (4) in the form of a grant or a prize, the work plan of the Competence Centre may specify in particular:~~  
~~rules governing the operation of an infrastructure or capability, including where relevant entrusting the operation to a hosting entity based on criteria that the Competence Centre shall define;~~  
~~rules governing access to and use of an infrastructure or capability.~~
2. ~~The Competence Centre may be responsible for the overall execution of relevant joint procurement actions including pre-commercial procurements on behalf of members of the Network, members of the cybersecurity Competence Community, or other third parties representing the users of cybersecurity products and solutions. For this purpose, the Competence Centre may be assisted by one or more National Coordination Centres or members of the Cybersecurity Competence Community.~~

#### Article 6

##### **Nomination of National Coordination Centres**

1. By [date], each Member State shall nominate the entity to act as the National Coordination Centre for the purposes of this Regulation and notify it to the Commission.
2. On the basis of **the nomination by a Member State of an entity which fulfils an assessment concerning the compliance of that entity with** the criteria laid down in paragraph 4, the ~~Commission Governing Board~~ shall issue a decision within **6-2** months from the nomination transmitted by the Member State providing for the **accreditation registration** of the entity as a National Coordination Centre ~~or rejecting the nomination~~. The list of National Coordination Centres shall be published by the Commission.
3. Member States may at any time nominate a new entity as the National Coordination Centre for the purposes of this Regulation. Paragraphs 1 and 2 shall apply to nomination of any new entity.
4. The nominated National Coordination Centre shall have the capability to support the **Competence** Centre and the Network in fulfilling their mission laid out in Article 3 of this Regulation. They shall possess or have direct access to technological expertise in cybersecurity and be in a position to effectively engage and coordinate with industry, the public sector and the research community.

**Commented [A23]:** Six months is far too long for the Member States to get a decision. Six months in a transposition phase at national level is a lot of time, especially given that the implementation time of the regulation is expected to be short. We have no opportunity to wait for six months for a decision. This regulation can in turn mean changes in regulations at national level, a work that takes time. We believe that two months is a more reasonable time.

5. The relationship between the **Competence** Centre and the National Coordination Centres shall be based on a **harmonised** contractual agreement signed between the **Competence** Centre and each of the National Coordination Centres. The agreement shall provide for the rules governing the relationship and division of tasks between the **Competence** Centre and each National Coordination Centre.
6. The National Coordination Centres Network shall be composed of all the National Coordination Centres nominated by the Member States.

**Commented [A24]:** Could the COM explain why there is a need for these agreements and what is expected to be regulated by them? Shouldn't the different roles be specified within this regulation to avoid any misunderstandings? Based on the MS differences in national organization the provisions in such an agreement might be harder for some MS to fulfil.

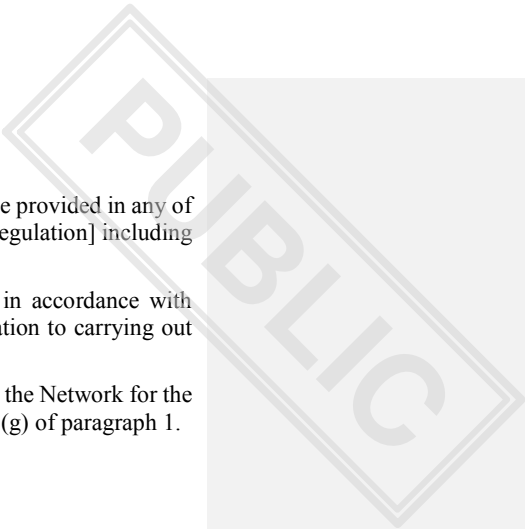
#### *Article 7*

##### **Tasks of the National Coordination Centres**

1. The National Coordination Centres shall have the following tasks:
- a) supporting the **Competence** Centre in achieving its objectives and in particular in coordinating the Cybersecurity Competence Community;
  - b) facilitating the participation of industry and other actors at the Member State level in cross-border projects;
  - c) contributing, together with the **Competence** Centre, to identifying and addressing sector-specific cyber security industrial challenges;
  - d) acting as contact point at the national level for the Cybersecurity Competence Community and the **Competence** Centre;
  - e) seeking to establish synergies with relevant activities at the national and regional level, including national policies on research, development and innovation in the area of cybersecurity, and in particular those stated in the national cybersecurity strategies;
  - f) implementing specific actions for which grants have been awarded by the **Competence** Centre, including through provision of financial support to third parties in line with Article 204 of Regulation XXX [new Financial Regulation] under conditions specified in the concerned grant agreements;
  - g) promoting and disseminating the relevant outcomes of the work by the Network, the Cybersecurity Competence Community and the **Competence** Centre at national or regional level;
  - h) assessing requests by entities established in the same Member State as the Coordination Centre for becoming part of the Cybersecurity Competence Community.

**Commented [A25]:** SE cannot support this addition since it governs the Member States' choice of actor within this regulation and also the national policy.



- 
2. For the purposes of point (f), the financial support to third parties may be provided in any of the forms specified in Article 125 of Regulation XXX [new Financial Regulation] including in the form of lump sums.
  3. National Coordination Centres may receive a grant from the Union in accordance with Article 195 (d) of Regulation XXX [new Financial Regulation] in relation to carrying out the tasks laid down in this Article.
  4. National Coordination Centres shall, where relevant, cooperate through the Network for the purpose of implementing tasks referred to in points (a), (b), (c), (e) and (g) of paragraph 1.

#### *Article 8*

##### **The Cybersecurity Competence Community**

1. The Cybersecurity Competence Community shall contribute to the mission of the ~~Competence~~ Centre as laid down in Article 3 and enhance and disseminate cybersecurity expertise across the Union.
2. The Cybersecurity Competence Community shall consist of industry, academic and non-profit research organisations, **other relevant civil society actors**, and associations as well as public entities and other entities dealing with operational and technical matters. It shall bring together the main stakeholders with regard to cybersecurity technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise.
3. Only entities which are established within the Union may be accredited as members of the Cybersecurity Competence Community. They shall demonstrate that they have cybersecurity expertise with regard to at least one of the following domains:
  - a) research;
  - b) industrial development;
  - c) training and education.
4. The ~~Competence~~ Centre shall accredit entities established under national law as members of the Cybersecurity Competence Community after an assessment made by the National Coordination Centre of the Member State where the entity is established, on whether that entity meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the ~~Competence~~ Centre at any time if it or the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation].

5. The ~~Competence~~ Centre shall accredit relevant bodies, agencies and offices of the Union as members of the Cybersecurity Competence Community after carrying out an assessment whether that entity meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the ~~Competence~~ Centre at any time if it considers that the entity does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation].
6. The representatives of the Commission may participate in the work of the Community.

#### *Article 9*

##### **Tasks of the members of the Cybersecurity Competence Community**

The members of the Cybersecurity Competence Community shall:

1. support the ~~Competence~~ Centre in achieving the mission and the objectives laid down in Articles 3 and 4 and, for this purpose, work closely with the Competence Centre and the relevant National Coordinating Centres;
2. participate in activities promoted by the ~~Competence~~ Centre and National Coordination Centres;
3. where relevant, participate in working groups established by the Governing Board of the ~~Competence~~ Centre to carry out specific activities as provided by the ~~Competence~~ Centre's work plan;
4. where relevant, support the ~~Competence~~ Centre and the National Coordination Centres in promoting specific projects;
5. promote and disseminate the relevant outcomes of the activities and projects carried out within the community.

#### *Article 10*

##### **Cooperation of the ~~Competence~~ Centre with Union institutions, bodies, offices and agencies and other international organisations**

1. ~~To ensure coherence and complementarity, the~~ **To ensure coherence and complementarity,** The ~~Competence~~ Centre shall cooperate with relevant Union institutions, bodies, offices and agencies including the European Union Agency for ~~Cybersecurity Network and Information Security~~, the Computer Emergency Response Team (CERT-EU), the European External Action Service, the Joint Research Centre of the Commission, the Research Executive Agency, Innovation and Networks Executive Agency, European Cybercrime Centre at Europol as well as the European Defence Agency.
2. Such cooperation shall take place within the framework of working arrangements. Those arrangements shall be submitted to the prior approval of the Commission.

## CHAPTER II

### ORGANISATION OF THE ~~COMPETENCE~~ CENTRE

#### *Article 11*

##### **Membership and structure**

1. The members of the ~~Competence~~ Centre shall be the Union, represented by the Commission, and the Member States.
2. The structure of the ~~Competence~~ Centre shall comprise:
  - 1) a Governing Board which shall exercise the tasks set out in Article 13;
  - 2) an Executive Director who shall exercise the tasks set out in Article ~~16~~17;
  - 3) an Industrial and Scientific Advisory Board which shall exercise the functions set out in Article 20.

**SECTION I**  
**GOVERNING BOARD**

*Article 12*

**Composition of the Governing Board**

1. The Governing Board shall be composed of one representative of each Member State, and ~~five~~two representatives of the Commission, on behalf of the Union.
2. Each member of the Governing Board shall have an alternate to represent them in their absence.
3. Members of the Governing Board and their alternates shall be appointed in light of their knowledge in the field of technology as well as of relevant managerial, administrative and budgetary skills. The Commission and the Member States shall make efforts to limit the turnover of their representatives in the Governing Board, in order to ensure continuity of the Board's work. The Commission and the Member States shall aim to achieve a balanced representation between men and women on the Governing Board.
4. The term of office of members of the Governing Board and of their alternates shall be four years. That term shall be renewable.
5. The Governing Board members shall act ~~in the interest of the Competence Centre, safeguarding to safeguard the Centre's its~~ goals and mission, identity, autonomy and coherence, in an independent and transparent way.
6. The Commission may invite observers, including representatives of relevant Union bodies, offices and agencies, to take part in the meetings of the Governing Board as appropriate.
7. The European Union Agency for Cybersecurity ~~Network and Information Security~~ (ENISA) shall be a permanent observer in the Governing Board.

*Article 13*

**Tasks of the Governing Board**

1. The Governing Board shall have the overall responsibility for the strategic orientation and the operations of the **Competence** Centre and shall supervise the implementation of its activities.
2. The Governing Board shall adopt its rules of procedure. These rules shall include specific procedures for identifying and avoiding conflicts of interest and ensure the confidentiality of any sensitive information.
3. The Governing Board shall take the necessary strategic decisions, in particular:
  - a) adopt a multi-annual strategic plan, containing a statement of the major priorities and planned initiatives of the **Competence** Centre, including an estimate of financing needs and sources;
  - b) adopt the **Competence** Centre's work plan, annual accounts and balance sheet and annual activity report, on the basis of a proposal from the Executive Director;
  - c) adopt the specific financial rules of the **Competence** Centre in accordance with [Article 70 of the Financial Regulation];
  - d) adopt a procedure for appointing the Executive Director;
  - e) adopt the criteria and procedures for assessing and accrediting the entities as members of the Cybersecurity Competence Community;
  - f) appoint, dismiss, extend the term of office of, provide guidance to and monitor the performance of the Executive Director, and appoint the Accounting Officer;
  - g) adopt the annual budget of the **Competence** Centre, including the corresponding staff establishment plan indicating the number of temporary posts by function group and by grade, the number of contract staff and seconded national experts expressed in full-time equivalents;
  - h) adopt rules regarding conflicts of interest;

- i) establish working groups with members of the Cybersecurity Competence Community;
- j) appoint members of the Industrial and Scientific Advisory Board;
- k) set up an Internal Auditing Function in accordance with Commission Delegated Regulation (EU) No 1271/2013<sup>13</sup>;
- l) promote the Competence Centre globally, so as to raise its attractiveness and make it a world-class body for excellence in cybersecurity;
- m) establish the **Competence** Centre's communications policy upon recommendation by the Executive Director;
- n) be responsible to monitor the adequate follow-up of the conclusions of retrospective evaluations;
- o) where appropriate, establish implementing rules to the Staff Regulations and the Conditions of Employment in accordance with Article 31(3);
- p) where appropriate, lay down rules on the secondment of national experts to the **Competence** Centre and on the use of trainees in accordance with Article 32(2);
- q) adopt security rules for the **Competence** Centre;
- r) adopt an anti-fraud strategy that is proportionate to the fraud risks having regard to a cost-benefit analysis of the measures to be implemented;
- s) adopt the methodology to calculate the financial contribution from **contributing** Member States;
- u) register entities nominated by Member States as their National Coordination Centres;**
- v) in deciding on the Work Plan and the multi-annual strategic plan, ensure coherence and synergies with those parts of the Digital Europe and the Horizon Europe programmes which are not managed by the Centre as well as with other Union programmes;**
- t) be responsible for any task that is not specifically allocated to a particular body of the **Competence** Centre; it may assign such tasks to anybody of the **Competence** Centre.

**Commented [A26]:** See comment to art 4.1. It states that SE believes that the board should not have the task of promoting the centre globally becoming a world-leading player for excellence in cyber security as stated in article 13.3.1. It cannot be a task for a centre that we believe should primarily have a coordinating tasks.

**Commented [A27]:** The regulation should set up, a minimum standard for this, given the sensitive nature of cyber security and cyber defence. COM SEG or Council security group should be advised

**Commented [A28]:** SE supports this paragraph.

<sup>13</sup> Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council (OJ L 328, 7.12.2013, p. 42).

*Article 14*

**Chairperson and Meetings of the Governing Board**

1. The Governing Board shall elect a Chairperson and a Deputy Chairperson from among ~~the~~ **its** members ~~with voting rights~~, for a period of two years. The mandate of the Chairperson and the Deputy Chairperson may be extended once, following a decision by the Governing Board. If, however, their membership of the Governing Board ends at any time during their term of office, their term of office shall automatically expire on that date. The Deputy Chairperson shall *ex officio* replace the Chairperson if the latter is unable to attend to his or her duties. The Chairperson shall take part in the voting.
2. The Governing Board shall hold its ordinary meetings at least three times a year. It may hold extraordinary meetings at the request of the Commission, at the request of one third of all its members, at the request of the chair, or at the request of the Executive Director in the fulfilment of his/her tasks.
3. The Executive Director shall take part in the deliberations, unless decided otherwise by the Governing Board, but shall have no voting rights. The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers.
4. Members of the Industrial and Scientific Advisory Board may take part, upon invitation from the Chairperson, in the meetings of the Governing Board, without voting rights.
5. The members of the Governing Board and their alternates may, subject to its rules of procedure, be assisted at the meetings by advisers or experts.
6. The ~~Competence~~ Centre shall provide the secretariat for the Governing Board.

Article 15

**Voting rules of the Governing Board**

**Commented [A29]:** SE still believes that this article is hard to understand.

- 1. The representatives of the members of the Governing Board shall make every effort to achieve consensus. Failing consensus, a vote shall be held.
- 2. Decisions subject to vote may concern: (i) governance and organisation of the Centre and Network; (ii) allocation of EU operational budget; (iii) joint actions by several Member States, possibly complemented by EU budget further to decision allocated according to (ii).
- 3. The Governing Board shall take its decisions by a majority of at least 75% of all votes. An absent member of the Governing Board may delegate his or her vote to another member. Any member of the Governing Board may represent not more than one other member., including the votes of the members who are absent.
  1. The Union shall hold 50 % of the voting rights for decisions under Articles 15.(2).(i) and ii15.2.ii. The voting rights of the Union shall be indivisible.
  - ~~2. Every participating Member State shall hold one vote for decisions under article 15.(2).(i) and (ii).~~
  - 2a. Every Member State shall hold one vote for any decision under the articles 15.(2).(i) and (ii).
  - 2b Every Member State shall hold one vote for ~~the any?~~ decision ~~on creating any joint action~~ under the article 15.(2).(iii).
  - 2c. Contributing Member States and the Commission shall hold votes proportional to their relevant contribution on the conditions for and management of a joint action budget under the article 15.(2).(iii).
  - ~~2d. Contributing Member States and the Commission, acting on behalf of EU interests, shall hold votes proportional to their contribution for decisions under article 15.(2).(iii).~~
  - ~~3. The Governing Board shall take its decisions by a majority of at least 75% of all votes, including the votes of the members who are absent, representing at least 75% of the total financial contributions to the Competence Centre. The financial contribution will be calculated based on the estimated expenditures proposed by the Member States referred to in point e of Article 17(2) and based on the report on the value of the contributions of the participating Member States referred to in Article 22(5).~~

**Commented [A30]:** Suggestion to align the text with previous paragraphs.



4. ~~Only the representatives of the Commission and the representatives of the participating Member States shall hold voting rights.~~
5. The Chairperson shall take part in the voting as a representative of his/her Member State.

## SECTION II

### EXECUTIVE DIRECTOR

#### *Article 16*

#### Appointment, dismissal or extension of the term of office of the Executive Director

Commented [A31]: Security requirements?

1. The Executive Director shall be a person with expertise and high reputation in the areas where the ~~Competence~~ Centre operates.
2. The Executive Director shall be engaged as a temporary agent of the ~~Competence~~ Centre under Article 2(a) of the Conditions of Employment of Other Servants.
3. The Executive Director shall be appointed by the Governing Board from a list of candidates proposed by the Commission, following an open and transparent selection procedure.
4. For the purpose of concluding the contract of the Executive Director, the ~~Competence~~ Centre shall be represented by the Chairperson of the Governing Board.
5. The term of office of the Executive Director shall be four years. By the end of that period, the Commission shall carry out an assessment which takes into account the evaluation of the performance of the Executive Director and the ~~Competence~~ Centre's future tasks and challenges.
6. The Governing Board may, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 5, extend once the term of office of the Executive Director for no more than four years.
7. An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post.
8. The Executive Director shall be removed from office only by decision of the Governing Board, acting on a proposal from the Commission or at least 50% of the Member States.

*Article 17*

**Tasks of the Executive Director**

1. The Executive Director shall be responsible for operations and for the day-to-day management of the ~~Competence~~ Centre and shall be its legal representative. The Executive Director shall be accountable to the Governing Board and perform his or her duties with complete independence within the powers assigned to him or her.
2. The Executive Director shall in particular carry out the following tasks in an independent manner:
  - a) implement the decisions adopted by the Governing Board;
  - b) support the Governing Board in its work, provide the secretariat for their meetings and supply all information necessary for the performance of their duties;
  - c) after consultation with the Governing Board and the Commission, prepare and submit for adoption to the Governing Board the draft multiannual strategic plan and the draft annual work plan of the ~~Competence~~ Centre including the scope of the calls for proposals, calls for expressions of interest and calls for tenders needed to implement the work plan and the corresponding expenditure estimates as proposed by the Member States and the Commission;
  - d) prepare and submit for adoption to the Governing Board the draft annual budget, including the corresponding staff establishment plan indicating the number of temporary posts in each grade and function group and the number of contract staff and seconded national experts expressed in full-time equivalents;
  - e) implement the work plan and report to the Governing Board thereon;
  - f) prepare the draft annual activity report on the ~~Competence~~ Centre, including the information on corresponding expenditure;
  - g) ensure the implementation of effective monitoring and evaluation procedures relating to the performance of the ~~Competence~~ Centre;
  - h) prepare an action plan following-up on the conclusions of the retrospective evaluations and reporting on progress every two years to the Commission;

- PUBLIC
- i) prepare, ~~negotiate~~ and conclude the agreements with the National Coordination Centres;
  - j) be responsible for administrative, financial and staff matters, including the implementation of the ~~Competence~~ Centre budget, taking due account of advice received from the Internal Auditing Function, within the limits of the delegation by the Governing Board;
  - k) approve and manage the launch of calls for proposals, in accordance with the work plan and administer the grant agreements and decisions;
  - l) approve the list of actions selected for funding on the basis of the ranking list established by a panel of independent experts;
  - m) approve and manage the launch of calls for tenders, in accordance with the work plan and administer the contracts;
  - n) approve the tenders selected for funding;
  - o) submit the draft annual accounts and balance sheet to the Internal Auditing Function, and subsequently to the Governing Board;
  - p) ensure that risk assessment and risk management are performed;
  - q) sign individual grant agreements, decisions and contracts;
  - r) sign procurement contracts;
  - s) prepare an action plan following-up conclusions of internal or external audit reports, as well as investigations by the European Anti-Fraud Office (OLAF) and reporting on progress twice a year to the Commission and regularly to the Governing Board;
  - t) prepare draft financial rules applicable to the ~~Competence~~ Centre;
  - u) establish and ensure the functioning of an effective and efficient internal control system and report any significant change to it to the Governing Board;
  - v) ensure effective communication with the Union's institutions;
  - w) take any other measures needed to assess the progress of the ~~Competence~~ Centre towards its mission and objectives as set out in Articles 3 and 4 of this Regulation;
  - x) perform any other tasks entrusted or delegated to him or her by the Governing Board.

ensure the functioning of an effective and secure management of sensitive and classified information and report any significant change to it to the Governing Board.

**Commented [A32]:** Responsibility for ensuring secure management of information needs to be tasked to someone, include compliance and measurement if any mismanagement would be discovered, if cyber defence issues are to be within the scope of the CCCN

### SECTION III

#### INDUSTRIAL AND SCIENTIFIC ADVISORY BOARD

##### *Article 18*

##### **Composition of the Industrial and Scientific Advisory Board**

1. The Industrial and Scientific Advisory Board shall consist of no more than ~~16~~27 members. The members shall be appointed by the Governing Board from among the representatives of the entities of the Cybersecurity Competence Community.
2. Members of the Industrial and Scientific Advisory Board shall have expertise either with regard to cybersecurity research, industrial development, professional services or the deployment thereof. The requirements for such expertise shall be further specified by the Governing Board.
- 2a. The Governing Board shall ensure that the membership of the Industrial and Scientific Advisory Board be balanced between scientific, industrial and civil society entities, demand and supply side industries, as well as in terms of geographic provenance and gender.**
3. Procedures concerning the appointment of its members by the Governing Board and the operation of the Advisory Board, shall be specified in the ~~Competence~~ Centre's rules of procedure and shall be made public.
4. The term of office of members of the Industrial and Scientific Advisory Board shall be three years. That term shall be renewable.
5. Representatives of the Commission and of the European Network and Information Security Agency may participate in and support the works of the Industrial and Scientific Advisory Board.

#### *Article 19*

##### **Functioning of the Industrial and Scientific Advisory Board**

1. The Industrial and Scientific Advisory Board shall meet at least twice a year.
2. The Industrial and Scientific Advisory Board may advise the Governing Board on the establishment of working groups on specific issues relevant to the work of the **Competence** Centre where necessary under the overall coordination of one or more members of the Industrial and Scientific Advisory Board.
3. The Industrial and Scientific Advisory Board shall elect its chair.
4. The Industrial and Scientific Advisory Board shall adopt its rules of procedure, including the nomination of the representatives that shall represent the Advisory Board where relevant and the duration of their nomination.

#### *Article 20*

##### **Tasks of the Industrial and Scientific Advisory Board**

The Industrial and Scientific Advisory Board shall advise the **Competence** Centre in respect of the performance of its activities and shall:

1. provide to the Executive Director and the Governing Board strategic advice and input for drafting the work plan and multi-annual strategic plan within the deadlines set by the Governing Board;
2. organise public consultations open to all public and private stakeholders having an interest in the field of cybersecurity, in order to collect input for the strategic advice referred to in paragraph 1;
3. promote and collect feedback on the work plan and multi-annual strategic plan of the **Competence** Centre.

## CHAPTER III

### FINANCIAL PROVISIONS

#### Article 21

##### Union financial contribution

1. The Union's contribution to the ~~Competence~~ Centre to cover administrative costs and operational costs shall comprise the following:
  - a) EUR 1 981 668 000 from the Digital Europe Programme, including up to EUR 23 746 000 for administrative costs;
  - b) An amount from the Horizon Europe Programme, including for administrative costs, to be determined taking into account the strategic planning process to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation].
2. The maximum Union contribution shall be paid from the appropriations in the general budget of the Union allocated to [Digital Europe Programme] and to the specific programme implementing Horizon Europe, established by Decision XXX.
3. The ~~Competence~~ Centre shall implement cybersecurity actions of [Digital Europe Programme] and [Horizon Europe Programme] in accordance with point (c) (iv) of Article 62 of Regulation (EU, Euratom) XXX<sup>14</sup> [the financial regulation].
4. The Union financial contribution mentioned in paragraph 1 of this Article shall not cover the tasks referred to in Article 4(8)(b) ~~(410)~~.
5. **Contributions from Union programmes other than those referred to in paragraphs (1) and (2) above that are part of a Union co-financing to a programme implemented by one of the Member States shall not be accounted for in the calculation of the Union maximum financial contribution referred to in paragraphs (1) and (2) above.**

**Commented [A33]:** Could the Presidency or the COM explain the meaning of this paragraph. What is the aim with this regulation? This shall not apply to EDF-funds

#### Article 22

##### Contributions of ~~participating Member State~~ contributing Member States

- ~~1.1.~~ —The ~~participating~~ Member States shall make a total contribution ~~can contribute~~ to the operational and administrative costs of the ~~Competence~~ Centre **in view of actions pursuant Article 4a(32) of at least the same amounts as those in Article 21(1) of this Regulation decided according to Article 15(2)(iii).**
- 1a. **Member States co-funding of actions supported by EU programmes other than Horizon Europe and Digital Europe could be considered as contributions in the sense of Article 22.1. insofar as those actions are in the remit of the Centre missions and tasks.**
2. For the purpose of assessing the contributions referred to in paragraph 1 and in point (b)ii of Article 23(3), the costs shall be determined in accordance with the usual cost accounting practices of the Member States concerned, the applicable accounting standards of the Member State, and the applicable International Accounting Standards and International Financial Reporting Standards. The costs shall be certified by an independent external

<sup>14</sup> [add full title and OJ reference]

auditor appointed by the Member State concerned. The valuation method may be verified by the ~~Competence~~ Centre should there be any uncertainty arising from the certification.

3. Should any ~~participating Member State~~ **Member State** be in default of its commitments concerning its financial contribution **pursuant to actions pursuant Article 4a(32) of this Regulation decided according to Article 15(2)(iii)**, the Executive Director shall put this in writing and shall set a reasonable period within which such default shall be remedied. If the situation is not remedied within that period, the Executive Director shall convene a meeting of the Governing Board to decide whether the defaulting participating Member State's right to vote is to be revoked or whether any other measures are to be taken until its obligations have been met. The defaulting Member State's voting rights **concerning actions actions pursuant Article 4a(32) of this Regulation decided according to Article 15(2)(iii)** shall be suspended until the default of its commitments is remedied.
4. The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to **actions pursuant Article 4a(32) of this Regulation decided according to Article 15(2)(iii)** ~~the Competence Centre~~ if the ~~participating Member State~~ **contributing Member States** do not contribute, contribute only partially or contribute late with regard to the contributions referred to in paragraph 1.
5. The ~~participating Member State~~ **contributing Member States** shall report by 31 January each year to the Governing Board on the value of the contributions referred to in paragraphs 1 made in each of the previous financial year.

### Article 23

#### Costs and resources of the Competence Centre

1. The ~~Competence~~ Centre shall be ~~jointly~~-funded by the Union, ~~and~~ Member States ~~may~~ **make voluntary contributions to actions pursuant Article 4a(2) of this Regulation decided according to Article 15(2)(iii)** through financial contributions paid in instalments and contributions consisting of costs incurred by National Coordination Centres and beneficiaries in implementing actions that are not reimbursed by the ~~Competence~~ Centre.
2. The administrative costs of the ~~Competence~~ Centre ~~shall not exceed EUR [number] and shall be covered by means of financial contributions divided equally proportionally on an annual basis between from the Union, and the participating Member State~~ **Additional contributions shall be made by from contributing Member States in proportion to their as applicable voluntary contributions to actions pursuant Article 4a(2) of this Regulation decided according to Article 15(2)(iii)**. If part of the contribution for administrative costs is not used, it may be made available to cover the operational costs of the ~~Competence~~ Centre.
3. The operational costs of the ~~Competence~~ Centre shall be covered by means of:
  - a) the Union's financial contribution;
  - b) **voluntary** contributions from the ~~participating Member State~~ **contributing Member States** in the form of:
    - i. ~~(i)~~ Financial contributions; and
    - ii. ~~(ii)~~ —where relevant, in-kind contributions by the ~~participating Member State~~ **contributing Member States**. **A contributing Member State's in-kind contribution to a given action supported by the Centre shall consist of the relevant costs incurred by the National Coordination Centres and beneficiaries established in that Member State in implementing indirect actions** less the contribution of the ~~Competence~~ Centre and any other Union contribution to those costs;
4. The resources of the ~~Competence~~ Centre entered into its budget shall be composed of the following contributions:
  - a) **the Union's financial contributions to the operational and administrative costs;**
  - b) ~~participating Member State~~ **contributing Member States'** financial contributions to the administrative costs;
  - c) ~~participating Member State~~ **contributing Member States'** financial contributions to the operational costs;



- c) any revenue generated by ~~the~~**Competence** Centre;
- d) any other financial contributions, resources and revenues.
5. Any interest yielded by the contributions paid to the **Competence** Centre by the ~~participating Member State~~**contributing Member States** shall be considered to be its revenue.
6. All resources of the **Competence** Centre and its activities shall be aimed to achieve ~~to~~ the objectives set out in Article 4.
7. The **Competence** Centre shall own all assets generated by it or transferred to it for the fulfilment of its objectives.
8. Except when the **Competence** Centre is wound up, any excess revenue over expenditure shall not be paid to the ~~participating~~**contributing** members of the **Competence** Centre.

*Article 24*

**Financial commitments**

The financial commitments of the **Competence** Centre shall not exceed the amount of financial resources available or committed to its budget by its members.

*Article 25*

**Financial year**

The financial year shall run from 1 January to 31 December.

*Article 26*

**Establishment of the budget**

1. Each year, the Executive Director shall draw up a draft statement of estimates of the ~~Competence~~ Centre's revenue and expenditure for the following financial year, and shall forward it to the Governing Board, together with a draft establishment plan. Revenue and expenditure shall be in balance. The expenditure of the ~~Competence~~ Centre shall include the staff, administrative, infrastructure and operational expenses. Administrative expenses shall be kept to a minimum.
2. Each year, the Governing Board shall, on the basis of the draft statement of estimates of revenue and expenditure referred to in paragraph 1, produce a statement of estimates of revenue and expenditure for the ~~Competence~~ Centre for the following financial year.
3. The Governing Board shall, by 31 January each year, send the statement of estimates referred to in paragraph 2, which shall be part of the draft single programming document, to the Commission.
4. On the basis of that statement of estimates, the Commission shall enter in the draft budget of the Union the estimates it deems necessary for the establishment plan and the amount of the contribution to be charged to the general budget, which it shall submit to the European Parliament and the Council in accordance with Articles 313 and 314 TFEU.
5. The European Parliament and the Council shall authorise the appropriations for the contribution to the ~~Competence~~ Centre.
6. The European Parliament and the Council shall adopt the establishment plan for the ~~Competence~~ Centre.
7. Together with the Work Plan, the Governing Board shall adopt the Centre's budget. It shall become final following definitive adoption of the general budget of the Union. Where appropriate, the Governing Board shall adjust the ~~Competence~~ Centre's budget and Work Plan in accordance with the general budget of the Union.

*Article 27*

**Presentation of the ~~Competence~~ Centre's accounts and discharge**

The presentation of the ~~Competence~~ Centre's provisional and final accounts and the discharge shall follow the rules and timetable of the Financial Regulation and of its financial rules adopted in accordance with Article 29.

*Article 28*

**Operational and financial reporting**

1. The Executive Director shall report annually to the Governing Board on the performance of his/her duties in accordance with the financial rules of the ~~Competence~~ Centre.
2. Within two months of the closure of each financial year, the Executive Director shall submit to the Governing Board for approval an annual activity report on the progress made by the ~~Competence~~ Centre in the previous calendar year, in particular in relation to the work plan for that year. That report shall include, inter alia, information on the following matters:
  - a) operational actions carried out and the corresponding expenditure;
  - b) the actions submitted, including a breakdown by participant type, including SMEs, and by Member State;
  - c) the actions selected for funding, including a breakdown by participant type, including SMEs, and by Member State and indicating the contribution of the ~~Competence~~ Centre to the individual participants and actions;
  - d) progress towards the achievement of the objectives set out in Article 4 and proposals for further necessary work to achieve these objectives.
3. Once approved by the Governing Board, the annual activity report shall be made publicly available.

*Article 29*

**Financial rules**

The ~~Competence~~ Centre shall adopt its specific financial rules in accordance with Article 70 of Regulation XXX [new Financial Regulation].

*Article 30*

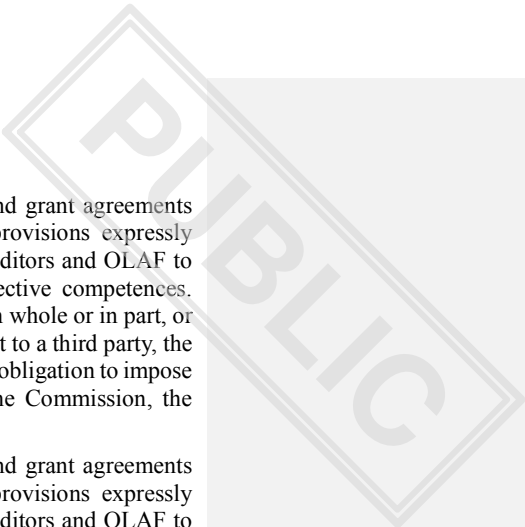
**Protection of financial interests**

1. The ~~Competence~~ Centre shall take appropriate measures to ensure that, when actions financed under this Regulation are implemented, the financial interests of the Union are protected by the application of preventive measures against fraud, corruption and any other illegal activities, by effective checks and, if irregularities are detected, by the recovery of the amounts wrongly paid and, where appropriate, by effective, proportionate and dissuasive administrative sanctions.
2. The ~~Competence~~ Centre shall grant Commission staff and other persons authorised by the Commission, as well as the Court of Auditors, access to its sites and premises and to all the information, including information in electronic format that is needed in order to conduct their audits.
3. The European Anti-Fraud Office (OLAF) may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Council Regulation (Euratom, EC) No 2185/96<sup>15</sup> and Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council<sup>16</sup> with a view to establishing whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant agreement or a contract funded, directly or indirectly, in accordance with this Regulation.

---

<sup>15</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).

<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, 18.9.2013, p. 1).

- 
4. Without prejudice to paragraphs 1, 2 and 3 of this Article, contracts and grant agreements resulting from the implementation of this Regulation shall contain provisions expressly empowering the Commission, the ~~Competence~~ Centre, the Court of Auditors and OLAF to conduct such audits and investigations in accordance with their respective competences. Where the implementation of an action is outsourced or sub-delegated, in whole or in part, or where it requires the award of a procurement contract or financial support to a third party, the contract, or grant agreement shall include the contractor's or beneficiary's obligation to impose on any third party involved explicit acceptance of those powers of the Commission, the ~~Competence~~ Centre, the Court of Auditors and OLAF.
5. Without prejudice to paragraphs 1, 2 and 3 of this Article, contracts and grant agreements resulting from the implementation of this Regulation shall contain provisions expressly empowering the Commission, the ~~Competence~~ Centre, the Court of Auditors and OLAF to conduct such audits and investigations in accordance with their respective competences. Where the implementation of an action is outsourced or sub-delegated, in whole or in part, or where it requires the award of a procurement contract or financial support to a third party, the contract, or grant agreement shall include the contractor's or beneficiary's obligation to impose on any third party involved explicit acceptance of those powers of the Commission, the ~~Competence~~ Centre, the Court of Auditors and OLAF.

## CHAPTER IV

### COMPETENCE CENTRE STAFF

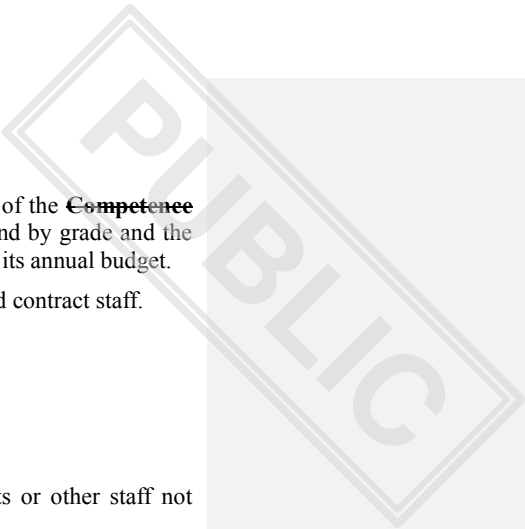
#### *Article 31*

##### **Staff**

1. The Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union as laid down by Council Regulation (EEC, Euratom, ECSC) No 259/68<sup>17</sup> ('Staff Regulations' and 'Conditions of Employment') and the rules adopted jointly by the institutions of the Union for the purpose of applying the Staff Regulations and Conditions of Employment shall apply to the staff of the ~~Competence~~ Centre.
2. The Governing Board shall exercise, with respect to the staff of the ~~Competence~~ Centre, the powers conferred by the Staff Regulations on the Appointing Authority and the powers conferred by the Conditions of Employment on the authority empowered to conclude contract ('the appointing authority powers').
3. The Governing Board shall adopt, in accordance with Article 110 of the Staff Regulations, a decision based on Article 2(1) of the Staff Regulations and on Article 6 of the Conditions of Employment delegating the relevant appointing authority powers to the Executive Director and defining the conditions under which that delegation may be suspended. The Executive Director is authorised to sub-delegate those powers.
4. Where exceptional circumstances so require, the Governing Board may by decision temporarily suspend the delegation of the appointing authority powers to the Executive Director and any sub-delegation made by the latter. In such a case the Governing Board shall exercise itself the appointing authority powers or delegate them to one of its members or to a staff member of the ~~Competence~~ Centre other than the Executive Director.
5. The Governing Board shall adopt implementing rules as regards the Staff Regulations and the Conditions of Employment in accordance with Article 110 of the Staff Regulations.

---

<sup>17</sup> Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1).

- 
6. The staff resources shall be determined in the staff establishment plan of the **Competence** Centre, indicating the number of temporary posts by function group and by grade and the number of contract staff expressed in full-time equivalents, in line with its annual budget.
  7. The staff of the **Competence** Centre shall consist of temporary staff and contract staff.
  8. All costs related to staff shall be borne by the **Competence** Centre.

*Article 32*

**Seconded national experts and other staff**

1. The **Competence** Centre may make use of seconded national experts or other staff not employed by the **Competence** Centre.
2. The Governing Board shall adopt a decision laying down rules on the secondment of national experts to the **Competence** Centre, in agreement with the Commission.

*Article 33*

**Privileges and Immunities**

Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union shall apply to the **Competence** Centre and its staff.

## CHAPTER V

### COMMON PROVISIONS

#### Article 34

#### Security Rules

**-1. In the establishment of each annual Work Plan, the need for security rules shall be assessed.**

1. Article 12(7) Regulation (EU) No XXX [Digital Europe Programme] shall apply to participation in all actions funded by the ~~Competence~~ Centre.
2. The following specific security rules shall apply to actions funded from Horizon Europe:
  - a) for the purposes of Article 34(1) [Ownership and protection] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan, the grant of non-exclusive licenses may be limited to third parties established or deemed to be established in Member States and controlled by Member States and/or nationals of Member States;
  - b) for the purposes of Article 36(4)(b) [Transfer and licensing] of Regulation (EU) No XXX [Horizon Europe], the transfer or license to a legal entity established in an associated country or established in the Union but controlled from third countries shall also be a ground to object to transfers of ownership of results, or to grants of an exclusive license regarding results;
  - c) for the purposes of Article 37(3)(a) [Access rights] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan, granting of access to results and background may be limited only to a legal entity established or deemed to be established in Member States and controlled by Member States and/or nationals of Member States.

**Commented [A34]:** This article does not cover readiness for the CCCN to manage/assist etc in any EDF of defence related issue. Either this is managed appropriately or the task/objectives of the CCCN must be modified

**Commented [A35]:** The Article referred to is not sufficiently comprehensive and clear to be applied for any EDF of defence related issue. If the CCCN is to work with defence related issues a security rule such as the one in the EDF is required. This Article should be rewritten and constructed as a standalone Article, and should not refer to DEP.



*Article 35*

**Transparency**

1. The ~~Competence~~ Centre shall carry out its activities with a high level of transparency.
2. The ~~Competence~~ Centre shall ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information, in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Article 41.
3. The Governing Board, acting on a proposal from the Executive Director, may authorise interested parties to observe the proceedings of some of the ~~Competence~~ Centre's activities.
4. The ~~Competence~~ Centre shall lay down, in its rules of procedure, the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2. For actions funded from Horizon Europe this will take due account of the provisions in Annex III of the Horizon Europe Regulation.

*Article 36*

**Security rules on the protection of classified information and sensitive non-classified information**

1. Without prejudice to Article 35, the ~~Competence~~ Centre shall not divulge to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment, in whole or in part, has been made.
2. Members of the Governing Board, the Executive Director, the members of the Industrial and Scientific Advisory Board, external experts participating in ad hoc Working Groups, and members of the staff of the Centre shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union, even after their duties have ceased.

**Commented [A36]:** SE proposes that art 34 and 36 should be collected under one article instead of two

3. The Governing Board of the **Competence** Centre shall adopt the **Competence** Centre's security rules, following approval by the Commission, based on the principles and rules laid down in the Commission's security rules for protecting European Union classified information (EUCI) and sensitive non-classified information including inter alia provisions for the processing and storage of such information as set out in Commission Decisions (EU, Euratom) 2015/443<sup>18</sup> and 2015/444<sup>19</sup>.
4. The **Competence** Centre may take all necessary measures to facilitate the exchange of information relevant to its tasks with the Commission and the Member States and where appropriate, the relevant Union agencies and bodies. Any administrative arrangement concluded to this end on sharing EUCI or, in the absence of such arrangement, any exceptional ad hoc release of EUCI shall have received the Commission's prior approval.

**Commented [A37]:** The regulation should also have a reference to the Council decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU)

#### *Article 37*

##### **Access to documents**

1. Regulation (EC) No 1049/2001 shall apply to documents held by the **Competence** Centre.
2. The Governing Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001 within six months of the establishment of the **Competence** Centre.
3. Decisions taken by the **Competence** Centre pursuant to Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the Ombudsman under Article 228 of Treaty on the Functioning of the European Union or of an action before the Court of Justice of the European Union under Article 263 of Treaty on the Functioning of the European Union.

<sup>18</sup> Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).

<sup>19</sup> Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

### Article 38

#### Monitoring, evaluation and review

1. The ~~Competence~~ Centre shall ensure that its activities, including those managed through the National Coordination Centres and the Network, shall be subject to continuous and systematic monitoring and periodic evaluation. The ~~Competence~~ Centre shall ensure that the data for monitoring programme implementation and results are collected efficiently, effectively, and in timely manner and proportionate reporting requirements shall be imposed on recipients of Union funds and Member States. The outcomes of the evaluation shall be made public.
2. Once there is sufficient information available about the implementation of this Regulation, but no later than three and a half years after the start of the implementation of this Regulation, the Commission shall carry out an interim evaluation of the ~~Competence~~ Centre. The Commission shall prepare a report on that evaluation and shall submit that report to the European Parliament and to the Council by 31 December 2024. The ~~Competence~~ Centre and Member States shall provide the Commission with the information necessary for the preparation of that report.
3. The evaluation referred to in paragraph 2 shall include an assessment of the results achieved by the ~~Competence~~ Centre, having regard to its objectives, mandate and tasks. If the Commission considers that the continuation of the ~~Competence~~ Centre is justified with regard to its assigned objectives, mandate and tasks, it may propose that the duration of the mandate of the ~~Competence~~ Centre set out in Article 46 be extended.
4. On the basis of the conclusions of the interim evaluation referred to in paragraph 2 the Commission may act in accordance with [Article 22(54)] or take any other appropriate actions.
5. The monitoring, evaluation, phasing out and renewal of the contribution from Horizon Europe will follow the provisions of articles 8, 45 and 47 and Annex III of the Horizon Europe Regulation and agreed implementation modalities.
6. The monitoring, reporting and evaluation of the contribution from Digital Europe will follow the provisions of articles 24, 25 of the Digital Europe programme.
7. In case of a winding up of the ~~Competence~~ Centre, the Commission shall conduct a final evaluation of the ~~Competence~~ Centre within six months after the winding-up of the ~~Competence~~ Centre, but no later than two years after the triggering of the winding-up procedure referred to in Article 46 of this Regulation. The results of that final evaluation shall be presented to the European Parliament and to the Council.

*Article 39*

**Liability of the Competence Centre**

1. The contractual liability of the Competence Centre shall be governed by the law applicable to the agreement, decision or contract in question.
2. In the case of non-contractual liability, the Competence Centre shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its staff in the performance of their duties.
3. Any payment by the Competence Centre in respect of the liability referred to in paragraphs 1 and 2 and the costs and expenses incurred in connection therewith shall be considered to be expenditure of the Competence Centre and shall be covered by its resources.
4. The Competence Centre shall be solely responsible for meeting its obligations.

*Article 40*

**Jurisdiction of the Court of Justice of the European Union and applicable law**

1. The Court of Justice of the European Union shall have jurisdiction:
  - a) pursuant to any arbitration clause contained in agreements, decisions or contracts concluded by the Competence Centre;
  - b) in disputes related to compensation for damage caused by the staff of the Competence Centre in the performance of their duties;
  - c) in any dispute between the Competence Centre and its staff within the limits and under the conditions laid down in the Staff Regulations.
2. Regarding any matter not covered by this Regulation or by other Union legal acts, the law of the Member State where the seat of the Competence Centre is located shall apply.

*Article 41*

**Liability of members and insurance**

1. The financial liability of the members for the debts of the Competence Centre shall be limited to their contribution already made for the administrative costs.
2. The Competence Centre shall take out and maintain appropriate insurance.

*Article 42*

**Conflicts of interest**

The ~~Competence~~ Centre Governing Board shall adopt rules for the prevention and management of conflicts of interest in respect of its members, bodies and staff. Those rules shall contain the provisions intended to avoid a conflict of interest in respect of the representatives of the members serving in the Governing Board as well as the Scientific and Industrial Advisory Board in accordance with Regulation XXX [new Financial Regulation].

*Article 43*

**Protection of Personal Data**

1. The processing of personal data by the ~~Competence~~ Centre shall be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council.
2. The Governing Board shall adopt implementing measures referred to in Article xx(3) of Regulation (EU) No xxx/2018. The Governing Board may adopt additional measures necessary for the application of Regulation (EU) No xxx/2018 by the ~~Competence~~ Centre.

*Article 44*

**Support from the host Member State**

An administrative agreement may be concluded between the ~~Competence~~ Centre and the Member State ~~(Belgium)~~ in which its seat is located concerning privileges and immunities and other support to be provided by that Member State to the ~~Competence~~ Centre.

## CHAPTER VII

### FINAL PROVISIONS

#### *Article 45*

##### **Initial actions**

1. The Commission shall be responsible for the establishment and initial operation of the ~~Competence~~ Centre until it has the operational capacity to implement its own budget. The Commission shall carry out, in accordance with Union law, all necessary actions with the involvement of the competent bodies of the ~~Competence~~ Centre.
2. For the purpose of paragraph 1, until the Executive Director takes up his/her duties following his/her appointment by the Governing Board in accordance with Article 16, the Commission may designate an interim Executive Director and exercise the duties assigned to the Executive Director who may be assisted by a limited number of Commission officials. The Commission may assign a limited number of its officials on an interim basis.
3. The interim Executive Director may authorise all payments covered by the appropriations provided in the annual budget of the ~~Competence~~ Centre once approved by the Governing Board and may conclude agreements, decisions and contracts, including staff contracts following the adoption of the ~~Competence~~ Centre's staff establishment plan.
4. The interim Executive Director shall determine, in common accord with the Executive Director of the ~~Competence~~ Centre and subject to the approval of the Governing Board, the date on which the ~~Competence~~ Centre will have the capacity to implement its own budget. From that date onwards, the Commission shall abstain from making commitments and executing payments for the activities of the ~~Competence~~ Centre.

*Article 46*

**Duration**

1. The ~~Competence~~ Centre shall be established for the period from 1 January 2021 to 31 December 2029.
2. At the end of this period, unless decided otherwise through a review of this Regulation, the winding-up procedure shall be triggered. ~~The winding-up procedure shall be automatically triggered if the Union or all participating Member States withdraw from the Competence Centre.~~
3. For the purpose of conducting the proceedings to wind up the ~~Competence~~ Centre, the Governing Board shall appoint one or more liquidators, who shall comply with the decisions of the Governing Board.
4. When the ~~Competence~~ Centre is being wound up, its assets shall be used to cover its liabilities and the expenditure relating to its winding-up. Any surplus shall be distributed among the Union and the ~~participating Member State~~ **contributing Member States** in proportion to their financial contribution to the ~~Competence~~ Centre. Any such surplus distributed to the Union shall be returned to the Union budget.

*Article 47*

**Entry into force**

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

*For the European Parliament*  
*The President*

*For the Council*  
*The President*

---