European Parliament

Committee on Industry, Research and Energy
The Chair

D 300144 14.01.2021

HE Ambassador Pedro LOURTIE
Deputy Permanent Representative
Chair of COREPER I
Council of the European Union
Rue de la Loi 175
1048 Brussels

Ref.: D (2021) 0171
HB/mk

Subject: **Council's position in view of the adoption of a Regulation of the European Parliament and the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (COD 2018/0328) - Early second reading agreement**

Dear Mr Lourtie,

I understand that at its meeting of 18 December 2020 COREPER I decided to accept the result of the last informal trilogue held on 11 December 2020 regarding the above mentioned Regulation.

I would like to inform you that should the Council transmit formally to the Parliament its position in the form as it stands in the annex, I will, in my capacity as Chair of the Committee on Industry, Research and Energy, recommend to the Plenary that the Council's position be accepted without amendment, subject to legal-linguistic verification, at Parliament's second reading.

At the same time, I would like to thank the German Presidency for the efforts made and the work accomplished to achieve an early second reading agreement on this file.

Yours sincerely,

Cristian-Silviu BUŞOI

Annex: text agreed

Council of the European Union

Brussels, 16 December 2020
(OR. en)

13856/20

Interinstitutional File:
2018/0328(COD)

LIMITE

CYBER 274
TELECOM 265
COPEN 385
CODEC 1351
COPS 482
COSI 252
CSC 365
CSCI 95
IND 271
RECH 523
ESPACE 83

NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee
No. prev. doc.:	8625/20, 9745/20, 10781/20, 11234/20, 12293, 12952, 13373
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 - Analysis of the final compromise text with a view to agreement

I. INTRODUCTION

1. 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 Centres, with Articles 173(3) and 188 TFEU as the legal basis.

2. This proposal provides for the creation of a Competence 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.

3. The Competence Centre would be:

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

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

      b. enable the Member States to take decisions related to their financial contribution tojoint actions and

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

   (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 Competence Centre would also be able to facilitate the shared acquisition of capacities on behalf of Member States.

4. 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).

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

6. On 13 March 2019, COREPER gave a mandate to start the negotiations with the European Parliament. Five Trilogues have taken place since then: 13 and 20 March 2019 under Romanian Presidency, 25 June 2020 under Croatian Presidency as well as 29 October and 11 December 2020 under German Presidency.

7. COREPER agreed to a new mandate at its meeting on 3 June 2020. Two pending Council positions, the seat of the Centre and the voting rights of the Centre's Governing Board, were solved within the Council during the German Presidency. On 22 July 2020, another renewed mandate was adopted at the COREPER meeting, clarifying the scope of the Commission's veto right.

8. In the margins of COREPER on 28 October 2020, the representatives of the governments of the Member States agreed on a procedure for selecting the seat of the Competence Centre. The decision on the seat was taken in the margins of COREPER on 9 December 2020.

9. At the trilogue on 11 December 2020, an agreement was reached between the European Parliament and the Council in line with the mandate which was renewed by COREPER on 9 December 2020.

10. In the light of the above, the Permanent Representatives Committee is invited to:

– approve the final compromise text set out in annex as agreed in the trilogue[1];

– mandate the Presidency to inform the European Parliament accordingly.

---

[1] New text is indicated in **bold** whereas deleted text is indicated in ~~strikethrough~~ or by **[…]**.

ANNEX

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],

Acting in accordance with the ordinary legislative procedure,

[2] OJ C , p. .

Whereas:

(1) ~~Our~~***The majority of the population of the Union is connected to the internet and our*** daily lives and economies ***are becoming*** ~~become~~ increasingly dependent on digital technologies, ***with*** citizens ~~become~~***and companies becoming*** more and more exposed to serious cyber incidents. ~~Future security depends, among others~~***Every year many European companies experience at least one cyber incident. This underlines the necessity for resilience***, ~~on~~ enhancing technological and industrial ability***, the use of high cybersecurity standards and holistic cybersecurity solutions, involving people, products, processes and technology in*** ~~to protect~~ the Union***, as well as for the Union's leadership in the matter, and for digital autonomy. Cybersecurity can also be improved by raising the awareness for cybersecurity threats, by developing competences,*** ~~against cyber threats, as both civilian infrastructure and military~~ capacities***, capabilities throughout the Union, thoroughly taking into account the societal and ethical implications and concerns*** ~~rely on secure digital systems~~.

(2) The Union has steadily increased its activities to address growing cybersecurity challenges following the ***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[3]***"). 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 ~~Joint Communication to~~ ***Directive (EU) 2016/1148 of*** the European Parliament and ***of*** the Council~~:: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013) 1 final~~ ***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)***.

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).~~

(3) In September 2017, the Commission and the High Representative ~~of the Union for Foreign Affairs and Security Policy presented a Joint Communication[5] on~~***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***, safer*** and law-governed internet~~.~~"***, and declared to "make more use of open source solutions and/or open standards when (re)building Information and Communication Technology (ICT) systems and solutions (among else, to avoid vendor lock-ins), including those developed and/or promoted by EU programmes for interoperability and standardisation, such as ISA".***

(4a) The European Cybersecurity Industrial, Technology and Research Competence Centre (the 'Competence Centre') should help to increase the security of network and information systems, including the internet and other infrastructures which are critical for the functioning of society such as transport, health, energy, digital infrastructure, water, financial market and banking systems.

(5) Substantial disruption of network and information systems can affect individual Member States and the Union as a whole. ~~The security of~~ ***A high level of security of*** network and information systems ***throughout the Union*** is therefore essential ~~for the smooth functioning of the internal market~~ ***for society and economy alike***. 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*** ~~cybersecurity~~ technological capacities to secure ~~its Digital Single Market, and~~ ***network and information systems of European citizens and companies, and*** in particular to protect critical ~~networks~~ ***network*** and information systems***,*** and to provide key cybersecurity services.

---

[5] ~~Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017) 450 final.~~

(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 ***and effective protection of networks and systems*** 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***, skills*** and industrial capacities at Union and national levels. ***Whereas ICT sector faces important challenges, such as fulfilling its demand for skilled workers, it can benefit from representing the diversity of society at large, and from achieving a balanced representation of genders, ethnic diversity, and non-discrimination against disabled persons, as well as from facilitating the access to knowledge and training for future cybersecurity experts, including their education in non-formal contexts, for example in Free and Open Source Software projects, civic tech projects, start-ups and micro-enterprises.***

(6a) Small and medium-sized enterprises (SMEs) are crucial actors in the Union's cybersecurity sector, which can provide cutting-edge solutions due to their agility. SMEs that are not specialised in cybersecurity are, however, also prone to be more vulnerable to cyber incidents due to high investment and knowledge requirements to establish effective cybersecurity solutions. It is therefore necessary that the Competence Centre and the Cybersecurity Competence Network (the 'Network') provide support for SMEs by facilitating their access to knowledge and through tailored access to the results of research and development, in order to allow them to secure themselves sufficiently and to allow those who are active in cybersecurity to be competitive and contribute to the Union's leadership in the field.

(6b) Expertise exists beyond industrial and research contexts. Non-commercial and pre-commercial projects, referred to as "civic tech" projects, make use of open standards, Open Data, and Free and Open Source Software, in the interest of society and the public good.

(6c) The cybersecurity field is a diverse one. Hence, relevant stakeholders can be from public entities, including Member States and the European Union, as well as from industry and other entities, as well as civil society, e.g. trade unions, consumer associations, the Free and Open Source Software community, and the academic and research community.

(7) The Council Conclusions adopted in November 2017 called on the Commission to provide rapidly an impact assessment on the possible options to create a Network of Cybersecurity Competence Centres***, together with a*** ~~with the~~ European ***Cybersecurity*** Research and Competence Centre and propose by mid-2018 the relevant legal instrument.

(7a) 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.

(7b) The option of creating a network of National Coordination Centres, together with a European Cybersecurity Industrial, Technology and Research Competence Centre, with a 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 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 Cybersecurity Competence~~***a Network of National Coordination Centre ("the*** Network***"). The Competence Centre***~~. It~~ should deliver cybersecurity-related financial support from ***Horizon Europe - the Framework Programme for Research and Innovation established by Regulation 2020/… of the European Parliament and of the Council***[6] ***(‘***the Horizon Europe ***programme’) and the*** ~~and~~ Digital Europe ~~programmes, and should be open to~~***programme established by Regulation 2020/… of*** the European ~~Regional Development Fund and~~ ***Parliament and of the Council***[7] ***(‘the Digital Europe programme) and should be open to*** other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to ***Union initiatives in the field of*** cybersecurity research ***and development***, innovation, technology and industrial development and avoiding ***unnecessary*** duplication.

(8aa) It is important to ensure respect for fundamental rights and ethical conduct in Cybersecurity research projects supported by the Centre.

(8ab) The Competence Centre should not carry out operational cybersecurity tasks, such as tasks associated with Computer Security Incident Response Teams (CSIRTs), including monitoring and handling of Cybersecurity incidents. However, the Competence Centre could facilitate the development of ICT infrastructures at the service of industries, in particular SMEs, research communities, civil society and the public sector, in line with the mission and objectives laid down in this Regulation. Where CSIRTs and other actors seek to promote the reporting and disclosing of vulnerabilities, the Competence Centre and members of the Community within the limits of their respective tasks, while avoiding any duplication with ENISA, may support these actors, at the request of these actors.

---

[6] ***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)].***

[7] ***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)].***

(8ac) The Competence Centre, the Cybersecurity Community and the Network should benefit from the 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[8], and the lessons learned from four pilot projects[9] launched in early 2019 under Horizon 2020 and from the pilot project and the preparatory action on Free and Open Source Software Audits (EU FOSSA), for the management of the Cybersecurity Competence Community, and the representation of the Cybersecurity Competence Community in the Centre.

(8b) In view of the extent of the cybersecurity challenge and in view of the investments made in cybersecurity capacities and capabilities in other parts of the world, the Union and its Member States should be encouraged to step up their financial support to research, development and deployment in this area. In order to realise economies of scale and achieve a comparable level of protection across the Union, the Member States should put their efforts into a European framework by actively contributing to the work of the Competence Centre and the Network.

---

8 *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).*

9 *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".*

(8c) The Competence Centre and the Cybersecurity Competence Community should, in order to foster the Union's competitiveness and high cybersecurity standards internationally, seek the exchange on developments in cybersecurity, including on products and processes, standards and technical standards with the international community, where relevant to its mission, objectives and tasks.

Relevant technical standards could include for the purpose of this Regulation, the creation of reference implementations, including those published under open standard licences.

(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~~***The seat*** of the Competence Centre ~~should hold voting rights~~***is in Bucharest***.

(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 cybersecurity, 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 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 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, it is necessary that the Centre is considered as a partnership for the purpose of budget implementation, including the programming phase.

(10) ***As a result of Union contribution, access to the results of the Centre's activities and project results will be as open as possible and as closed as necessary, and re-use is possible where appropriate*** ~~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 ***Network, which should be*** ~~Cybersecurity Competence Network ("the Network"),~~ made up of National Coordination Centres***, one from*** ~~in~~ each Member State. National Coordination Centres ***which have been recognised by the Commission as fulfilling the capacity to manage funds so as to achieve the mission and objectives laid down in this Regulation,*** 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 ~~selected by Member States. In addition to the necessary~~***public sector entities, or entities with a majority of public participation, performing public*** administrative ~~capacity, Centres~~***functions under national law, including by means of delegation, and they*** should ~~either possess or have direct access to cybersecurity technological expertise in cybersecurity, notably in domains such as cryptography, ICT security services, intrusion detection, system security, network security, software and application security~~***be selected by Member States. The functions of a National Coordination Centre in a given Member State can be carried out by an entity that carries out other functions arising under Union law, such as those of a national competent authority, a single point of contact in the meaning of Directive (EU) 2016/1148, any other EU Regulation, or a digital innovation hub in the meaning of the Digital Europe programme. Other*** ~~or human and societal aspects of security and privacy. They should also have the capacity to effectively engage and coordinate with the industry, the~~ public sector~~, including authorities designated pursuant to the Directive (EU) 2016/1148 of the European Parliament and of the Council[10], and the research community~~ ***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) The National Coordination Centres should have the necessary administrative capacity and should possess or have access to cybersecurity industrial, technological and research expertise and be in a position to effectively engage and coordinate with the industry, the public sector, and the research community.

(12b) Education in the Member States of the European Union should reflect the importance of adequate cybersecurity awareness and skills. To this end and taking into account the role of ENISA and without prejudice to national competences of Member States for education, the National Coordination Centres alongside relevant public authorities and stakeholders, should contribute to promoting and disseminating cybersecurity educational programmes.

---

10 ~~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).~~

(13) ~~Where financial support is provided to National Coordination Centres~~***The National Coordination Centres may receive grants from the Centre*** in order to ***provide financial*** support ***to*** third parties ~~at~~***in the form of grants. The direct cost incurred by*** the National ~~level, this shall be passed on to relevant stakeholders through cascading grant agreements~~***Coordination Centres for the provision and administration of financial support to third parties shall be eligible for funding***.

(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~~***The Centre, the Network and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity products and solutions.*** At the same time ~~new challenges for~~***the Centre and the Network should promote the*** 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~~***capability of the demand side industry, in particular by supporting developers and operators in sectors such as transport, energy, health, finance, government, telecom, manufacturing, and space to help them solve their cybersecurity challenges, for example in order to achieve security-by-design***. ~~The Competence Centre, the Network and the~~ ***They should also support the standardisation and deployment of*** cybersecurity ~~Competence Community should help advance and disseminate the latest~~***products and solutions while promoting, where possible, the implementation of the European*** cybersecurity ~~solutions. At the same time the Competence Centre and the Network should be at the service of developers and operators in critical sectors such as transport, energy, health, financial, government, telecom, manufacturing, defence, and space to help them solve their~~ ***certification framework as defined by Regulation (EU) 2019/881 of the European Parliament and of the Council***[11]***.***

---

11 ***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 ~~challenges~~***Act) (OJ 151, 7.6.2019, p. 15)***.

(14a) Due to the fast changing nature of cyber threats and cybersecurity, the Union needs to be able to adapt fast and continuously to new developments in the field. Hence, the Competence Centre, the Network and the Cybersecurity Competence Community should be flexible enough to ensure the required reactivity. They should facilitate projects that help entities to be able to constantly build capability to enhance their and the Union's resilience.

(15) The Competence Centre should ~~have several key functions. First, the Competence~~ ***support the Cybersecurity Competence Community. The*** Centre should ~~facilitate and help coordinate the work~~***implement cybersecurity relevant parts*** of the ~~European Cybersecurity Competence Network and nurture the Cybersecurity Competence Community.~~***Digital Europe programme and the Horizon Europe programme in accordance with*** the Centre***'s multiannual work programme ("multiannual work programme") and the annual work programme*** ~~should drive the cybersecurity technological agenda and facilitate access to the expertise gathered in the Network~~ and the ~~Cybersecurity Competence Community. Secondly, it should implement relevant parts of Digital Europe and Horizon Europe programmes by allocating grants~~***strategic planning process of the Horizon Europe programme by allocating grants and other forms of funding***, ~~typically~~ ***primarily*** following a competitive call for proposals~~. Thirdly~~, ***facilitate transfer of expertise in the Network and the Cybersecurity Competence Community and support*** ~~the Competence Centre should facilitate~~ joint investment by the Union, Member States and/or industry. ***It should pay special attention to the enabling of SMEs in the area of cybersecurity as well as to actions that help overcome the skills gap.***

(15a) Technical assistance for project preparation must be done in a fully objective and transparent way to ensure that all potential beneficiaries receive the same information and must avoid conflicts of interest.

(16) The Competence Centre should stimulate and support the ***long-term strategic*** cooperation and coordination of the activities of the Cybersecurity Competence Community, which would involve a large, open, ***interdisciplinary*** and diverse group of ***European*** actors involved in cybersecurity technology. That Community should include in particular research entities, ~~supply-side~~ industries~~, demand side industries,~~ and the public sector. The Cybersecurity Competence Community***, in particular through the Strategic Advisory Group,*** should provide input to the activities***, the multiannual work programme and the annual work programme*** ~~and work plan of the Competence Centre~~ and it should also benefit from the community-building activities of the Competence Centre and the Network, but otherwise should not be privileged with regard to calls for proposals or calls for tender. ***The Community should be made up of collective bodies/organisations. At the same time, in order to benefit from all the cybersecurity expertise in Europe the Competence Centre and its bodies could also resort to the expertise of individual and natural persons as ad-hoc experts.***

(16a) The Competence Centre should cooperate and ensure synergies with the European Network and Information Security Agency (ENISA). Therefore, ENISA should provide relevant input to the Competence Centre in its task of defining funding priorities.

(17) In order to respond to the needs of both demand and supply side ~~industries~~***of cybersecurity***, the Competence Centre's task to provide cybersecurity knowledge and technical assistance to industries should refer to both ICT products***, processes*** and services and all other ~~industrial and~~ technological products and ~~solutions~~***processes*** in which cybersecurity is to be embedded. ***Upon request, the public sector can also benefit from support from the Centre.***

(17a) In order to achieve a sustainable cybersecurity environment, it is important that "security by design" is used as a principle in the process of developing, maintaining, operating, and updating infrastructures, products and services, in particular by supporting state-of-the-art secure development methods, adequate security testing, security audits, and making available updates remedying known vulnerabilities or threats without delay, and where possible enabling third parties to create and provide updates beyond the respective end-of-service of products. Security should be ensured by design throughout the lifetime of ICT products, services or process and by the development processes that constantly evolve to reduce the risk of harm from malicious exploitation.

(18) Whereas the Competence Centre and the Network should strive to ~~achieve~~***enhance*** synergies ***and coordination*** between the cybersecurity civilian and defence spheres, projects ***under this Regulation*** financed by the Horizon Europe Programme ~~will~~***should*** be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe ~~shall have a~~***are to have an exclusive*** focus on civil applications.

(18a) Without prejudice to the civilian nature of this Regulation, Member States' activities under this Regulation may reflect specificities of Member States in cases when cybersecurity policy is pursued by civil-military or military authorities, and strive for complementarity and avoid overlap with 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 ***and those undertakings receiving funding, in line with the respective programme regulations***.

(20a) The implementation of deployment projects, in particular those relating to infrastructures and capabilities deployed at European level or in joint procurement, could be divided into different phases of implementation, such as separate tenders for the architecture of hard- and software, their production and their operation and maintenance, whereas companies could only participate in one of the phases each and where appropriate could require that the beneficiaries in one or several of those phases meet certain conditions in terms of European ownership or control.

(21) In view of ~~their respective~~***its*** expertise in cybersecurity~~, the Joint Research Centre of the Commission~~ ***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, and in view of its collection of input through its tasks,*** the European ~~Network and Information Security Agency (~~***Union Agency for Cybersecurity as established by Regulation (EU) 2019/881 ("***ENISA***")*** should play an active part in the ~~Cybersecurity Competence Community~~***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 ~~Industrial and Scientific Advisory~~***multi-annual 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 ~~the present initiative~~***this Regulation***.

(23) The ~~Union contribution to the Competence Centre should finance half~~***costs arising from the establishment, administrative and coordination activities*** of the ***Competence Centre should be financed by the Union and, in proportion to their voluntary contributions to Joint Actions, by Member States*** ~~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 ~~it~~***the Centre*** carries out its tasks in accordance with this Regulation. The Governing Board should ~~be entrusted with the powers necessary to establish the budget, verify its execution,~~ adopt the ~~appropriate financial rules, establish transparent working procedures for decision making by the Competence Centre, adopt the Competence Centre's work plan and multiannual strategic plan reflecting the priorities in achieving the objectives and tasks of the Competence Centre, adopt its rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof~~***Agenda***.

(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 Centre, reflecting the Agenda adopt the annual work programme and the multiannual work programme , 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 alignment 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 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 Representatives on the Governing Board in order to ensure continuity in its work.

(25a) In view of the Centre's specific status and responsibility for the implementation of Union funds, in particular those from Horizon Europe and Digital Europe programmes, in the Governing Board, the Commission should have 26% of the total votes on decisions involving Union funds, with the aim of maximising the EU value added of those decisions, while ensuring their legality and alignment with Union priorities.

(26) The smooth functioning of the Competence Centre requires that its Executive Director be appointed ***in a transparent manner on the*** ~~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 ***Cybersecurity*** Competence Centre should have ~~an Industrial and Scientific~~***a Strategic*** Advisory ~~Board~~***Group*** as an advisory body ~~to ensure~~***that should provide advice following*** regular dialogue ~~with the~~ ***between the Centre and the Community, formed by the representatives of the*** private sector, consumers' organisations***, academia*** and other relevant stakeholders. The ~~Industrial and Scientific~~***Strategic*** Advisory ~~Board~~***Group*** should focus on issues relevant to stakeholders and bring them to the attention of the Competence Centre's Governing Board ***and the Executive Director***. The composition of the ~~Industrial and Scientific~~***Strategic*** Advisory ~~Board~~***Group*** and the tasks assigned to it, such as ~~being consulted~~***providing advice*** regarding the ***Agenda, annual work programme and the multi-annual work programme*** ~~work plan,~~ should ***include a balanced representation of the different stakeholders, with particular attention paid to SMEs, in order to*** ensure ~~sufficient~~***appropriate*** representation of stakeholders in the work of the Competence Centre.

(28) ~~The Competence Centre should benefit from the particular expertise and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity during the duration of Horizon2020, through its Industrial and Scientific Advisory Board.~~

The Competence Centre will be a Union body, to which Commission Delegated Regulation (EU) 2019/7151[12] shall apply.

(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 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 would be accounted for as in-kind contributions.

---

12 ***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):***

(29) ***In line with Article 42 of the Framework Financial Regulation for Bodies established under Article 70 of the Financial Regulation,*** the Competence Centre should have in place rules regarding the prevention***, identification and resolution and*** ~~and the~~ management of ~~conflict~~***conflicts*** of interest ***in respect of its members, bodies and staff, the Governing Board, as well as the Strategic Advisory Group, and the Community. Member States should ensure the prevention, identification, and resolution of conflicts of interest in respect of the National Coordination Centres, according to the national legislations***. 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[13]. Processing of personal data by the Competence Centre will be subject to Regulation (EU) ~~No XXX/2018~~***No 1725/2018*** of the European Parliament and of the Council. The Competence Centre should comply with the provisions applicable to ~~the~~ Union institutions, and with national ~~legislation~~***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 ~~XXX~~ (EU, Euratom) ***2018/1046*** of the European Parliament and of the Council[14] ~~[the Financial Regulation]~~.

---

13 ***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).***
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).

14 ***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 ***strengthening the Union's competitiveness and capacities,*** 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*** ~~due~~ the fact that existing, limited resources are dispersed as well as due to the scale of the investment necessary, but can rather by reason of avoiding unnecessary duplication ofthese 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***. In addition, actions at Union level can promote a high level of cybersecurity in all Member States. Hence***, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve ~~that objective~~***those objectives***.

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 to~~***have an essential role in*** 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 ***contribute to the implementation*** of the Horizon Europe programme ~~established by Regulation No XXX~~ and in particular Section ~~2.2.6~~***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].

2a. Member States shall collectively contribute to the work of the Competence Centre and the Network

~~3. The seat of the Competence Centre shall be located in [Brussels, 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 laws of that Member State. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings.~~

-a This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the state in areas of criminal law.

Article 2

Definitions

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

(1) ~~'~~‘cybersecurity~~'~~***’*** means the ~~protection of~~***activities necessary to protect*** network and information systems, ~~their~~***the*** users ***of such systems***, and other persons ~~against~~***affected by*** cyber threats;

(-a) ‘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 ***commercial and non-commercial*** ICT products, services or ~~process~~***processes*** with the specific purpose of protecting network and information systems ***and/or ensuring the confidentiality, integrity and accessibility of data, that is processed or stored in network and information systems, as well as the cybersecurity of the***~~,~~ ~~their~~ users ***of such systems and other***~~and affected~~ persons ~~from~~***affected by*** cyber threats;

(-b) ‘cyber threat’ means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;

(3) ~~'public authority'~~ ***"joint action"*** 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;~~***an action included in the annual work programme receiving Union financial support from the Horizon Europe programme, the Digital Europe programme and/or other Union programmes, 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 ~~Member State' means a Member State~~***in projects funded through this Regulation,*** which ~~voluntarily contributes financially to the administrative and operational costs of the Competence Centre~~***are not financed by a Union contribution or by financial contributions by Member States***.

(-c) 'European Digital Innovation Hubs' means a legal entity as defined in Regulation (EU) 2019/XXX of the European Parliament and of the Council[15].

(5) 'Agenda' means a comprehensive and sustainable Cybersecurity Industrial, Technology and Research strategy, which shall set out strategic recommendations for the development and growth of the European cybersecurity industrial, technological and research sector and shall set out strategic priorities for the Competence Centre's activities (the "Agenda"). The Agenda shall not be binding with respect to decisions to be taken on the annual work programmes.

---

15 ***Regulation (EU) 2019/XXX of the European Parliament and of the Council of ... establishing the Digital Europe programme for the period 2021-2027 (OJ L ...) (2018/0227(COD)).***

(6) 'Technical assistance' when offered by the Competence Centre means assisting the National Coordination Centres or the Community for the performance of theirs tasks, by providing knowledge or facilitating access to expertise in the field of cybersecurity research, technology and industry, facilitating networking, raising awareness, promoting cooperation, and when offered by the Competence Centre together with the National Coordination Centres to stakeholders means project preparation in relation to the mission and objectives set out in this Regulation.

Article 3

Mission of the Centre and the Network

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

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

   (aa) support European technological capacities, capabilities and skills in relation to the resilience and reliability of the infrastructure of network and information systems, including critical infrastructure and commonly used hardware and software in the Union;

   (b) increase the ***global*** competitiveness of the Union's cybersecurity industry***, to ensure high cybersecurity standards throughout the Union*** and turn cybersecurity into ***a*** competitive advantage of other Union industries~~.~~***;***

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

-a The Competence Centre shall utilise relevant Union financial resources in such a way so as to contribute to the mission set out in paragraph 1 in accordance with the legal acts establishing these programmes notably Horizon Europe and Digital Europe.

Article 4

Objectives ~~and Tasks~~ of the Centre

The Competence Centre shall ~~have the following objectives and related tasks:~~***enhance research, innovation and deployment in the field of cybersecurity in order to fulfil the mission as described in Article 3 by;***

(a) enhancing cybersecurity capacities, capabilities, knowledge and infrastructures at the service of industries, in particular SMEs, research communities, the public sector and civil society as appropriate

(b) complementing the efforts of other public actors, promote cybersecurity resilience, the uptake of cybersecurity best practices, the principle of security by design, and the certification of the security of digital products and services,

(c) contributing to a strong European cybersecurity ecosystem which brings together all relevant stakeholders in particular by

(1) defining strategic recommendations for research, innovation and deployment in cybersecurity in line with Union law and setting out strategic priorities for the Centre's activities;

(2) implementing actions under relevant Union funding programmes in line with the respective work programmes and programme regulations;

(3) fostering cooperation and coordination amongst the National Coordination Centres and with and within the Cybersecurity Competence Community, and

(4) where relevant and appropriate, acquiring and operating ICT infrastructures and services where necessary to fulfil the tasks below and in accordance with the respective work programmes set out below

~~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[16] 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[17] 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;~~

~~16 [add full title and OJ reference]~~
~~17 [add full title and OJ reference]~~

(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;

(d) providing financial support and technical assistance to cybersecurity start-ups and SMEs to connect to potential markets and to attract investment;

5. improve the understanding of cybersecurity and contribute to reducing skills gaps in the Union related to cybersecurity by carrying out the following tasks:

(a) supporting further development of cybersecurity skills , where appropriate together with relevant EU agencies and bodies including ENISA.

6. contribute to the reinforcement of cybersecurity research and development in the Union by:

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

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

(c) 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:

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

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

(c) ~~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:~~

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

(b) ~~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 fulfil the mission laid out in Article 3 and the objective 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 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:

(2)i defining priorities for its work on:

- *the enhancement of cybersecurity research and innovation, covering the entire innovation cycle, and its deployment,*
- *the development of cybersecurity industrial, technological and research capacities, capabilities, and infrastructure,*
- *the reinforcement of cybersecurity and technology skills and competences in industry, technology, research and at all relevant educational levels, supporting gender balance,*
- *the deployment of cybersecurity products and solutions,*
- *support the market uptake of cybersecurity products, processes and services contributing to the mission set out in Article 3,*
- *the support of the adoption and integration of state-of-the-art cybersecurity products and processes by public authorities at their request, demand side industries and other users; and*

(2)ii supporting cybersecurity industry, and in particular SMEs, with a view to strengthening the Union excellence, capacities and competitiveness on cybersecurity, including with a view to connecting to potential markets and deployment opportunities, and to attracting investment;

(2)iii providing support and technical assistance to cybersecurity start-ups, SMEs, microenterprises, associations, individual experts and to civic tech projects;

(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, including with regard to procurements and deployment of technologies, upon request from a Member State to that Member State;

(6) facilitating collaboration and sharing of expertise among all relevant stakeholders, in particular members of the Cybersecurity Competence Community;

(6a) attending national, European and international conferences, fairs and fora related to its mission, objectives and other tasks, as appropriate, with the aim of sharing views and exchanging relevant best-practices with other participants;

(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 replicating good cybersecurity practices and cybersecurity products and solutions, and in particular those developed by small and medium enterprises (SMEs) and those using open source software;

(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, SMEs, micro-enterprises, associations and civic tech projects in the Union and facilitating their access to expertise, funding, investment and to markets;

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

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

(2) 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

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

(2a) supporting, where appropriate, the achievement of the specific objective 4, Advanced digital skills, of the Digital Europe Programme in cooperation with European Digital Innovation Hubs; providing expert advice on cybersecurity industry, technology and research to the Commission when it prepares the draft work programmes pursuant to Article 11 of Council Decision (XXXX)[18];

(3) providing expert advice on cybersecurity industry, technology and research to the Commission when it prepares the draft work programmes pursuant to Article 11 of Council Decision (XXXX)[19];

(4) carrying out or enabling the deployment and facilitating the acquisition of ICT infrastructures, at the service of society, industries, the public sector at the request of the respective Member State, research communities and operators of essential services, through inter alia contributions from Member States and Union funding for joint actions, in line with the Agenda, the multiannual work programme and the annual work programme.

---

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

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

(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]

(ca) raising awareness of the Centre's and Network's mission, objectives and tasks as laid down in articles 3, 4, and 4a of this regulation.

(aa) without prejudice to the civilian nature of projects to be financed from the Horizon Europe programme and in line with the respective programme regulations, enhancing synergies and coordination between the cybersecurity civilian and defence spheres, by:

- *facilitating the exchange of knowledge and information with regard to dual use technologies and applications,*
- *facilitating the exchange of results, requirements and best practices,*
- *facilitating the exchange of information with regard to the priorities of relevant Union programmes.*

Article 5

[…]

Article 6

Nomination of National Coordination Centres

1. ~~By [date],~~ ***Within 6 months after the entry into force*** each Member State shall nominate ~~the~~***one*** entity to act as the National Coordination Centre for the purposes of this Regulation and notify it ***without delay*** to the ***Governing Board. Such entity may be an entity already established in that Member State.***

   This maximum period of 6 month shall be extended for the period during which the Commission ***delivers the opinion referred to in paragraph 1a***.

1a. A Member State may, at any time, ask the Commission for an opinion concerning the capacity of the entity that the Member State has nominated or intends to nominate as its National Coordination Centre to manage funds so as to achieve the mission and objectives laid down in this Regulation. The Commission shall deliver its opinion to that Member State within three months.

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

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, 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***. It shall have the capacity*** ~~and be in a position~~ to effectively engage and coordinate with ***the*** industry, the public sector ~~and the~~ ***, the academic and*** research community ***and citizens, including authorities designated pursuant to the Directive (EU) 2016/1148***.

4a. At any time, the National Coordination Centres may request to be recognized as fulfilling the capacity to manage funds so as to achieve the mission and objectives laid down in this Regulation, in accordance with the rules of Horizon Europe and Digital Europe.
Based on such a request, the Commission shall assess the capacity of that National Coordination Centre to manage funds so as to achieve the mission and objectives laid down in this Regulation and issue a decision within three months of the request.

Where the Commission has provided a positive opinion to a Member State in accordance with the procedure laid down in paragraph 1a, that opinion shall be deemed to be an approval decision regarding the respective entity in accordance with this paragraph.

Following a consultation with the Governing Board, the Commission shall issue, no later than 2 months from the entry into force of this Regulation, guidelines, including a specification of the conditions and how opinions and assessments are conducted.

When adopting its opinion and decision, the Commission shall take into account the information and documentation provided by the requesting National Coordination Centre.

In order to ensure that the opinion and decision process is transparent, any rejection must be duly justified, setting out the requirements the requesting National Coordination Centre has not yet fulfilled in order to for the request to be approved. Any National Coordination Centre whose request has been rejected, may at any time re-submit its request with additional information.

Member States shall inform the Commission in case of changes of the National Coordination Centre (in the composition, legal nature or other relevant aspects) affecting its capacity to manage EU funds upon which the Commission may review its decision accordingly.

5. **[…]**

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) ~~supporting the~~ ***acting as contact points at the national level for the Cybersecurity*** Competence ***Community to support the*** Centre in achieving its ~~objectives and~~ ***objective and mission*** in particular in coordinating the Cybersecurity Competence Community ***through the coordination of its national members***;

   (aa) providing expertise and actively contributing to the strategic tasks referred to in Article 4a, taking into account relevant national and regional challenges for cybersecurity in different sectors;

   (b) ~~facilitating~~***promote, encourage and facilitate*** the participation of ***civil society,*** industry***, in particular start-ups and SMEs, academic and research communities*** and other actors at the Member State level in cross-border projects ***and cybersecurity actions funded through all relevant Union programmes***;

(ba) Provide technical assistance to stakeholders by supporting the stakeholders in their application phase for projects managed by the Centre in relation to the mission and objectives set out in this Regulation, and in full compliance with the rules of sound financial management, especially on conflict of interests.

(c) **[…]**

(d) **[…]**

(e) seeking to establish synergies with relevant activities at the national***, regional and local*** ~~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 ~~XXX [new Financial Regulation]~~***(EU, Euratom) 2018/1046*** under conditions specified in the ~~concerned~~ grant agreements~~.~~ ***concerned;***

(fa) without prejudice to the national competences of Member States for education and taking into account the relevant tasks of ENISA, engage with national authorities regarding a possible contribution to promoting and disseminating cybersecurity educational programmes;

(g) promoting and disseminating the relevant outcomes of the work by the Network, the Cybersecurity Competence Community and the Competence Centre at national***, regional or local*** ~~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~~.~~***;***

(ha) 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 ~~XXX [new Financial Regulation]~~***(EU, Euratom) 2018/1046,*** including in the form of lump sums.

3. ***Based on the decision in Art. 6 para 4a,*** 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 ~~XXX [new Financial Regulation] in~~***(EU, Euratom) 2018/1046in*** relation to carrying out the tasks laid down in this Article.

4. National Coordination Centres shall, where relevant, cooperate through the Network~~ for the purpose of implementing tasks referred to in points (a), (b), (c), (e) and (g) of paragraph 1.~~**.**

Article 8

The Cybersecurity Competence Community

1. The Cybersecurity Competence Community shall contribute to the mission of the ~~Competence Centre~~***Centre and the Network*** as laid down in Article 3 and enhance***, share*** and disseminate cybersecurity expertise across the Union.

2. The Cybersecurity Competence Community shall***, on the one hand,*** consist of industry, ***including SMEs,*** academic and ~~non-profit~~ research organisations, ~~and~~***other relevant civil society*** associations as well ***as, as appropriate, relevant European Standardisation Organisations,*** ~~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 technological***, industrial, academic and research*** ~~and industrial~~ capacities in the Union. It shall involve National Coordination Centres***, European Digital Innovation Hubs where relevant*** as well as Union Institutions and bodies with relevant expertise~~.~~***, such as ENISA***.

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

(a) ***academia,*** research ***and innovation***;

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

(c) training and education.

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

(da) ethics;

(db) formal and technical standardisation and specifications.

4. The ~~Competence~~ Centre shall ~~accredit~~***register*** entities***, upon their request,*** ~~established under national law~~ as members of the Cybersecurity Competence Community after an assessment made by the National Coordination Centre of the Member State where the entity is established, ~~on~~ ***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 registration***. ~~An accreditation~~ shall not be limited in time but may be revoked by the ~~Competence~~ Centre at any time if ~~it or~~ the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 ***of this Article*** or ~~it~~ falls under the relevant provisions set out in Article 136 of Regulation ~~XXX [new financial regulation]~~***(EU, Euratom) 2018/1046, or for justified security reasons. Where Community membership is revoked on security grounds, such a decision shall be proportional and justified. The National Coordination Centres of the Member States shall aim to achieve a balanced representation of stakeholders in the Community, actively stimulating participation from SMEs in particular***.

-a National Coordination Centres shall be encouraged to cooperate through the Network in order to harmonise the way in which they apply the criteria provided for in paragraph 3 of this Article and the procedures for assessing and registering entities referred to in paragraph 4 of this Article.

5. 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 ~~entity~~ ***Union body, agency or office*** meets the criteria provided for in paragraph 3. ~~An accreditation~~ ***of this Article. A registration*** shall not be limited in time but may be revoked by the Competence Centre at any time if it considers that the ~~entity~~ ***Union body, agency or office*** does not fulfil the criteria set out in paragraph 3 ~~or it~~***of this Article or*** falls under the relevant provisions set out in Article 136 of Regulation ~~XXX [new financial regulation]~~***(EU, Euratom) 2018/1046*** .

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

6a. Entities registered as members of the Cyber Competence Community shall designate their respective representatives to ensure an efficient dialogue. Those representatives shall have expertise with regard to cybersecurity research, technology or industry. The requirements may be further specified by the Governing Board, without unduly limiting the entities in designating their representatives.

6b. The Cybersecurity Competence Community shall through its working groups and in particular through the Strategic Advisory Group referred to in Article 18 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.

Article 9

Tasks of the members of the Cybersecurity Competence Community

The members of the Cybersecurity Competence Community shall:

(1) support the Competence Centre in achieving the mission and the objectives laid down in Articles 3 and 4 and, for this purpose, work closely with the Competence Centre and the ~~relevant~~ National ~~Coordinating~~***Coordination*** Centres;

(2) **[…]**

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

Article 10

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

1. ~~The Competence~~***To ensure coherence and complementarity, avoiding any duplication of efforts the*** Centre shall cooperate with relevant Union institutions, bodies, offices and agencies including ~~the European Union Agency for Network and Information Security~~***ENISA*** , ~~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[20], the*** ~~,~~ Innovation and Networks Executive Agency ***established by Commission Implementing Decision 2013/801/EU[21], relevant European Digital Innovation Hubs, 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[22],*** ~~as well as~~ the European Defence Agency ***in relation to the tasks specified in art 4a , and other relevant Union entities***. ***The Centre may also cooperate with international organisations, where relevant.***

2. Such cooperation ~~shall~~***may*** take place within the framework of working arrangements. Those arrangements shall be submitted to the ~~prior~~ approval of the ***Governing Board*** ~~Commission~~. ***Any sharing of classified information shall take place within the framework of administrative arrangements concluded in accordance with Article 36 (4).***

---

20 ***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).***

21 ***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).***

22 ***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 ***ensure the achievement of 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 and who shall be supported by the staff of the Competence Centre***

   (c) ~~an Industrial and Scientific~~***a Strategic*** Advisory ~~Board~~***Group*** which shall exercise the functions set out in Article 20.

SECTION I
GOVERNING BOARD

Article 12

Composition of the Governing Board

1. The Governing Board shall be composed of one representative of each Member State, and ~~five~~***two*** representatives of the Commission, on behalf of the Union.

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

3. Members of the Governing Board and their alternates ***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 ***cybersecurity research,*** technology ~~as well as of~~ ***and industry, their interlink with their respective National Coordination Centre or their relevant managerial, administrative and budgetary skills. Members of the Governing Board and their alternates appointed by the Commission shall be appointed in light of their knowledge in the field of cybersecurity, technology, or their*** relevant managerial, administrative and budgetary skills ***and of their capacity 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 ~~Governing Board members~~ ***members of the Governing Board*** shall act ~~in the interest of the Competence~~ ***to safeguard the*** Centre~~, safeguarding its~~ ***'s*** 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***, and the members of the Community***, to take part in the meetings of the Governing Board as appropriate.

7. ~~The European Agency for Network and Information Security (~~ ***A representative from*** ENISA~~)~~ shall be a permanent observer in the Governing Board. ***The Governing Board may invite a representative from the Strategic Advisory Group.***

7a. The Executive Director shall take part in the meetings of the Governing Board but shall have no right to vote.

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. These rules shall include specific procedures for identifying and avoiding conflicts of interest and ensure the confidentiality of any sensitive information.

3. The Governing Board shall take the necessary strategic decisions, in particular:

   (a) ~~adopt a multi-annual strategic plan, containing a statement of the major priorities and planned initiatives of the Competence Centre, including an estimate of financing needs and sources~~***develop and adopt the Agenda and monitor its implementation***;

   (aa) reflecting the Union's policy priorities and the Agenda, adopt the multiannual work programme containing the common, industrial, technology and research priorities, which are based on 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;

(ab) adopt the annual work programme for implementing the relevant Union funds, notably the cybersecurity parts of the Horizon Europe programme insofar as they are co-financed voluntarily by Member States and the Digital Europe programme, in accordance with the Centre's multiannual work programme and the strategic planning process of the Horizon Europe programme. Insofar the annual work programme contains joint actions, it shall contain information about Member States' voluntary contributions to joint actions. Where appropriate, proposals and in particular the annual work programme shall assess the need to apply security measures 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,~~ ***'s*** annual accounts, balance sheet and annual activity report, on the basis of a proposal from the Executive Director;

(c) adopt the specific financial rules of the Competence Centre in accordance with [Article 70 of ~~the FR~~***Regulation (EU, Euratom) 2018/1046***];

(ca) as part of the annual work programme adopt decisions to allocate funds from the Union budget to topics for 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), and 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~~;~~ ***and appoint, dismiss, extend the term of office of, provide guidance to and monitor the performance of the Executive Director***

(e) ~~adopt the criteria and procedures~~***decide on the adoption of guidelines*** for assessing and accrediting the entities as members of the Cybersecurity Competence Community;

(ea) adopt the working arrangements referred to in Article 10(2);

(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 ***transparency*** rules ~~regarding~~***for the Competence Centre and rules for the prevention and management of*** conflicts of interest ***including in respect of the Governing Board members in accordance with Article 42 of the Commission Delegated Regulation (EU) 2019/715***;

[1] 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).

(i) ~~establish~~***decide on the establishment of*** working groups ***within the Community, where relevant taking into account advice provided by the Strategic Advisory Group.*** ~~with members of the Cybersecurity Competence Community;~~

(j) appoint members of the ~~Industrial and Scientific~~***Strategic*** Advisory ~~Board;~~***Group.***

(k) ~~set up an Internal Auditing Function in accordance with Commission Delegated Regulation (EU) No 1271/2013[23];~~***decide on the adoption of rules on the reimbursement of expenses for the members for the Strategic Advisory Group***

~~[23] 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).~~

(l) ~~promote the Competence~~***set up a monitoring mechanism to ensure that the implementation of the respective funds managed by the*** Centre ~~globally, so as to raise its attractiveness and make it a world-class body for excellence in cybersecurity~~***is done in accordance with the Agenda, the mission and the multiannual work programme and with the rules of programmes where funding originates from***;

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

(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 ***and anti-corruption*** strategy that is proportionate to the fraud ***and corruption*** risks ***as well as adopt comprehensive protection measures for persons reporting on breaches of Union law in accordance with applicable Union legislation,*** having regard to a cost-benefit analysis of the measures to be implemented;

(s) ***if necessary*** 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, or any other applicable Regulation***;

(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;~~

(ta) 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 (ab) of paragraph 3, the Executive Director and the Governing Board shall take into account any relevant strategic advice and input provided by ENISA, 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 ~~chair~~***Chairperson***, or at the request of the Executive Director in the fulfilment of his/her tasks.

3. The Executive Director shall take part in the deliberations, unless decided otherwise by the Governing Board, but shall have no voting rights. ~~The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers.~~

-a The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers.

4. ~~Members~~***Representatives*** of the ~~Industrial and Scientific Advisory Board~~ ***Cybersecurity Competence Community*** 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, the representatives of the Commission constituting a single member for this purpose and accounting for 26% for the total vote in the cases referred to in paragraph -3 of this Article. 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.

-2a. 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).

-3. For decisions which are taken under Article 13(3) subparagraphs (b), (c), (g), (o), (p), (r), (s), (f), (k), (aa), (ab), (ca), (sb) and (l), the Commission shall have 26% of the total vote.

1. ~~The Union shall hold 50 % of the voting rights. The voting rights~~***For decisions other than those referred to in paragraphs -2a (b) and -3, each Member State and the Union shall have one vote. The vote*** of the Union shall be ~~indivisible~~***cast jointly by the two representatives of the Commission***.

2. ~~Every participating~~***If the Chairperson has been elected from among the representatives of the*** Member ~~State~~***States, the Chairperson*** shall ~~hold one vote~~***take part in the voting as a representative of his or her Member State***.

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***, transparent and non-discriminatory*** ~~and transparent~~ selection procedure.

4. For the purpose of concluding the contract of the Executive Director, the Competence Centre shall be represented by the Chairperson of the Governing Board.

5. The term of office of the Executive Director shall be four years. By the end of that period, the Commission shall carry out an assessment which takes into account the evaluation of the performance of the Executive Director and the Competence Centre's future tasks and challenges.

6. The Governing Board may, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 5, extend once the term of office of the Executive Director for no more than four years.

7. An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post.

8. The Executive Director shall be removed from office only by decision of the Governing Board, acting on a proposal from the Commission ***or at least 50% of the Member States***.

Article 17

Tasks of the Executive Director

1. The Executive Director shall be responsible for operations and for the day-to-day management of the Competence Centre and shall be its legal representative. The Executive Director shall be accountable to the Governing Board and perform his or her duties with complete independence within the powers assigned to him or her.

2. The Executive Director shall in particular carry out the following tasks in an independent manner:

   (a) implement the decisions adopted by the Governing Board;

   (b) support the Governing Board ***in*** its work, provide the secretariat for ~~their~~***its*** meetings and supply all information necessary for the performance of ~~their~~***its*** duties;

   (c) after consultation with the Governing Board and the Commission, ***and taking into account the input of the National Coordination Centres and the Cybersecurity Competence Community,*** prepare and submit for adoption to the Governing Board the ***agenda, and in accordance with it the*** draft multiannual ~~strategic plan~~***work programme*** and the draft annual work ~~plan~~***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*** ~~work plan~~ and the corresponding expenditure estimates as proposed by the Member States and the Commission~~;~~

   (d) prepare and submit for adoption to the Governing Board the draft annual budget, including the corresponding ***establishment plan referred to in point (g) of Article 13(3),*** ~~staff establishment plan~~ indicating the number of temporary posts in each grade and function group and the number of contract staff and seconded national experts expressed in full-time equivalents;

   (e) implement the ***annual work programme and the multiannual work programme*** ~~work plan~~ and report to the Governing Board thereon;

(f) prepare the draft annual activity report on the Competence Centre, including the information on corresponding expenditure ***and the realisation of the Agenda and the multiannual work programme of the Competence Centre; 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 ~~following-up~~ ***that follows up*** on the conclusions of the retrospective evaluations and ~~reporting~~***reports*** on progress every two years to the Commission ***and the European Parliament;***

(i) prepare~~, negotiate~~ and conclude ~~the~~ agreements with the National Coordination Centres;

(j) be responsible for administrative, financial and staff matters, including the implementation of the Competence Centre budget, taking due account of advice received from the Internal Auditing Function, within the limits of the ~~delegation by the Governing Board~~***decisions referred to in points (c), (g), (o), (p), (q) and (r) of Article 13(3)*** ;

(k) approve and manage the launch of calls for proposals, in accordance with the ***annual work programme,*** ~~work plan~~ 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 fortenders, in accordance with the ***annual work programme,*** ~~work plan~~ and administer the contracts;

(n) approve the tenders selected for funding;

(o) submit the draft annual accounts and balance sheet to the Internal Auditing Function, and subsequently to the Governing Board,

(p) ensure that risk assessment and risk management are performed;

(q) sign individual grant agreements, decisions and contracts;

(r) sign procurement contracts;

(s) prepare an action plan ~~following up~~***that follows 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***[24] ***("OLAF") and report***~~and reporting~~ on progress twice a year to the Commission and regularly to the Governing Board;

(t) prepare draft financial rules applicable to the Competence Centre;

(u) establish and ensure the functioning of an effective and efficient internal control system and report any significant change to it to the Governing Board;

(v) ensure effective communication with the Union's institutions ***and report, upon invitation, to the European Parliament and to the Council***;

(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.

---

[24] ***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~~STRATEGIC ADVISORY ~~BOARD~~GROUP

Article 18

Composition of ~~the Industrial and Scientific~~

Strategic** Advisory ~~Board~~**Group

1. The ~~Industrial and Scientific~~***Strategic*** Advisory ~~Board~~***Group*** shall consist of no more than ~~16~~***20*** members. The members shall be appointed by the Governing Board***, acting on a proposal from the Executive Director*** from among the representatives of the entities of the ***Community, except Union bodies. Only representatives of entities which are not controlled by a third country or a third-country entity shall be eligible. The appointment shall be made in accordance with an open, transparent, and non-discriminatory procedure. The Group's composition shall aim to achieve a balanced representation of the*** Cybersecurity Competence community ***between scientific, industrial and civil society entities, demand and supply side industries, large, medium and small enterprises, as well as in terms of geographical provenance and gender, as well as intra sectorial balance, having regard to the cohesion of the Union and all of its Member States in the field of cybersecurity research, industry and technology. Its membership shall enable a comprehensive, continuous, and permanent dialogue between the Community and the Competence Centre***.

2. Members of the ~~Industrial and Scientific~~***Strategic*** Advisory ~~Board~~***Group*** shall have expertise either with regard to cybersecurity research, industrial development, ~~professional services or the deployment thereof~~***offering, implementing, or deploying professional services or products***. The requirements for such expertise shall be further specified by the Governing Board.

3. Procedures concerning the appointment of its members by the Governing Board and the operation of the ~~Advisory Board~~***Strategic Group***, shall be specified in the ~~Competence Centre's~~***Governing Board's*** rules of procedure and shall be made public.

4. The term of office of members of the ~~Industrial and Scientific~~***Strategic*** Advisory ~~Board~~***Group*** shall be ~~three~~***two*** years. That term shall be renewable ***once***.

5. Representatives of the Commission and of ***other Union bodies, in particular the ENISA, may be invited by the Strategic Advisory Group to***~~the European Network and Information Security Agency may~~ participate in and support ***its works. The Group may invite additional representatives from the Community in an observer, adviser, or expert capacity as appropriate, on a case-by-case basis, to take into account the dynamic of developments in the field of cybersecurity. Members of the Governing***~~the works of the Industrial and Scientific Advisory~~ Board ***may participate as observers in the meetings of the Strategic Advisory Group***.

Article 19

Functioning of the ~~Industrial and Scientific~~

Strategic *Advisory* ~~*Board*~~***Group***

1. The ~~Industrial and Scientific~~***Strategic*** Advisory ~~Board~~***Group*** shall meet at ***least three times*** ~~least twice~~ a year.

2. The ~~Industrial and Scientific Advisory Board may advise~~***Strategic Advisory Group shall provide suggestions to*** the Governing Board on the establishment of working groups ***within the Community in accordance with point (i) of Article 13(3)*** on specific issues relevant to the work of the Competence Centre***, whenever those issues fall within the tasks and areas of competence outlined in Article 20 and*** where necessary under the overall coordination of one or more members of ~~the Industrial and Scientific~~ ***the Strategic*** Advisory ~~Board~~***Group***.

3. The ~~Industrial and Scientific~~***Strategic*** Advisory ~~Board~~***Group*** shall elect its chair ***by simple majority of its members***.

3a. The secretariat of the Strategic Advisory Group shall be provided by the Executive Director and his/her staff, using existing resources and with due regard to their overall workload. The resources assigned to the support of the Strategic Advisory Group shall be indicated in the draft annual budget.

4. The ~~Industrial and Scientific~~***Strategic*** Advisory ~~Board~~***Group*** shall adopt its rules of procedure~~, including the nomination of the representatives that shall represent the Advisory Board where relevant and the duration of their nomination~~ ***by simple majority***.

Article 20

Tasks of the ~~Industrial and Scientific~~

Strategic *Advisory ~~Board~~****Group***

The ~~Industrial and Scientific~~***Strategic*** Advisory ~~Board~~***Group*** shall ***regularly*** advise the Competence Centre in respect of the performance of its activities***, ensure communication with the Community and other relevant stakeholders,*** and shall:

(1) ***taking into account contributions from the Community and working groups referred to in point (i) of Article 13(3) where relevant,*** provide ***and continuously update strategic advice and input*** to the Executive Director and the Governing Board ~~strategic advice and input for drafting the work plan~~***with regard to the Agenda and the annual*** and multi-annual ~~strategic plan~~***work programmes*** within the deadlines set by the Governing Board;

(-a) advise the Governing Board on the establishment of working groups within the Community in accordance with point (i) of Article 13(3) on specific issues relevant to the work of the Competence Centre;

(2) ***subject to approval by the Governing Board, decide on and*** 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 Competence Centre shall be funded by the Union while joint actions shall be funded by the Union and voluntary contributions by the Member States.

-1a. The administrative and operational costs of joint actions shall be covered by the Union and by the Member States contributing to the joint actions, in accordance with the HEP and DEP Regulations.

1. The Union's contribution to the Competence Centre to cover administrative costs and operational costs shall comprise the following:

   (a) ***up to EUR 1 649 566 000***~~EUR 1 981 668 000~~ from the Digital Europe programme, including up to EUR ~~23 746 000~~***32 000 000*** 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 by Member States pursuant to paragraph 5 of this Article but not exceed the amount determined in***~~to be determined taking into account~~ the strategic planning process ***of the Horizon Europe programme*** to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation] ***and the multiannual work programme and the annual work programme***.

   (ba) an amount from the other relevant European Union programmes, as needed for the implementation of tasks or achievement of objectives of the Centre set in Article 4, subject to decisions taken in line with the regulations establishing these 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 ***and to other programmes and projects falling within the scope of the Competence Centre or the Network***.

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~~***62(1)*** of Regulation (EU, Euratom) ~~XXX~~[25] ~~[the financial regulation]~~ ***2018/1046***.

4. ~~The~~***Contributions from*** Union ~~financial contribution~~***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 ~~cover the tasks~~***be accounted for in the calculation of the Union maximum financial contribution*** referred to in ~~Article 4(8)(b)~~***paragraphs 1 and 2.***

5. Member States shall voluntarily take part in joint actions with their voluntary financial and/or in-kind contributions. When a Member State takes part in a joint action, the financial contribution by that Member State shall cover administrative costs in proportion to its contribution to that joint action. Contribution to administrative costs of joint actions shall be financial. Contribution to the operational costs of joint actions may be financial or in-kind, in accordance with the Horizon Europe programme and/or the Digital Europe programme. Contributions by each Member State may take the form of support by that Member State provided in a joint action to beneficiaries stemming from that Member State joint action. 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 Regulation (EU, Euratom) 2018/1046.

---

[25] ~~[add full title and OJ reference]~~

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) – reference to be checked] of this Regulation.

[…]

7. Member States' national co-funding of actions supported by Union programmes other than Horizon Europe and Digital Europe shall be considered as Member States' national contributions as far as these are part of joint actions and included in the Competence Centre's work programme.

~~2~~***8***. 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 ~~the~~***that*** Member State, and the applicable international accounting standards and international financial reporting standards. 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.

~~3~~***9***. 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 ~~its obligations have been met~~***that Member State meets its obligations***. The defaulting Member State's voting rights ***concerning joint actions*** shall be suspended until the default of its commitments is remedied.

4***10***. 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. ***The Commission's termination, reduction or suspension of the Union's financial contribution shall be proportionate in amount and time to the reduction, termination or suspension of the Member States' contributions.***

~~5~~***11***. 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 ~~paragraphs 1~~***paragraph 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. **[…]**

2. The administrative costs of the Competence Centre shall ~~not exceed EUR [number] and shall be~~***be in principle*** covered by means of financial contributions ~~divided equally~~ on an annual basis ~~between~~***from*** the Union***. Additional financial contributions shall be made by contributing*** ~~and the participating~~ Member States ***in proportion to their voluntary contributions to joint actions***. 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 ~~the form of:~~***case of joint actions***

   […]

4. The resources of the Competence Centre entered into its budget shall be composed of the following contributions:

   (a) ~~participating Member States'~~***the Union's*** financial contributions to the ***operational and*** administrative costs;

   (b) ~~participating~~***contributing*** Member States' ***voluntary*** financial contributions to the ~~operational~~***administrative*** costs ***in case of joint actions*** ;

   (c) ~~any revenue generated by Competence Centre~~***contributing Member States' voluntary financial contributions to the operational costs in case of joint actions*** ;

   (d) any ~~other financial contributions, resources and revenues.~~***revenue generated by Centre;***

(da) 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 Competence Centre and*** not be paid to the ~~participating~~***contributing*** members of the Competence Centre.

-a The Competence Centre shall cooperate closely with other Union institutions, agencies and bodies, having due regard to their respective mandates and without duplicating existing cooperation mechanisms, in order to benefit from synergies and, where possible and appropriate, to reduce administrative costs.

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***[26], to the Commission.

4. On the basis of ~~that~~***the*** 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~~***Articles*** 313 and 314 TFEU.

5. The European Parliament and the Council shall authorise the appropriations for the contribution to the Competence Centre.

---

[26] ***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).***

6. The European Parliament and the Council shall adopt the establishment plan ~~for the Competence Centre~~***referred to in point (g) of Article 13(3)***.

7. Together with the ***annual work programme and multi annual work programme***~~Work Plan~~, the Governing Board shall adopt the ***Competence*** 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***~~Work Plan~~ in accordance with the general budget of the Union.

Article 27

Presentation of the Competence Centre's accounts and discharge

The presentation of the Competence Centre's provisional and final accounts and the discharge shall follow the rules and timetable of ***Regulation (EU, Euratom) 2018/1046*** ~~the Financial Regulation~~ and of ~~its~~ ***the*** financial rules ~~adopted in accordance with Article 29~~***of the Competence Centre*** .

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***~~work plan~~ 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 by Member State and indicating the contribution of the Competence Centre to the individual participants and actions;

(d) progress towards the achievement of the ***mission set out in Article 3 and the*** objectives set out in Article 4 and proposals for further necessary work to achieve ~~these~~***that mission and those*** objectives~~.~~***;***

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

3. Once approved by the Governing Board, the annual activity report shall be made publicly available.

Article 29

Financial rules

The Competence Centre shall adopt its specific financial rules in accordance with Article 70 of Regulation ~~XXX [new Financial Regulation]~~***(EU, Euratom) 2018/1046*** .

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 ***regular and*** 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)~~***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[27] and Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council[28]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.

---

27 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).

28 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[29] ('Staff Regulations' and 'Conditions of Employment') and the rules adopted jointly by the institutions of the Union for the purpose of applying the Staff Regulations and Conditions of Employment shall apply to the staff of the Competence Centre.

2. The Governing Board shall exercise, with respect to the staff of the Competence Centre, the powers conferred by the Staff Regulations on the Appointing Authority and the powers conferred by the Conditions of Employment on the authority empowered to conclude contract ('the appointing authority powers').

3. The Governing Board shall adopt, in accordance with Article 110 of the Staff Regulations, a decision based on Article 2(1) of the Staff Regulations and on Article 6 of the Conditions of Employment delegating the relevant appointing authority powers to the Executive Director and defining the conditions under which that delegation may be suspended. The Executive Director is authorised to sub-delegate those powers.

4. Where exceptional circumstances so require, the Governing Board may***, through a*** ~~by~~ decision**,** temporarily suspend the delegation of the appointing authority powers to the Executive Director and any sub-delegation made by the latter. In such a case the Governing Board shall exercise itself the appointing authority powers or delegate them to one of its members or to a ~~staff~~ member of ~~the Competence~~ ***staff of the*** Centre other than the Executive Director.

---

[29] 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).

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 ~~of the Competence Centre~~***referred to in point (g) of Article 13(3)*** , 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 in the first instance by redeployment of*** staff ~~of the Competence~~ ***or posts from Union institutions, bodies, offices and agencies, and additional human resources through recruitment. The staff of the*** 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)~~***12*** 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 ofArticle 34(1) [Ownership and protection] of Regulation (EU) No XXX [Horizon Europe], when provided for in the ***annual work programme*** ~~Work plan~~, 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 ***for objection*** ~~to object~~ to transfers of ownership of results, or to grants of an exclusive license regarding results;

   (c) for the purposes of Article 37(3)(a) [Access rights] of Regulation (EU) No XXX [Horizon Europe], when provided for in the ***annual work programme***~~Work plan~~, 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 due time***, 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. The same transparency requirement applies to the national coordination centres, the community and the Strategic Advisory Group in accordance with relevant legislation***.

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 ***of the Horizon Europe Regulation.***

Article 35a

Gender Balance

In the implementation of this Regulation, when nominating candidates or proposing representatives, the European Commission, Member States and all other institutional and private sector stakeholders will choose representatives from several candidates, where possible, and with the aim of ensuring gender balance.

Article 36

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

1. ~~Without prejudice to Article 35, the Competence Centre shall not divulge to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment, in whole or in part, has been made.~~

2. ~~Members of~~ The Governing Board~~, the Executive Director, the members of the Industrial and Scientific Advisory Board, external experts participating in ad hoc Working Groups, and members of the staff of the Centre shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union, even after their duties have ceased~~ ***shall adopt the Centre's security rules, following approval by the Commission, applying the principles and rules laid down in Commission Decisions (EU, Euratom) 2015/443[30] and 2015/444[31]***.

3. ~~The Governing Board~~ ***Members*** 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[32] and 2015/444[33]~~***Governing Board, the Executive Director, external experts participating in ad hoc Working Groups, and members of the staff of the Competence 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***.

---

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

31 ***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).***

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

33 ~~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).~~

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 of the~~ ***conclusions of that*** evaluation shall be made public.

2. Once there is sufficient information available about the implementation of this Regulation, but no later than ~~three~~***two*** and a half years after the ~~start of the implementation~~***date referred to in Article 45 (4)*** of this Regulation, the Commission shall carry out an ~~interim evaluation~~***implementing report*** of the Competence Centre***, taking into account the preliminary input of the Governing Board, the National Coordination Centres and the Community***. 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~~***30 June*** 2024. The Competence Centre and Member States shall provide the Commission with the information necessary for the preparation of that report.

3. The ~~evaluation~~***implementation report*** 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 the 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~~. If the Commission considers that the continuation~~***, 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;

(d) an assessment of the ~~Competence~~***coordination and cooperation of the*** Centre ~~is justified with regard to its assigned objectives, mandate and tasks, it may propose that the duration of the mandate~~***with the Programme 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 ~~Competence~~ Centre***, the Horizon Europe programme and the Digital Europe programme;***

(e) an assessment on joint actions; ~~set out in Article 46 be extended.~~

(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 taking into account the preliminary input from the Governing Board, the National Coordination Centres and the Community. 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 assess legal and administrative aspects regarding the mandate of the Centre and potential to create synergies and reduce fragmentation with other Union bodies.

If the Commission considers that the continuation of the Centre is justified with regard to its assigned objectives, mandate and tasks, it may make a legislative proposal to extend the duration of the mandate of the Centre set out in Article 46.

4. On the basis of the conclusions of the interim ~~evaluation~~***report*** referred to in paragraph 2***,*** the Commission may ~~act in accordance with [Article 22(5)] or take any other~~***take*** 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 38a

Legal Personality of the Competence Centre

1. The Competence Centre shall have legal personality.

2. In each Member State, the Competence Centre shall enjoy the most extensive legal capacity accorded to legal persons under the law of that Member State. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings.

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:

   (1) pursuant to any arbitration clause contained in agreements, decisions or contracts concluded by the Competence Centre;

   (2) in disputes related to compensation for damage caused by the staff of the Competence Centre in the performance of their duties;

   (3) 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***, identification and resolution*** ~~and management~~ of conflicts of interest in respect of its members, bodies and staff***, including the Executive Director***. 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~~***Strategic*** Advisory ~~Board~~***Group,*** in accordance with Regulation ~~XXX [new Financial Regulation]~~***(EU, Euratom) 2018/1046, including provisions on any declarations of interest. Regarding conflict of interest, the National Coordination Centres shall be subject to national law***.

Article 43

Protection of Personal Data

1. The processing of personal data by the Competence Centre shall be subject to Regulation (EU) ~~No XXX/2018 of the European Parliament and of the Council~~***1725/2018*** .

2. The Governing Board shall adopt implementing measures referred to in Article ~~xx(3)~~***45(3)*** of Regulation (EU) ~~No xxx/2018~~***1725/2018***. The Governing Board may adopt additional measures necessary for the application of Regulation (EU) ~~No xxx/2018~~***No 1725/2018*** by the CompetenceCentre.

Article 44

Support from the host Member State

An administrative agreement may be concluded between the Competence Centre and the ***host*** 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 VI
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~~***his/her*** duties following his/her appointment by the Governing Board in accordance with Article 16, the Commission may designate an interim Executive Director***. That interim Executive Director shall*** ~~and~~ exercise the duties assigned to the Executive Director ~~who~~***and*** may be assisted by a limited number of ***members of staff of the*** Commission ~~officials~~. The Commission may assign a limited number of its ~~officials~~ ***members of staff*** 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~~***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 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~~ ***the date of entry into force of this Regulation*** to 31 December 2029.

2. At the end of ~~this~~***the*** period~~, unless decided otherwise through a review~~ ***referred to in paragraph 1*** of this ~~Regulation, the winding-up procedure shall be triggered. The winding-up procedure shall be automatically triggered if the Union or all participating Member States withdraw from the Competence Centre~~***Article, unless the mandate of the Centre is extended in accordance with the second subparagraph of Article 38(3), the winding-up procedure shall be triggered***.

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~~***contributing*** Member States in proportion to their financial contribution to the Competence Centre. Any such surplus distributed to the Union shall be returned to the Union budget.

Article 47

Entry into force

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

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

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*