Council of the European Union

Brussels, 28 May 2020
(OR. en)

8315/20

Interinstitutional File: 2018/0328(COD)

LIMITE

CYBER 79
TELECOM 75
CODEC 417
COPEN 136
COPS 162
COSI 89
CSC 146
CSCI 37
IND 62
JAI 412
RECH 184
ESPACE 21

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	5341/5/20, 13469/19, 7583/19
No. Cion doc.:	12104/18
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 - Mandate for negotiations with European Parliament

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (13.07.2020)

I. INTRODUCTION

1. In October 2017, the European Council called for the Commission's cybersecurity proposals to be developed in a holistic way, delivered timely and examined without delay, on the basis of an action plan to be set up by the Council.

2. On 12 September 2018, in the context of its Digital Single Market Strategy, the Commission adopted and transmitted to the Council and to the European Parliament the 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. with Articles 173(3) and 188 TFEU as a legal basis[1].

3. This proposal provides for the creation of a centre which would be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development. It would also deliver cybersecurity-related financial support from Horizon Europe and Digital Europe programmes. As stated above, the proposal provides for the setting up of the Network of National Coordination Centres and a Cybersecurity Competence Community.

4. The Centre would be:

(i) co-governed by the Member States and the Commission, and the aim would be to

i. ensure stronger coordination between research and innovation as well as deployment strategies at the EU and national level;

ii. enable the Member States to take decisions related to their financial contribution to the joint actions and

(ii) able , in accordance with the above governance (i.e. Commission and Member States), to implement research and innovation actions (supported from Horizon Europe) as well as capacity building actions (supported by Digital Europe Programme).

[1] 12104/18

(iii) able together with Member States to support the build-up and procurement of advanced cybersecurity equipment, tools and data infrastructures in Europe and ensure a wide deployment of the latest cybersecurity solutions across the economy (as also indicated in the Digital Europe Programme's Partial General Approach). To this end, the Centre would also be able to facilitate the shared acquisition of capacities on behalf of Member States.

5. Within the European Parliament, the file was assigned to the Committee on Industry, Research and Energy (ITRE) and Ms. Julia REDA (ITRE, Greens/EFA) was appointed as rapporteur in the previous legislative period. The report was adopted on 19 February 2019 in ITRE committee and voted by Parliament during the March I 2019 plenary. The Parliament adopted its position at first reading on 17 April 2019. After the European elections a new rapporteur was appointed, Mr Rasmus ANDRESEN (ITRE, Greens/EFA).

6. The European Economic and Social Committee adopted its opinion on 23 January 2019.

II. WORK WITHIN THE COUNCIL

7. The Horizontal Working Party (HWP) on Cyber Issues started to discuss the proposal on 17 September 2018 when the Commission gave a general presentation. The impact assessment was presented at the meeting of the HWP on Cyber Issues on 28 September 2018. The text of the draft Regulation was then examined at various meetings of the HWP on Cyber Issues under the Romanian Presidency.

8. On 13 March 2019, COREPER agreed on the text of a mandate for negotiations with the European Parliament and two trilogues were held. The first informal trilogue was held on 13 March in Strasbourg where both co-legislators confirmed their commitment to reaching an agreement as soon as possible. A second trilogue was held on 20 March. Some substantial issues such as the Centre's mission and tasks, financing and the Governing Board were discussed. A third trilogue was provisionally scheduled to take place on 28 March in Strasbourg, provided that enough progress was being made by the Council and the EP. On 27 March 2019, COREPER could not reach agreement on a revised mandate, and as a consequence, the third informal trilogue was cancelled.

9. After the establishment of the Common Understanding in March 2019 between the Council and the Parliament on the Horizon Europe Regulation, the Commission expressed the view that there was a legal incompatibility between that Common Understanding and the mandate for negotiations on the Cyber Regulation, notably in respect of the financial provisions as set out, in particular, in Article 21 of that Regulation. The question was discussed in the Horizontal Working Party on Cyber Issues which invited the Council Legal Service to present a written opinion on the compatibility of the two legal acts, insofar as the Union contribution from Horizon Europe to the Centre was concerned.

10. On 18 June 2019, Council Legal Service submitted an opinion (9320/19) advising that some changes should be made to the proposed CCCN Regulation to avoid inconsistency with the Horizon Europe Regulation.

11. During the Finnish Presidency, the necessary amendments as advised by the Council Legal Service were introduced in the provisions regarding the funding processes (in particular Article 21) to ensure compliance with the Horizon Europe Regulation. On request of the Presidency the Commission suggested text amendments in September 2019 which were subject to in-depth discussions at several meetings of the HWP on CI.

12. On 13 November 2019 Coreper was asked to provide quidance on the most appropriate way ahead. Following the outcome of Coreper, discussions continued at the level of the Horizontal Working Party and some workshops were organised by the Commission, in cooperation with the Presidency, to clarify certain topics such as the joint actions.

13. The HR Presidency prepared a new draft of the Regulation which has been discussed at several meetings of the HWP since the beginning of January 2020. This new draft included some important changes compared to the previous mandate (7583/19), notably:

- the introduction of a definition of in-kind contribution (Art 2(4))
- the distinction between the strategic tasks and the implementation tasks of the Centre (Art 4a)
- the introduction of the Cybersecurity Industrial, Technology and Research Agenda ("the Agenda")
- clarifications regarding the nature of the Centre and the National Coordination Centres
- a stronger emphasis on ENISA (permanent observer in the Management Board) and the importance of avoiding duplication of activities with ENISA.
- the deletion of the Industrial and Scientific Advisory Board (Articles 18, 19, 20)
- the further elaboration of the review clause (Art. 38)
- clarifications regarding the concept of voluntary contribution (Art. 21)

14. **DELETED**

DELETED

15. The Presidency is of the opinion that its compromise text, as set out in the Annex, reflects efforts of the Presidency and Member States to strike a proper balance in the text. All changes compared to the Commission proposal are indicated in **bold** or strikethrough. The changes compared to the latest mandate of March 2019 are indicated in **bold underlined** and all deletions are in **bold underline strikethrough**.

III. CONCLUSION

16. The Permanent Representatives Committee is therefore invited to endorse the revised mandate for negotiations with the European Parliament as laid down in the Annex of this note.

ANNEX

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~~

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[2],

Having regard to the opinion of the Committee of the Regions[3],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Our daily lives and economies **are** becom**ing** increasingly dependent on digital technologies, **and** citizens become more and more exposed to serious cyber incidents. Future security depends, among other~~s~~ **things**, 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.

[2] OJ C , , p. .
[3] OJ C , , p. .

(2) The Union has steadily increased its activities to address growing cybersecurity challenges following the ~~2013~~ Cybersecurity Strategy **put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy ("High Representative") in their Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" ("the 2013 Cybersecurity Strategy"). The 2013 Cybersecurity Strategy** 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[4] 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 **to the European Parliament and the Council entitled** "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."

[4] 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).

(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 **research and** technological capacities to secure its Digital Single Market **as outlined by the Commission in its Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled "A Digital Single Market Strategy for Europe",** and in particular to protect critical network~~s~~ 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, networked and 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 **N**etwork of **C**ybersecurity **C**ompetence **C**entres, **together** with ~~**the**~~ **a** European **Cybersecurity** Research and Competence Centre and propose by mid-2018 the relevant legal instrument.

(7a) [The decision regarding the seat of the European Cybersecurity Industrial, Technology and Research Centre (the "Centre") will be taken by common agreement between the Representatives of the Governments of the Member States. It is imperative for the proper and efficient performance of its tasks, for staff recruitment and retention and for enhancing the efficiency of networking and coordination activities that the Centre be based in an appropriate location, among other things providing appropriate transport connections and facilities for spouses, partners 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.]

(7b) The Union still lacks sufficient technological and industrial capacities and capabilities to autonomously secure its economy and critical infrastructures and to become a global leader in cybersecurity field. There is an insufficient level of strategic and sustainable coordination and cooperation between industries, cybersecurity research communities and governments; the EU suffers from subscale investment and limited access to cybersecurity know- how, skills and facilities across Europe; and few European cybersecurity research and innovation outcomes are translated into marketable solutions and widely deployed across the economy.

(7c) The option of creating a network of national coordination centres, together with a European Cybersecurity Industrial, Technology and Research Centre, with a dual mandate to pursue measures in support of industrial technologies, as well as in the domain of research and innovation, is best suited to achieve the goals of this ~~initiative~~ Regulation, while offering the highest economic, societal, and environmental impact and safeguarding the Union's interests.

(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~~ a** ~~Cybersecurity Competence~~ Network **of National Coordination Centre ("the Network"). The Centre ~~It~~** should deliver cybersecurity-related financial support from **~~the~~** Horizon Europe - **the Framework Programme for Research and Innovation established by Regulation 2020/… of the European Parliament and of the Council[5] ('the Horizon Europe programme')** and **the** Digital Europe **programme established by Regulation 2020/… of the European Parliament and of the Council[6] ('the Digital Europe** programmeand should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating fin~~-s~~**'),** ancial support related to cybersecurity research, innovation, technology and industrial development and avoiding **unnecessary** duplication**.**

8a) The Centre should not play an operational role nor provide operational technical assistance. Upon request from a Member State the Centre, within the scope of its mandate, should be able to provide expert cybersecurity industrial, technological, and research advice to that Member State.

5 Regulation 2020/… of the European Parliament and of the Council, of …, establishing Horizon Europe - the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination (OJ …) [2018/0224(COD)].

6 Regulation 2020/… of the European Parliament and of the Council, of …, establishing the Digital Europe programme for the period 2021-2027 (OJ …) [2018/0227(COD)].

(8aa) The Centre would benefit from the ~~particular~~ ~~expertise~~ experience and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity between the Commission and European Cyber Security Organisation ECSO Association during the duration of the Framework Programme for Research and Innovation (2014-2020) ("Horizon 2020"), established by Regulation (EU) No 1291/2013 of the European Parliament and of the Council[7], and the lessons learned from four pilot projects[8] launched in early 2019 under Horizon 2020, for the management of the Cybersecurity Competence Community, and the representation of the Cybersecurity Competence Community in the Centre.

(9) The Centre should develop and monitor the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda ~~Strategy~~ which will set out strategic recommendations and priorities for development and growth of the European cybersecurity ~~ecosystem~~ industrial, technological and research sector (the "Agenda"). The Agenda should provide the basis for the annual and multi-annual work programme of the Centre. Furthermore, the Agenda should provide guidance ~~advice~~ in particular within the planning and implementation of the Horizon Europe programme and the Digital Europe programme in the area of cybersecurity. The Agenda could also serve as cybersecurity industrial, technological, and research guidance ~~advice~~, where relevant, for the implementation of other Union programmes.

---

7 Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC (OJ L 347, 20.12.2013, p. 104).

8 CONCORDIA, ECHO, SPARTA and CyberSec4Europe are the four winning pilot projects of the 2018 Horizon 2020 cybersecurity call "establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap".

(9a) When the Centre is preparing its annual work programme ("annual work programme"), it should inform the Commission on its co-funding needs based on the Member States' planned co-funding contributions to joint actions, in order for the Commission to take into account the Union matching contribution in the preparation of the draft general budget for the following year.

(9b) Where the Commission prepares the work programme of the Horizon Europe programme for matters related to cyber security, including in the context of its stakeholder consultation process and particularly before the adoption of that work programme, the Commission should take into account the input of the Centre and share ~~such~~ that input with the Programme Committee of the Horizon Europe programme.

(9c) In order to support its role in the area of cybersecurity and the involvement of the Network and to provide a strong governance role for the Member States, the Centre should be established as a Union body with legal personality. The Centre should perform a dual role by undertaking specific tasks in the area of cybersecurity industry, technology and research as laid down in this Regulation and by managing cybersecurity related funding from several programmes at the same time – notably the Horizon Europe programme and the Digital Europe programme, and possibly even further Union programmes. Such management ~~must~~ is to be in accordance with the rules applicable to those programmes. Nevertheless, considering that the funding for the functioning of the Centre would originate primarily from the Digital Europe programme and the Horizon Europe programme~~s~~, it is necessary that the Centre is considered as a partnership for the purpose of budget implementation, including the programming phase.

~~(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")**~~, **which should be** made up of National Coordination Centres, **one** ~~**in**~~ **from** 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 **their** activities related to this Regulation.

(12) National Coordination Centres should be **public sector entities, or entities with a majority of public participation, performing public administrative functions under national law, including by means of delegation, and they should be** selected by Member States. **The functions of a National Coordination Centre in a given Member State can be carried out by** ~~**the same**~~ **an entity that carries out** ~~**also fulfilling**~~ **other functions arising** ~~**created**~~ **under Union law, such as those of a national competent authority,** ~~**and/or**~~ **a single point of contact in the meaning of** ~~**the NIS**~~ **Directive (EU) 2016/1148, any other EU Regulation, or a digital innovation hub in the meaning of the Digital Europe programme. Other public sector entities or entities performing public administrative functions in a Member State could assist the National Coordination Centre in that Member State, in carrying out its functions.**

(12a) ~~**In addition to the necessary administrative capacity**~~, **The National Coordination** Centres **should have the necessary administrative capacity and** should ~~either~~ possess or have ~~direct~~ access to cybersecurity **industrial, technological and research** 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~~ **and be in a position** 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~~[9], and the research community.

(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.**~~

The National Coordination Centres may receive grants from the Centre in order to provide financial support to third parties in the form of grants. The direct cost incurred by the National Coordination Centres for the provision and administration of financial support to third parties shall be eligible for funding.

~~[9] 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).~~

(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 **products and** solutions. At the same time the ~~Competence~~ Centre and the Network should ~~be at the service of~~ **promote the cybersecurity capability of the demand side industry, in particular by ~~activities~~ supporting** developers and operators in ~~critical~~ sectors such as transport, energy, health, financ**~~ial~~e**, government, telecom, manufacturing, **~~defence~~**, and space to help them solve their cybersecurity challenges**, for example in order to achieve security-by-design. They should also support the deployment of cybersecurity products and solutions while promoting, where possible, the implementation of the European cybersecurity certification framework as defined by Regulation (EU) 2019/881 of the European Parliament and of the Council[10].**

[10] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ 151, 7.6.2019, p. 15).

(15) The ~~Competence~~ Centre ~~should have several key functions. First, the Competence Centre~~ should **~~facilitate and~~** ~~help~~ **~~coordinate the work of the European Cybersecurity Competence Network and nurture~~** **support** the Cybersecurity Competence Community. The Centre should ~~drive~~ **implement cybersecurity relevant parts of the Digital Europe programme and the Horizon Europe programme in accordance with ~~its~~ the Centre's multiannual work programme ("multiannual work programme") and the annual ~~strategic~~ work programme and the strategic planning process of the Horizon Europe programme by allocating grants and other forms of funding, ~~typically~~ primarily following a competitive call for proposals** ~~the cybersecurity technological agenda **in accordance with its multi-annual strategic plan**, and~~ facilitate **transfer of** ~~access to the~~ expertise ~~gathered~~ in the Network and the Cybersecurity Competence Community **and .** ~~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~~ **support** joint investment by the Union, Member States **~~and~~**/or industry.

(16) ~~The Competence Centre and the National Coordination Centres 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 **multiannual** work **programme and the annual** work **programme ~~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 of the~~ **Centre and the Network ~~to~~ should** provide **access to** cybersecurity knowledge ~~and technical assistance to industries should refer to~~ **in** both **information and communications technology** (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 exchange of knowledge** between the cybersecurity civilian and defence spheres, projects **under this Regulation** financed by the Horizon Europe Programme **should** be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe **are to** have a**n exclusive** focus on civil applications.

~~(18a) This Regulation should not utilise resources from Horizon Europe to fund projects which have a focus on military 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~~ **its** expertise in cybersecurity **and its mandate as a reference point for advice and expertise on cybersecurity for Union institutions, agencies and bodies, as well as for relevant Union stakeholders, ~~as well as~~ and in view of its collection of input through its tasks**, **~~for instance on cybersecurity certification and standardisation~~** the European Union **Agency** for Cybersecurity **~~(ENISA)~~ as established by Regulation (EU) 2019/881** ("ENISA") should play an active part in the activities of the Centre including the development of the Agenda, avoiding any duplication of their tasks in particular through its role as permanent observer in the Governing Board **of the Centre ("Governing Board")**. **Regarding the drafting of the Agenda, the annual work programme and the multiannual work programme, the Executive Director of the Centre ("Executive Director") and the Governing Board should take into account any relevant strategic advice and input provided by ENISA, according to the rules of procedure set by the Governing Board.**

(22) Where they receive a financial contribution 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 th**is ~~present initiative~~ Regulation**.

~~(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 **representatives from** the Member States and the Commission, should define the general direction of the ~~Competence~~ Centre's operations, and ensure that **the Centre ~~it~~** carries out its tasks in accordance with this Regulation. The Governing Board should **adopt the Agenda consisting of strategic goals that have to be fulfilled by the Centre.**

(24a) The Governing Board should be entrusted with the powers necessary to establish the budget **of the Centre**, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the ~~Competence~~ Centre, adopt the ~~Competence~~ **~~Centre's~~ annual** work **programme** and the multiannual **work programme** reflecting the priorities **set in the Agenda** 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.

(24b) The Governing Board should have an oversight of the strategic and implementation activities of the Centre and ensure the synergy between them. In its annual report the Centre should put special emphasis on the achieved realisation of its strategic goals and, if necessary, propose actions for further improvement of ~~the~~ such realisation.

(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 **r**epresentatives on the Governing Board in order to ensure continuity in its work.

(26) The smooth functioning of the ~~Competence~~ Centre requires that ~~its~~ **the** 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~~ **The Cybersecurity Competence Community should act also** as a **source of advice** ~~ensure~~ **through** regular dialogue ~~of~~ **between the Centre** ~~with~~ **and** the private sector, consumers' organisations, **academia** 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 **Cybersecurity Competence Community** ~~Industrial and Scientific Advisory Board~~ and the tasks assigned to it, such as ~~being consulted~~ **providing advice** regarding the **annual** work **programme and the multiannual work programme**, should ensure sufficient representation of stakeholders in the work of the ~~Competence~~ Centre.

(28) ~~The Competence Centre should benefit from the particular experteseexperience and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity during the duration of Horizon 2020, and the four pilot projects, thereby building on the existing experience that has been set up by the contractual public-private partnership on cybersecurity, for the management of the Community, and the representation of the Community in the Centre. through its Industrial and Scientific Advisory Board.~~

(28a) Contributions of the Member States to the resources of the Centre can be financial and/or in-kind. Financial contributions could for example consist of a grant given by a Member State to a beneficiary in that Member State complementing Union financial support to a project under the annual work programme. On the other hand, in-kind contributions would typically accrue where a Member State entity is itself the beneficiary of a Union financial support. For example, if the Union subsidised an activity of a National Coordination Centre at the financing rate of 50%, the remaining cost ~~will~~ would be accounted for as in-kind contribution. In another example, where a Member State entity received Union financial support for creating or upgrading an infrastructure to be shared among stakeholders in line with the annual work programme, the related non-subsidised costs ~~are~~ would be accounted for as in-kind contributions.

(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[11]. Processing of personal data by the ~~Competence~~ Centre will be subject to Regulation (EU) No **1725**/2018 of the European Parliament and of the Council[12]. The ~~Competence~~ Centre should comply with the provisions applicable to **~~the~~** Union institutions and with national **~~legislation~~ law** 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 (EU, Euratom) **2018/1046** of the European Parliament and of the Council[13] **~~[the Financial Regulation]~~**.

---

11 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).

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

13 **Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).**

(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 **research,** 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 **alone** due **to** 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 **those** objective**s,**

HAVE ADOPTED THIS REGULATION:

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~~ have an essential role in** ~~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 **3.1.3. ~~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].~~

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 law~~s~~ of that Member State. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings.

~~**4a. The seat of the Competence Centre shall be located in [XXXBrussels, Belgium].**~~

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~~ **the activities necessary to protect** network and information systems**, the** users **of such systems**, and other persons **affected by** ~~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**es** with the specific purpose of protecting network and information systems, the~~ir~~ users **of such systems** and **other ~~affected~~** persons **affected by** ~~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.~~

(3) "joint action~~s~~" means an action included in the ~~Centre's~~ annual work programme receiving Union financial support from the Horizon Europe programme and/or Digital Europe programme, in accordance with their Regulations, as well as financial or in-kind support by one or more Member States, which are implemented via projects involving beneficiaries established in the Member States which provide financial or in-kind support to those beneficiaries stemming from those Member States.

(4) "in-kind contribution" means those eligible costs, incurred by National Coordination Centres and other public entities when participating in projects funded through this Regulation, which are not financed by a Union contribution or by financial contributions by Member States.

Article 3

Mission of the ~~Competence~~ Centre and the Network

1. The ~~Competence~~ Centre and the Network shall help the Union to:

(a) **strengthen its strategic autonomy in the field of ~~retain and develop,~~ the cybersecurity by retaining and developing the Union's research,** technological and industrial **cybersecurity** capacities **and capabilities** necessary to ~~**strengthen**~~ **enhance trust and** security **in** ~~secure~~ **the** Digital Single Market;

(b) increase the **global** competitiveness of the Union's cybersecurity industry and turn cybersecurity into **a** competitive advantage of other Union industries.

2. The ~~Competence~~ Centre **and the Network** shall undertake **their** ~~its~~ tasks, where appropriate, in collaboration with **ENISA and** ~~the Network of National Coordination Centres and a~~ **the** Cybersecurity Competence Community.

2a. Only actions contributing to the missions~~s~~ set out in paragraph 1 shall be eligible for support through Union financial assistance in accordance with the legal acts establishing relevant programmes notably Horizon Europe and Digital Europe.

Article ~~4~~

Objectives ~~and Tasks~~ of the Centre

The ~~Competence~~ Centre shall **enhance the coordination of research, innovation and deployment in the field of cybersecurity in order to fulfil the missions as described in Article 3 ~~and strengthen the competitiveness of the European Union and its Digital Single Market~~, by:**

(1) defining strategic orientations and priorities for research, innovation and deployment in cybersecurity in line with Union law;

(2) implementing actions under relevant Union funding programmes in line with the defined Union's strategic orientations; and

(3) stimulating cooperation and coordination within National Coordination Centres and the Cybersecurity Competence Community. ~~have the following objectives and related tasks:~~

~~1. facilitate and help coordinate the work of the National Coordination Centres Network ('the Network') referred to in Article 6 and the Cybersecurity Competence Community referred to in Article 8;~~

2. contribute to the implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX[14] 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[15] 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];

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;

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:

(d) stimulating cybersecurity research, development and the uptake of Union cybersecurity products and solutions by public authorities and user industries;

(e) assisting public authorities, demand side industries and other users in adopting and integrating the latest cyber security solutions;

---

14 [add full title and OJ reference]
15 [add full title and OJ reference]

(f) 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;

(g) 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:

(h) 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:

(i) providing financial support to cybersecurity research efforts based on a common, continuously evaluated and improved multiannual strategic, industrial, technology and research agenda;

(j) support large-scale research and demonstration projects in next generation cybersecurity technological capabilities, in collaboration with the industry and the Network;

(k) support research and innovation for standardisation in cybersecurity technology

7. enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, by carrying out the following tasks:

(l) supporting Member States and industrial and research stakeholders with regard to research, development and deployment;

(m) contributing to cooperation between Member States by supporting education, training and exercises ;

(n) 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:

(o) providing advice, sharing expertise and facilitating collaboration among relevant stakeholders;

(p) 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].

Article 4a

Tasks of the Centre

1. In order to fulfill the mission laid out in Article 3 and the objectives laid out in Article 4, the Centre shall, in close cooperation with the Network, have the following tasks:

(a) strategic tasks, consisting of:

(1) developing and monitoring the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda, which ~~will~~ shall set out strategic recommendations and ~~goals~~ priorities for the development and growth of the European cybersecurity industrial, technological and research sector~~ecosystem~~ (the "Agenda");

(2) **through the Agenda and the multiannual work programme, while avoiding any duplication of activities with ENISA and taking into account the need to create synergies between cybersecurity and other parts of Horizon Europe and Digital Europe programmes**:

(i) defining priorities for its work on:

- the enhancement of cybersecurity research **and innovation** and its deployment,

- **the development of** cybersecurity **industrial, technological and research** capacities **~~and~~** capabilities, **~~skills~~** and infrastructure,

- **the reinforcement of cybersecurity industrial, technological and research skills and training and**

- the deployment of cybersecurity products and solutions, and

(ii) supporting cybersecurity industry, with a view to strengthening **Union** excellence, capacities and competitiveness on cybersecurity;

(**3**) ensuring synergies and cooperation with relevant Union institutions, agencies and bodies such as ENISA **while avoiding any duplication of activities with such Union institutions, agencies and bodies**;

(4) coordinating National Coordination Centres through the Network and ensuring regular exchange of expertise;

(5) providing expert cybersecurity industrial, technology and research advice upon request from a Member State to that Member State;

(**6**) **facilitating collaboration and sharing of expertise among relevant stakeholders, in particular members of the Cybersecurity Competence Community; ~~this may include financially supporting education, training, exercises and building up cyber security skills;~~**

(**7**) **facilitating** the use of results from research and innovation projects in actions related to the development of cybersecurity products and solutions, seeking to avoid fragmentation and duplication of efforts and ~~**to**~~ replicat**ing** good cybersecurity practices and **cybersecurity** products and solutions, including those developed by **small and medium enterprises (**SMEs**)** and those based on open-source software; ~~Support to the deployment of cybersecurity products and solutions should to the extent possible rely on the European cybersecurity certification framework as defined by the Cybersecurity Act.~~

(b) implementation tasks, consisting of:

(1) coordinating and administrating the work of the Network and the Cybersecurity Competence Community in order to achieve the mission set out in Article 3, in particular supporting cybersecurity start-ups and SMEs in the ~~European~~ Union and facilitating their access to expertise, funding, investment and to markets;

(2) **establishing and implementing the ~~Centre's~~ annual work programme, in accordance with the Agenda and the multiannual work programme, for the cybersecurity parts of:**

(i) **the Digital Europe programme and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme],**

(ii) **joint actions receiving support from the cybersecurity parts of the Horizon Europe programme and in particular Section 3.1.3. 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 in accordance with the multiannual work programme, and the strategic planning process of the Horizon Europe programme, and**

(iii) **other Union programmes when provided for in legal acts of the Union;**

(3) **providing expert advice on cybersecurity industry, technology and research to the Commission when it prepares ~~its~~ the draft work programmes pursuant to Article 11 of Council Decision (XXXX)[16];**

~~16~~ Council Decision …, of …, on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation (OJ …) [2018/0225(COD)].

(4) enabling the deployment and facilitating the acquisition of cybersecurity infrastructures, at the service of industries, the public sector, ~~and~~ research communities and operators of essential services, through inter alia ~~voluntary~~ contributions from Member States and Union funding for joint actions, in line with the Agenda, the multiannual work programme and the annual work programme. ~~EU funding shall not be conditioned to voluntary funding from Member States;~~

(5) without prejudice to the civilian nature of projects to be financed from the Horizon Europe programme and the Digital Europe programme and in line with the respective program regulations, enhancing synergies and exchange of knowledge and coordination between the cybersecurity civilian and defence spheres;

(c) monitoring the fulfilment of the strategic and implementation tasks and, whenever necessary, providing proposals for the enhancement of their realisation.

2. In accordance with Article 6 of the Horizon Europe Framework programme and subject to the conclusion of a contribution agreement as referred to in point (18) of Article 2 of Regulation (EU, Euratom) 2018/1046, the Centre may be entrusted with the implementation of the cybersecurity parts that are not co-funded by the Member States in the Horizon Europe Programme [established by Regulation No XXX and in particular Section 3.1.3. 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]

~~*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 **an** entity to act as the National Coordination Centre for the purposes of this Regulation and notify it **without delay** to the **Governing Board ~~of the Centre~~** ~~Commission~~**. Such entity may be an entity already established in that Member State.**

2. On the basis of **the nomination by a Member State of an entity which fulfils** the criteria laid down in paragraph 4, the ~~Commission~~ **Governing Board** shall ~~issue a decision within 6 months from the nomination transmitted by the Member State providing for the accreditation~~ **register** **list that** entity as a National Coordination Centre **no later than 3 months after the nomination** ~~or rejecting the nomination~~. The list of National Coordination Centres shall be published by the **Centre** ~~**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 **the** nomination of any new entity.

4. The ~~**nominated**~~ National Coordination Centre shall ~~have~~ **be a public sector entity or an entity with a majority of public participation performing public administrative functions under national law, including by means of delegation**~~**, subject to public law obligations**~~ **and having** the capability to support the ~~Competence~~ Centre and the Network in fulfilling their mission laid out in Article 3 of this Regulation. ~~They~~ **It** shall **either** possess or have ~~direct~~ access to **research and** technological expertise in cybersecurity**.** ~~and be in a position~~ **It shall** ~~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**~~ **,** and the research community. **It shall also have the administrative capacity to manage funds.**

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.

Article 7

Tasks of the National Coordination Centres

1. The National Coordination Centres shall have the following tasks:

(a) **acting as contact point<u>s</u> at the national level for the Cybersecurity Competence Community <u>to</u>** support~~ing~~ the ~~Competence~~ Centre in achieving its objective **and mission~~s~~**~~, and~~ in particular in coordinating the Cybersecurity Competence Community **through the coordination of its national members**;

(aa) providing expertise <u>and</u> <u>actively</u> <u>contributing</u> to the strategic ~~planning of the activities according to~~ tasks referred to <u>in</u> Article 4a, taking into account relevant <u>national and regional</u> challenges for cybersecurity <u>in</u> different sectors;

(b) facilitating the participation of industry**, research institutions** 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**, such as including national policies on research, development and innovation in the area of cybersecurity, and in particular those policies 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~~ accordance** with Article 204 of Regulation **(EU, Euratom) 2018/1046** under conditions specified in the **~~concerned~~** grant agreements **concerned**;

(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 **National** Coordination Centre for becoming part of the Cybersecurity Competence Community;

(i) advocating and promoting involvement by relevant entities in the activities arising from the Centre, Network and Cybersecurity Competence Community, and monitoring, as appropriate, the level of engagement with and grant actions awarded for cybersecurity research, developments and deployments.

2. For the purposes of point (f) **of paragraph 1 of this Article,** the financial support to third parties may be provided in any of the forms specified in Article 125 of Regulation **(EU, Euratom) 2018/1046,** including in the form of lump sums.

3. National Coordination Centres may receive a grant from the Union in accordance with **point (d) of the first paragraph of** Article 195 (d) of Regulation **(EU, Euratom) 2018/1046** 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), (c), 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 **and the Network** as laid down in Article 3 and enhance and disseminate cybersecurity expertise across the Union.

2. The Cybersecurity Competence Community shall, **on the one hand,** consist of industry, academic and non-profit research organisations, **other relevant civil society** ~~and~~ associations as well as public entities and other entities dealing with **cybersecurity** operational and technical matters **and, on the other hand, where relevant, actors of sectors having an interest in cybersecurity and facing cybersecurity challenges**. It shall bring together the main stakeholders with regard to cybersecurity **research,** technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise, **such as ENISA**.

3. Only entities which are established within the Union may be ~~accredited~~ **registered** as members of the Cybersecurity Competence Community. They shall demonstrate that they **can contribute to the missions~~.~~ as set out in Article 3 and shall** ~~-~~have cybersecurity expertise with regard to at least one of the following domains:

(a) research **and innovation**;

(b) industrial **or product** development;

(c) training and education**;**

(d) information security and/or incident response operations;

(e) scientific or technical partnerships or cooperation with academic and/or public authorities ~~**as defined under Article 2(3)**~~**.**

4. The ~~Competence~~ Centre shall ~~accredit~~ **register** 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, **of** whether that entity meets the criteria provided for in paragraph 3 **of this Article**. **That assessment shall also take into account**, **where relevant, any national assessment on security grounds made by the national competent authorities.** A~~n~~ **registration** ~~accreditation~~ shall not be limited in time but may be revoked by the ~~Competence~~ Centre at any time if ~~**the Centre it**~~ ~~or~~ the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 **of this Article** or ~~it~~ falls under the relevant provisions set out in Article 136 of Regulation **(EU, Euratom) 2018/1046, or for justified security reasons**.

4a. The ~~Competence~~ Centre shall ~~accredit~~ **register** relevant **Union** bodies, agencies and offices ~~**of the Union**~~ as members of the Cybersecurity Competence Community after carrying out an assessment whether that **Union body, agency or office** ~~**entity**~~ meets the criteria provided for in paragraph 3 **of this Article**. A~~**n accreditation**~~ **registration** shall not be limited in time but may be revoked by the Competence Centre at any time if it considers that the **Union body, agency or office** ~~**entity**~~ does not fulfil the criteria set out in paragraph 3 **of this Article** or falls under the relevant provisions set out in Article 136 of **(EU, Euratom) 2018/1046** ~~**Regulation XXX [new financial regulation],**~~ **or for justified security reasons following an assessment by the Commission**.

5. The representatives of **the** ~~**Commission**~~ **Union institutions, agencies and bodies** may participate in the work of the **Cybersecurity Competence** Community.

6. The Cybersecurity Competence Community shall designate its own representatives to ensure an efficient and regular dialogue and cooperation with the Centre at Union level. Representatives of the Cybersecurity Competence Community shall have expertise with regard to cybersecurity research, technology and industry. The representation of the Cybersecurity Competence Community ~~**should**~~ **shall be balanced between scientific, industrial and civil society entities, demand and supply side industries, large and small and medium enterprises, as well as in terms of geographical provenance and gender as well as intra-sectorial balance. The requirements and number of representatives shall be further specified by the Governing Board.**

7. The Cybersecurity Competence Community shall through its representatives provide to the Executive Director and the Governing Board strategic advice on the Agenda, annual and multiannual work programme in accordance with the rules of procedure set by the Governing Board. The Cybersecurity Competence Community shall also promote and collect feedback on the annual work programme and the multiannual work programme.

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 Coordinati**on**~~ng~~ Centres;

2. ~~participate in activities promoted by the Competence Centre and National Coordination Centres;~~

3. where relevant, participate in **formal or informal activities and in the** working groups ~~**established by the Governing Board of the Competence Centre**~~ **referred to in point (i) of Article 13(3)** to carry out specific activities as provided by the ~~Competence~~ ~~**Centre's**~~ **annual** work **programme**;

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 **Cybersecurity Competence** 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, avoiding any duplication of efforts** the ~~Competence~~ Centre shall cooperate with relevant Union institutions, bodies, offices and agencies including **~~the European Union Agency for Cybersecurity~~ ENISA** ~~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 **established by Commission Implementing Decision 2013/778/EU**[17]**, the** Innovation and Networks Executive Agency **established by Commission Implementing Decision 2013/801/EU**[18]**, the** European Cybercrime Centre at **the European Union Agency for Law Enforcement Cooperation** (Europol) **established by Regulation (EU) 2016/794 of the European Parliament and of the Council**[19], ~~as well as~~ the European Defence Agency **and other relevant Union entities. The Centre may also cooperate with international organisations, where relevant.**

2. Such cooperation shall take place within the framework of working arrangements. Those arrangements shall be submitted to the ~~prior~~ approval of the **~~Commission~~ Governing Board**.

---

17 Commission Implementing Decision 2013/778/EU of 13 December 2013 establishing the Research Executive Agency and repealing Decision 2008/46/EC (OJ 346, 20.12.2013, p. 54).

18 Commission Implementing Decision 2013/801/EU of 23 December 2013 establishing the Innovation and Networks Executive Agency and repealing Decision 2007/60/EC as amended by Decision 2008/593/EC (OJ 352, 24.12.2013, p. 65).

19 Regulation (EU) 2016/794 of the European Parliament and of the Council, of 11 May 2016, on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

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 **reflect the objectives set out in Article 4 and tasks set out in Article 4a, and** comprise:

   (**a**) a Governing Board which shall exercise the tasks set out in Article 13;

   (**b**) 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. ~~**s**~~

2. Each member of the Governing Board shall have an alternate to represent them in their absence.

2a **Members of the Governing Board and their alternates shall possess adequate knowledge in the field of cybersecurity.**

3. Members of the Governing Board and their alternates **appointed by Member States** shall be **employees of their respective Member State's public sector** appointed in light of their knowledge in the field of technology**, their interlink with their respective National Coordination Centre ~~and~~ or their ~~knowledge in the field as well as~~ of** relevant managerial, administrative and budgetary skills. **Members of the Governing Board and their alternates appointed by the Commission shall be appointed ~~equally~~ in light of their knowledge in the field of technology, or their relevant managerial, administrative and budgetary skills and of their capacity ~~as well as being able~~ to ensure coordination, synergies and, as far as possible, joint initiatives between different Union policies (sectoral and horizontal), involving cybersecurity.** 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 **members of 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 **Governing Board** ~~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 **and shall be responsible for any task that is not specifically allocated to the Executive Director.**

2. The Governing Board shall adopt its rules of procedure. Th**o**se 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) **develop and** **adopt** **the Agenda encompassing strategic goals and priorities for a sustainable development of the European cybersecurity research, technological and industrial sector and monitor its implementation;**

   (aa) **based on the Agenda**, adopt **the** multiannual **work programme**~~,~~ containing **the development of** ~~**a**~~ **common, industrial, technology and research strategic priorities** ~~**roadmap**~~**, which are based on** ~~**the basis of**~~ **the needs identified by Member States in cooperation with the Cybersecurity Competence Community and which require the focus of Union's financial support. Such priorities shall include key technologies and domains for developing the Union's own capabilities in cybersecurity** ~~**strategic autonomy**~~**;** ~~a statement of the major priorities and planned initiatives of the Competence Centre, including an estimate of financing needs and sources;~~

(aaa) adopt the annual work ~~plan~~ programme for implementing the relevant Union funds, notably the cybersecurity parts of the Horizon Europe programme and the Digital Europe programme, in accordance with the Centre's multiannual work programme and the strategic planning process of the Horizon Europe programme ~~including an estimation of thee of financing needs and sources~~; Where appropriate, proposals and in particular the annual work programme shall assess the need to apply security rules as set out in Article 34 of this Regulation, including in particular the security self-assessment procedure in accordance with Article 16 of the [XXXX Horizon Europe Regulation];

(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 **Regulation (EU, Euratom) 2018/1046 ~~the FRFinancial Regulation~~];**

(ca) as part of the annual work programme adopt decisions to ~~dedicate~~ allocate funds from the Union budget to joint actions between the Union and Member States;

(cb) as part of the annual work programme and in accordance with the decisions referred to in point (ca) ~~of this paragraph~~, and ~~without prejudice to~~ in compliance with the regulations establishing Horizon Europe and the Digital Europe Programme, adopt decisions relating to the description of the joint actions referred to in point (ca) and lay down conditions for their implementation.

(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 **and** the number of contract staff and seconded national experts expressed in full-time equivalents;

(h) adopt rules **for the prevention and management of conflicts of interest in respect of its members;** ~~regarding conflicts of interest;~~

(i) **when appropriate, provide ~~seek~~ advice to the Cybersecurity Competence Community with regard to the** establish**ment of** working groups by **the Cybersecurity Competence Community and assist in the coordination of such groups;**

~~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[20];

(l) set up a monitoring mechanism to ensure that the implementation of the respective funds managed by the Centre is done in accordance with the Agenda, the missions and the multiannual work programme and with the rules of programmes where funding originates from ~~of the Centre~~;

[20] 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).

(la) ~~to~~ ensure a regular dialogue and establish an effective cooperation mechanism with the Cybersecurity Competence Community;

~~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 **voluntary** financial **and in-kind** contribution from **contributing** Member States **in accordance with Horizon Europe and Digital Europe Regulations;**

(sa) register entities nominated by Member States as their National Coordination Centres;

(sb) in deciding on the annual work programme and the multiannual work programme, ensure coherence and synergies with those parts of the Digital Europe programme and the Horizon Europe programme 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;~~

(u) discuss and adopt the annual report on the implementation of the Centre's strategic goals and priorities with a recommendation, if necessary, for their better realisation

4. Regarding the tasks laid down in points (a), (aa) and (aaa) of paragraph 3, the Executive Director and the Governing Board shall take into account any relevant strategic advice and input provided by ENISA, ~~within deadlines~~ according to the rules of procedure set by the Governing Board.

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~~ **three** 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 **C**hair**person**, 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.

3a. The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers, including additional representatives of the Commission, for ensuring coordination and synergies between different Union activities involving cybersecurity.

4. **Representatives of the Cybersecurity Competence Community** ~~**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

-1. A vote shall be held if the members of the Governing Board failed to achieve consensus.

-2. **The Governing Board shall take its decisions by a majority of at least 75% of all its members, ~~with voting rights,~~ the representatives of the Commission constituting a single member for this purpose. An absent member of the Governing Board may delegate his or her vote to his or her alternate or, in the absence of his or her alternate, to another member. Any member of the Governing Board may represent not more than one other member. [For financial decisions related to the usage of Union funds in Article 13(3) except point (cb), the Union should hold 50% of the voting rights].**

-2a. ~~**For decisions related to the task laid down in Article 13(3) (cb), contributing Member States and the Commission shall hold votes proportional to their relevant contribution on that specific action in line with the methodology adopted pursuant Article 13(3) s)**~~

Decisions of the Governing Board on the joint actions and their management laid down in points (ca) and (cb) of Article 13(3) shall be taken as follows:

(a) decisions to allocate funds from the Union budget to joint actions as referred to in point (ca) of Article 13(3) and the inclusion of such joint action in the annual work programme shall be taken in accordance with the rules set up in paragraph -2 of this Article;

(b) decisions relating to the description of the joint actions and laying down conditions for their implementation referred in point (cb) of Article 13(3) shall be taken by participating Members States and the Commission and the voting rights shall be proportional to their relevant contribution to that joint action in accordance with the methodology adopted pursuant to point (s) of Article 13(3).

1. **For ~~any other~~ decisions other than those referred to in paragraph -2a, ~~every~~ each Member State~~s~~ and t**he Union ~~shall hold 50 % of the voting rights~~ **shall have one vote.** The **vote ~~ing rights~~** of the Union shall be **cast jointly by the two representatives of the Commission.**

~~**2.** Every participating Member State shall hold one vote.~~

~~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 c 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).~~

~~**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.

SECTION II

EXECUTIVE DIRECTOR

Article 16

Appointment, dismissal ~~or~~ and extension of the term of office of the Executive Director

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 **its** meetings and supply all information necessary for the performance of **its** duties;

   (c) after consultation with the Governing Board and the Commission, **and taking into account the input of the Network and the Cybersecurity Competence Community, and in accordance with the Agenda,** prepare and submit for adoption to the Governing Board the draft multiannual **work programme** and the **draft** annual work **programme** 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 **annual** work **programme** 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 **referred to in point (g) of Article 13(3),** 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 **annual work programme and the multiannual** work **programme** and report to the Governing Board thereon;

(f) prepare the draft annual activity report on the ~~Competence~~ Centre, including the information on corresponding expenditure **and the realisation of the strategic goals and priorities set out in the Agenda and the multiannual work programme of the Centre; ~~and~~ if necessary, that report shall be accompanied by proposals for the further improvement of the realisation and/or the reformulation of the strategic goals and priorities;**

(g) ensure the implementation of effective monitoring and evaluation procedures relating to the performance of the ~~Competence~~ Centre;

(h) prepare an action plan **that follows up** ~~following up~~ on the conclusions of the retrospective evaluations and report**sing** on progress every two years to the Commission;

(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 decisions referred to in points (c), (g), (o), (p), (q) and (r) of Article 13(3) ~~delegation by the Governing Board~~;**

(k) approve and manage the launch of calls for proposals, in accordance with the **annual** work **programme,** and administer the grant agreements and decisions;

(l) approve the list of actions selected for funding on the basis of **~~the~~ a** ranking list established by a panel of independent experts;

(m) approve and manage the launch of calls for tenders, in accordance with the **annual** work **programme,** 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 **that** follow**s** up **on the** conclusions of internal or external audit reports, as well as investigations by the European Anti-Fraud Office (OLAF) **established with Commission Decision 1999/352/EC, ECSC, Euratom**[21] **("OLAF")** and **report** 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 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.

[21] Commission Decision 1999/352/EC, ECSC, Euratom of 28 April 1999 establishing the European Anti-fraud Office (OLAF) (OJ L 136, 31.5.1999, p. 20).

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 **20** 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, and between large providers and small and medium entreprises 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 **Union** Network and Cyber Security Agency **for Cybersecurity** 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 **election** of the representatives **chair,** that shall represent the Advisory Board where relevant and the duration of their nomination.

5. The secretariat of the Industrial and Scientific Advisory Board is provided by the Centre, based on Centre's rules of procedure.

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. participate in public consultations organised by the Centre and other stakeholders, at events open to all public and private stakeholders having an interest in the field of cybersecurity, on behalf of the Centre and collect input from the Community for the strategic advice referred to in paragraph 1;

~~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 and Member States´ financial contribution

-1. The Centre shall be funded by the Union.

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 **p**rogramme, including up to **[**EUR 23 746 000**]** for administrative costs;

b) an amount from the Horizon Europe programme, including for administrative costs, **for joint actions, which shall be equal to the amount contributed ~~voluntary~~ by Member States pursuant to paragraph 5 of this Article ~~21(5) and~~ but not exceed [the amount determined in the strategic planning process of the Horizon Europe programme] ~~to be determined by taking into account the strategic planning process~~** to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation] **and the multiannual work programme and the annual work programmes**.

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 the first subparagraph** of Article 62**(1)** of Regulation (EU, Euratom) ~~**XXX[23] [the Financial Regulation]**~~ **2018/1046.**

~~5~~4. ~~The Union financial contribution shall not cover the tasks referred to in Article 4(8)(b)~~**Contributions from Union programmes other than those referred to in paragraphs 1 and 2 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).**

~~65. Member States can make voluntary financial contributions for joint action with the Union, paid in instalments and in-kind contributions consisting of costs incurred by National Coordination Centres and beneficiaries in implementing actions that are not reimbursed by the Centre.~~

Voluntary contributions made by one or more Member States for joint actions with the Union in accordance with the Horizon Europe programme and/or the Digital Europe programme, may take the form of financial and/or in-kind contributions.

Financial contributions by Member States may take the form of support by Member States provided to participants in joint actions.

In-kind contributions by Member States shall consist of eligible costs incurred by National Coordination Centres and other public entities when participating in projects funded through this Regulation less any Union contribution to those costs. In the case of projects funded through Horizon Europe, eligible costs shall be calculated in line with Article 32 of the Regulation establishing Horizon Europe. In the case of projects funded through Digital Europe, eligible costs shall be calculated in line with ~~t~~ Regulation (EU, Euratom) 2018/1046.

The envisaged amount of total Member State voluntary contributions, including financial contributions for administrative costs, to joint actions under the Horizon Europe programme shall be determined in order to be taken into account in the strategic planning process of the Horizon Europe programme to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation], with input from the Governing Board.

For actions under the Digital Europe programme, notwithstanding Article 15 of the [Regulation establishing the Digital Europe Programme], the Member States may make a contribution to the costs of the Centre that are co-financed from the Digital Europe programme that is lower than the amounts specified in [Article 21(1)(a~~b~~) – reference to be checked] of this Regulation.

~~*Article 22*~~

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

~~1. The participating Member States shall make a total contribution to the operational and administrative costs of the Competence Centre of at least the same amounts as those in Article 21(1) of this Regulation.~~

7.~~1a.~~ Member States' co-funding of actions supported by Union programmes other than Horizon Europe and Digital Europe ~~could~~ shall be considered as contributions when ~~as~~ those actions are in the remit of the Centre's missions and tasks.

8.~~2.~~ For the purpose of assessing the contributions referred to in paragraph 1 **of this Article** 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 **that** Member State, and the applicable **i**nternational **a**ccounting **s**tandards and **i**nternational **f**inancial **r**eporting **s**tandards. The costs shall be certified by an independent external 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.

9.~~3~~. Should any ~~participating~~ Member State be in default of its commitments concerning its financial **and/or in-kind** contribution **pursuant to joint actions**, 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 **that Member State meets** its obligations ~~**have been met**~~. The defaulting Member State's voting rights **concerning joint actions** shall be suspended until the default of its commitments is remedied.

10.4. The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to ~~the Competence Centre~~ **joint actions** if the ~~participating~~ **contributing** Member States do not contribute, contribute only partially or contribute late with regard to the contributions referred to in **point (b) of** paragraph 1.

11.5. The ~~participating~~ **contributing** Member States shall report by 31 January **of** each year to the Governing Board on the value of the contributions referred to in paragraph~~s 1~~ **5 for joint action with the Union** 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 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~~ on an annual basis ~~between~~ **from** the Union. ~~and the participating Member State~~ **Additional contributions shall be made by contributing Member State**s **in proportion to their voluntary contributions to joint action**s **~~between the Union and Member States~~.** 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 financial and/or in-kind** contributions from the ~~participating~~ **contributing** Member States **in case of joint action**s **~~between the Union and Member States in the form of~~:**

~~i. Financial contributions; and~~

~~ii. where relevant, in-kind contributions by the participating 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. The Governing Board shall specify an operational methodology for calculating the in-kind contributions of Member States;~~

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~~ **contributing** Member States' **voluntary** financial contributions to the administrative **costs in case of joint actions ~~between the Union and Member States;~~**

(c) ~~participating~~ **contributing** Member States' **voluntary** financial contributions to the operational costs **in case of joint actions ~~between the Union and Member States~~;**

(d) any revenue generated by ~~the Competence~~ Centre;

(e) any other financial contributions, resources and revenues.

5. Any interest yielded by the contributions paid to the ~~Competence~~ Centre by the ~~participating~~ **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. **Without prejudice to the applicable rules of the relevant funding programme, ownership of assets generated or acquired in joint actions shall be decided in accordance with Article 15 (-2a).**

8. Except when the ~~Competence~~ Centre is wound up, any excess revenue over expenditure shall **remain in the ownership of the Centre and** 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 **as referred to in point (g) of Article 13(3)**. 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**, also through redeployment of staff or posts**.

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 **of** each year, send the statement of estimates referred to in paragraph 2, which shall be part of the draft single programming document **referred to in Article 32(1) of Commission Delegated Regulation (EU) 2019/715**[22]**,** to the Commission.

4. On the basis of th**e** statement of estimates **referred to in paragraph 2 of this Article,** the Commission shall enter in the draft budget of the Union the estimates it deems necessary for the establishment plan **referred to in point (g) of Article 13(3)** 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 Article**s** 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 **referred to in point (g) of Article 13(3).**

7. Together with the **annual work programme and multi annual** work **programme**, the Governing Board shall adopt the Centre's budget. It shall become final following **the** definitive adoption of the general budget of the Union. Where appropriate, the Governing Board shall adjust the ~~Competence~~ Centre's budget and **the annual** work **programme** in accordance with the general budget of the Union.

---

[22] **Commission Delegated Regulation (EU) 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (OJ L 122, 15.5.2019, p. 1).**

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 **(EU, Euratom) 2018/1046** and of **~~its~~ the** financial rules **of the Centre ~~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 **annual** work **programme** for that year **and the fulfilment of its strategic goals and priorities**. 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 technology related 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 **missions~~s~~ set out in Article 3 and the** objectives set out in Article 4 and proposals for further necessary work to achieve **that mission and** th**o**se objectives;

(e) coherence of the implementation tasks in accordance with the Agenda and the multiannual work programme ~~of the Centre.~~

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 **(EU, Euratom) 2018/1046 ~~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[23] and Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council[24] 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.

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.

---

[23] Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities (OJ L 292, 15.11.1996, p. 2).

[24] 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).

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[25] ('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.

[25] 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).

4. Where exceptional circumstances so require, the Governing Board may, **through a** 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 member **of staff** 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.

6. The staff resources shall be determined in the **~~staff~~** establishment plan **referred to in point (g) of Article 13(3)~~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 human resources required in the Centre shall be met primarily by redeployment of staff or posts from Union institutions, bodies, offices and agencies**. The staff of the ~~Competence~~ Centre ~~shall~~ **may** 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. Article 12(~~7~~**5**) 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 **annual** work **programme** , the grant of non-exclusive licenses may be limited to third parties established or deemed to be established in Members 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~~ **for** objec**tion** 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 **annual** work **programme**, granting of access to results and background may be limited only to a legal entity established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States.

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~~**42**.

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 classified information in whole or a part 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.~~ 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 Commission Decisions (EU, Euratom) 2015/443**[26] **and 2015/444**[27] **~~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 and 2015/444~~.**

[26] Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).

[27] 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).

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 and 2015/444.~~ 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.

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.

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.

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 **a** timely manner and proportionate reporting requirements shall be imposed on recipients of Union funds and Member States. The ~~**outcomes**~~ **conclusions** of th**at** evaluation shall be made public.

2. Once there is sufficient information available about the implementation of this Regulation, but no later than **two** ~~**three and a half**~~ years **after the date referred to in Article 45 paragraph 4 of this Regulation** ~~**after the start of the implementation of this Regulation.**~~ the Commission shall carry out an interim evaluation of the ~~Competence~~ Centre **following the input of the Governing Board**. 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 **2023**. ~~**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 **in particular**:

(a) an assessment of the working capacity of the Centre regarding objectives, mandate and tasks and the cooperation and coordination with other relevant actors, particularly National Coordination Centres, the Cybersecurity Competence Community and ENISA;

(b) an assessment of the results achieved by the ~~Competence~~ Centre**,** having regard to its **mission,** objectives, mandate and tasks**, and in particular the efficiency of the Centre in coordinating Union funds and pooling expertise;**

(c) an assessment of the coherence of implementation tasks in accordance with the Agenda and the multiannual work programme ~~of the Centre~~;

(d) an assessment of the coordination and cooperation of the Centre with the Program Committee of the Horizon Europe programme and the Digital Europe programme, especially with a view to increasing coherence and synergy with the strategic planning of the Centre, the Horizon Europe programme and the Digital Europe programme;

(e)an assessment on joint actions;

3a. After the submission of the report referred to in paragraph 2 of this Article, the Commission shall carry out a final evaluation of the Centre following the input of the Governing Board. That final evaluation shall refer to or update, as necessary, the assessments referred to in paragraph 3 of this Article and shall be carried out before the period specified in article 46(1), in order to determine well in advance whether the duration of the Centre should be extended beyond that period. That final evaluation shall include legal and administrative considerations whether the mandate of the Centre could be transferred to a different Union body to create synergies and reduce fragmentation.

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~~ make a legislative proposal to extend ~~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(5~~**~~4~~**~~)] 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~~ arrangements**.

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 **(EU, Euratom) 2018/1046**~~**XXX [new Financial Regulation]**~~**, including provisions on any declarations of interest. Regarding conflict of interest, the National Coordination Centres** ~~**will**~~ **shall be subject to national** ~~**legislation for conflict of interest**~~ **law.**

Article 43

Protection of Personal Data

1. The processing of personal data by the ~~Competence~~ Centre shall be subject to Regulation (EU) ~~XXX~~**1725**/2018 ~~of the European Parliament and of the Council~~.

2. The Governing Board shall adopt implementing measures referred to in Article ~~**xx**~~**45**(3) of Regulation (EU) ~~xxx~~**1725**/2018. The Governing Board may adopt additional measures necessary for the application of Regulation (EU) No **1725**/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 **of this Article,** 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~~ **That interim Executive Director shall** exercise the duties assigned to the Executive Director and ~~who~~ may be assisted by a limited number of **members of staff of the** Commission ~~officials~~. The Commission may assign a limited number of its **members of staff** ~~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 **referred to in point (g) of Article 13(3).**

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~~ shall** 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 **the** period **referred to in paragraph 1 of this Article**, **unless ~~decided otherwise through a review of this Regulation~~ the mandate of the Centre is extended in accordance with the second subparagraph of Article 38(3),** 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 State**s 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	*For the Council*
The President	*The President*