European Parliament
2014-2019

TEXTS ADOPTED

P8_TA(2019)0419

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

European Parliament legislative resolution of 17 April 2019 on 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 (COM(2018)0630 – C8-0404/2018 – 2018/0328(COD))

(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2018)0630),

– having regard to Article 294(2) and Articles 173(3) and the first paragraph of Article 188 of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C8-0404/2018),

– having regard to Article 294(3) of the Treaty on the Functioning of the European Union,

– having regard to the opinion of the European Economic and Social Committee of 23 January 2019[1],

– having regard to Rule 59 of its Rules of Procedure,

– having regard to the report of the Committee on Industry, Research and Energy and the opinion of the Committee on the Internal Market and Consumer Protection (A8-0084/2019),

1. Adopts its position at first reading hereinafter set out[2];

2. Calls on the Commission to refer the matter to Parliament again if it replaces, substantially amends or intends to substantially amend its proposal;

3. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

---

1 Not yet published in the Official Journal.

2 This position corresponds to the amendments adopted on 13 March 2019 (Texts adopted, P8_TA(2019)0189).

P8_TC1-COD(2018)0328

Position of the European Parliament adopted at first reading on 17 April 2019 with a view to the adoption of Regulation (EU) …/… 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

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[1],

Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure,

Whereas:

---

1 OJ C , p. .

2 OJ C , , p. .

(1) ***More than 80 % of the population of the Union is connected to the internet and*** our daily lives and economies ~~become~~ ***are becoming*** increasingly dependent on digital technologies, ***with*** citizens ~~become~~ ***becoming*** more and more exposed to serious cyber incidents. Future security depends, among others, on ***contributing to overall resilience, on*** enhancing technological and industrial ability to protect the Union against ***constantly evolving*** cyber threats, as both ~~civilian~~ infrastructure and ~~military~~ ***security*** capacities rely on secure digital systems. ***Such security can be achieved by raising the awareness for cybersecurity threats, by developing competences, capacities, capabilities throughout the Union, thoroughly taking into account the interplay of hardware and software infrastructure, networks, products and processes, and the societal and ethical implications and concerns.*** **[Am. 1]**

(1a) Cybercrime is a fast growing threat to the Union, its citizens and its economy. In 2017, 80 % of the European companies experienced at least one cyber incident. The Wannacry-attack in May 2017 affected more than 150 countries and 230 000 IT-systems and had significant impacts on critical infrastructures, such as hospitals. This underlines the necessity for the highest cybersecurity standards and holistic cybersecurity solutions, involving people, products, processes and technology in the Union, as well as for the Union's leadership in the matter, and for digital autonomy. **[Am. 2]**

(2) The Union has steadily increased its activities to address growing cybersecurity challenges following the 2013 Cybersecurity Strategy[3] aimed to foster a reliable, safe, and open cyber ecosystem. In 2016 the Union adopted the first measures in the area of cybersecurity through Directive (EU) 2016/1148 of the European Parliament and of the Council[4] on security of network and information systems.

(3) In September 2017, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a Joint Communication[5] on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" to further reinforce the Union's resilience, deterrence and response to cyber-attacks.

(4) The Heads of State and Government at the Tallinn Digital Summit, in September 2017, called for the Union to become "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free***, 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 ISA²".*** **[Am. 3]**

---

3 Joint Communication to the European Parliament and the Council: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013)0001 final.

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

5 Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017)0450 final.

(4a) ***The European Cybersecurity Industrial, Technology and Research Competence Centre (the 'Competence Centre') should help to increase the resilience and reliability of the infrastructure of network and information systems, including the internet and other critical infrastructure for the functioning of society such as transport, health, and banking systems.*** **[Am. 4]**

(4b) ***The Competence Centre and its actions should take into account the implementation of Regulation (EU) 2019/XXX [recast of Regulation (EC) No 428/2009 as proposed by COM(2016)0616][6].*** **[Am. 5]**

(5) Substantial disruption of network and information systems can affect individual Member States and the Union as a whole. The ***highest level of*** security of network and information systems ***throughout the Union*** is therefore essential for ~~the smooth functioning of the internal market~~ ***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 technological capacities ***and capabilities*** to secure ~~its Digital Single Market, and in particular to protect~~ ***the protection of data and*** critical networks and information systems ***of European citizens and companies, including critical infrastructures for the functioning of society such as transport systems, health systems and banking, and the Digital Single Market,*** and to provide key cybersecurity services. **[Am. 6]**

---

6 ***Regulation (EU) 2019/... of the European Parliament and of the Council of ... setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (OJ L ..., ..., p. ...).***

(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 critical data, 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 microenterprises.*** **[Am. 7]**

(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 special support for SMEs by facilitating their access to knowledge and training in order to allow them to secure themselves sufficiently and to allow those who are active in cybersecurity to contribute to the Union's leadership in the field.*** **[Am. 8]**

(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. They contribute to the resilience, awareness and development of competence in cybersecurity matters and play an important role in building capacities for industry and research in the field.*** **[Am. 9]**

(6c) ***The term 'stakeholders', when used in the context of this Regulation, refers to, inter alia, industry, public entities and other entities which deal with operational and technical matters in the area of cybersecurity, as well as to civil society, inter alia trade unions, consumer associations, the Free and Open Source Software community, and the academic and research community.*** **[Am. 10]**

(7) The Council Conclusions adopted in November 2017 called on the Commission to provide rapidly an impact assessment on the possible options to create a network of cybersecurity competence centres with the European Research and Competence Centre and propose by mid-2018 the relevant legal instrument.

(8) The Competence Centre should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with the ~~Cybersecurity Competence~~ Network. It should deliver cybersecurity-related financial support from the Horizon Europe and Digital Europe programmes, ***as well as from the European Defence Fund for actions and administrative costs related to defence,*** and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to ***Union initiatives in the field of*** cybersecurity research ***and development***, innovation, technology and industrial development and avoiding duplication. **[Am. 11]**

(8a) ***"Security by design" as a principle established in Commission Joint Communication of 13 September 2017 entitled "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" includes state-of-the-art methods by which to increase security, at all stages of the lifecycle of a product or service, starting with secure design and development methods, reducing the attack surface, and incorporating adequate security testing and security audits. For the duration of operation and maintenance, producers or providers need to make available updates remedying new vulnerabilities or threats without delay, for the estimated lifetime of a product and beyond. This can also be achieved by enabling third parties to create and provide such updates. The provision of updates is especially necessary in the case of commonly used infrastructures, products and processes.*** **[Am. 12]**

(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 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 investing through the Competence Centre mechanism where relevant.*** **[Am. 13]**

(8c) ***The Competence Centre and the Cybersecurity Competence Community should, in order to foster the Union's competitiveness and the highest cybersecurity standards internationally, seek the exchange on cybersecurity products and processes, standards and technical standards with the international community. Technical standards include the creation of reference implementations, published under open standard licences. The secure design of, in particular, reference implementations is crucial for the overall reliability and resilience of commonly used network and information system infrastructure like the internet and critical infrastructures.*** **[Am. 14]**

(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~~ ***contribute***, and as an incentive for Member States to take part, only Member States who contribute financially to the administrative and operational costs of the Competence Centre should hold voting rights. **[Am. 15]**

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

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

(12) National Coordination Centres should be selected by Member States. In addition to the necessary administrative capacity, Centres should either possess or have direct access to cybersecurity technological expertise in cybersecurity, notably in domains such as cryptography, ICT security services, intrusion detection, system security, network security, software and application security, or human***,*** ~~and~~ ***ethical,*** societal ***and environmental*** 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[7], and the research community ***in order to establish a continuous public-private dialogue on cybersecurity***. ***In addition, awareness should be raised among the general public about cybersecurity through appropriate means of communication.*** **[Am. 16]**

[7] 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 in order to support third parties at the national level, this shall be passed on to relevant stakeholders through cascading grant agreements.

(14) Emerging technologies such as artificial intelligence, Internet of Things, high-performance computing (HPC) and quantum computing, ~~blockchain and~~ ***as well as*** concepts such as secure digital identities create at the same time new challenges for cybersecurity as well as offer ~~solutions~~ ***products and processes***. Assessing and validating the robustness of existing or future ICT systems will require testing security ~~solutions~~ ***products and processes*** against attacks run on HPC and quantum machines. The Competence Centre, the Network***, the European Digital Innovation Hubs*** and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity ~~solutions. At the same time the Competence~~ ***products and processes, including dual use, in particular those that help organisations to be in a constant state of building capacity, resilience and appropriate governance. The Competence*** Centre and the Network ***should stimulate the whole innovation cycle and contribute to bridging the valley of death of innovation of cybersecurity technologies and services. At the same time the Competence Centre, the Network and the Community*** 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 cybersecurity challenges***, and research the various motivations of attacks on the integrity of networks and information systems, such as crime, industrial espionage, defamation, and disinformation***. **[Am. 17]**

(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 solutions that help entities to be able to constantly build capability to enhance their and the Union's resilience.*** **[Am. 18]**

(14b) ***The Competence Centre should have the objectives to establish the Union's leadership and expertise in cybersecurity, and by that guarantee the highest security standards in the Union, ensure the protection of data, information systems, networks and critical infrastructures in the Union, create new high-quality jobs in the area, prevent brain drain from the European cybersecurity experts to third countries, and add European value to the already existing national cybersecurity measures.*** **[Am. 19]**

(15) The Competence Centre should have several key functions. First, the Competence Centre should facilitate and help coordinate the work of the ~~European Cybersecurity Competence~~ Network and nurture the Cybersecurity Competence Community. The Centre should drive the cybersecurity technological agenda and ***pool, share and*** facilitate access to the expertise gathered in the Network and the Cybersecurity Competence Community***, and to cybersecurity infrastructure***. Secondly, it should implement relevant parts of Digital Europe and Horizon Europe programmes by allocating grants, typically following a competitive call for proposals. Thirdly, the Competence Centre should facilitate joint investment by the Union, Member States and/or industry ***as well as joint training opportunities and awareness raising programmes in line with the Digital Europe Programme for citizens and businesses to overcome the skill gap***. ***It should pay special attention to the enabling of SMEs in the area of cybersecurity.*** **[Am. 20]**

(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, ***including those working on cybersecurity ethics,*** supply-side industries, ~~demand side~~ ***demand-side*** industries ***including SMEs***, and the public sector. The Cybersecurity Competence Community should provide input to the activities and work plan of the Competence Centre and it should also benefit from the community-building activities of the Competence Centre and the Network, but otherwise should not be privileged with regard to calls for proposals or calls for tender. **[Am. 21]**

(16a) The Competence Centre should provide the appropriate support to the European Network and Information Security Agency (ENISA) in its tasks defined by Directive (EU) 2016/1148 ("NIS Directive") and Regulation (EU) 2019/XXX of the European Parliament and of the Council[8]("Cybersecurity Act"). Therefore, ENISA should provide relevant inputs to the Competence Centre in its task of defining funding priorities. **[Am. 22]**

---

8 ***Regulation (EU) 2019/… of the European Parliament and of the Council of … on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L ...) (2017/0225(COD)).***

(17) In order to respond to the needs of ***the public sector and*** both demand and supply side industries, the Competence Centre's task to provide cybersecurity knowledge and technical assistance to ***the public sector and*** 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. ***In particular, the Competence Centre should facilitate the deployment of dynamic enterprise-level solutions focused on building capabilities of entire organisations, including people, processes and technology, in order to effectively protect the organizations against constantly changing cyber threats.*** **[Am. 23]**

(17a) The Competence Centre should contribute to the wide deployment of state-of-the-art cybersecurity products and solutions, in particular those that are internationally recognised. **[Am. 24]**

(18) Whereas the Competence Centre and the Network should strive to achieve synergies ***and coordination*** between the cybersecurity civilian and defence spheres, projects financed by the Horizon Europe Programme will be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe shall have a focus on civil applications. **[Am. 25]**

(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 ***that should be harmonised at Union level***. **[Am. 26]**

(20) Appropriate provisions should be made to guarantee the liability and transparency of the Competence Centre ***and those undertakings receiving funding***. **[Am. 27]**

(20a) The implementation of deployment projects, in particular those relating to infrastructures and capabilities deployed at European level or in joint procurement, can 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 may only participate in one of the phases each and requiring that the beneficiaries in one or several of those phases meet certain conditions in terms of European ownership or control. **[Am. 28]**

(20b) With ENISA being the dedicated Union cybersecurity agency, the Competence Centre should seek the greatest possible synergies with it and the Governing Board should consult ENISA due to its experience in the field in all matters regarding cybersecurity, in particular on research-related projects. **[Am. 29]**

(20c) In the process of the nomination of the representative to the Governing Board, the European Parliament should include details of the mandate, including the obligation to report regularly to the European Parliament, or the committees responsible. **[Am. 30]**

(21) In view of their respective expertise in cybersecurity ***and in order to ensure greatest possible synergies***, the Joint Research Centre of the Commission as well as the European Network and Information Security Agency (ENISA) should play an active part in the Cybersecurity Competence Community and the Industrial and Scientific Advisory Board. ***ENISA should continue to fulfil its strategic objectives especially in the field of cybersecurity certification as defined in Regulation (EU) 2019/XXX [Cybersecurity Act][9] while the Competence Centre should act as an operational body in cybersecurity.*** **[Am. 31]**

---

9 ***Regulation (EU) 2019/… of the European Parliament and of the Council of … on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L ...) (2017/0225(COD)).***

(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.

(23) The Union contribution to the Competence Centre should finance half of the costs arising from the establishment, administrative and coordination activities of the Competence Centre, In order to avoid double funding, those activities should not benefit simultaneously from a contribution from other Union programmes.

(24) The Governing Board of the Competence Centre, composed of the Member States and the Commission, should define the general direction of the Competence Centre's operations, and ensure that it carries out its tasks in accordance with this Regulation. The Governing Board should be entrusted with the powers necessary to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Competence Centre, adopt the Competence Centre's work plan and multiannual strategic plan reflecting the priorities in achieving the objectives and tasks of the Competence Centre, adopt its rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof. ***In order to benefit from synergies, ENISA should be a permanent observer in the Governing Board and contribute the work of the Competence Centre, including by being consulted on the multi-annual strategic plan and on the work plan and on the list of actions selected for funding.*** **[Am. 32]**

(24a) ***The Governing Board should aim to promote the Competence Centre globally, so as to raise its attractiveness and make it a world-class body for excellence in cybersecurity.*** **[Am. 33]**

(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 ***and aim to achieve gender balance***. **[Am. 34]**

(25a) ***The weight of the Commission vote in the decisions of the Governing Board should be in line with the contribution of the Union budget to the Competence Centre, according to the Commission responsibility to ensure proper management of the Union budget in the Union interest, as set in the Treaties.*** **[Am. 35]**

(26) The smooth functioning of the Competence Centre requires that its Executive Director be appointed ~~on~~ ***in a transparent manner on the*** 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. **[Am. 36]**

(27) The Competence Centre should have an Industrial and Scientific Advisory Board as an advisory body to ensure regular ***and appropriately transparent*** dialogue with the private sector, consumers' organisations and other relevant stakeholders***. It should also provide the Executive Director and the Governing Board with independent advice on deployment and procurement***. The Industrial and Scientific Advisory Board should focus on issues relevant to stakeholders and bring them to the attention of the Competence Centre's Governing Board. The composition of the Industrial and Scientific Advisory Board and the tasks assigned to it, such as being consulted regarding the work plan, should ensure sufficient representation of stakeholders in the work of the Competence Centre. ***A minimum number of seats should be allocated to each category of industry stakeholders, with particular attention paid to the representation of SMEs.*** **[Am. 37]**

(28) The Competence Centre ***and its activities*** 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, ***and the pilot projects under Horizon2020 on the Cybersecurity Competence Network,*** through its Industrial and Scientific Advisory Board. ***The Competence Centre and Industrial and Scientific Advisory Board should, if appropriate, consider replications of existing structures, for example as working groups.*** **[Am. 38]**

(28a) The Competence Centre and its bodies should make use of the experience and contributions of past and current initiatives, such as the contractual public-private partnership (cPPP) on cybersecurity, the European Cyber Security Organisation (ECSO), and the pilot project and preparatory action on Free and Open Source Software Audits (EU FOSSA). **[Am. 39]**

(29) The Competence Centre should have in place rules regarding the prevention~~, and the management of conflict~~ ***identification and resolution of conflicts*** of interest ***in respect of its members, bodies and staff, the Governing Board, as well as the Scientific and Industrial Advisory Board, and the Community. Member States should ensure the prevention, identification, and resolution of conflicts of interest in respect of the National Coordination Centres***. 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[10]. Processing of personal data by the Competence Centre will be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council. The Competence Centre should comply with the provisions applicable to the Union institutions, and with national legislation regarding the handling of information, in particular sensitive non classified information and EU classified information. **[Am. 40]**

(30) The financial interests of the Union and of the Member States should be protected by proportionate measures throughout the expenditure cycle, including the prevention, detection and investigation of irregularities, the recovery of lost, wrongly paid or incorrectly used funds and, where appropriate, the application of administrative and financial penalties in accordance with Regulation XXX (EU, Euratom) of the European Parliament and of the Council[11] [the Financial Regulation].

---

10 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).

11 [add title and OJ reference]

(31) The Competence Centre should operate in an open and transparent way ***comprehensively*** providing ~~all relevant~~ information in a timely manner as well as promoting its activities, including information and dissemination activities to the wider public. ***It should provide the public and any interested parties with a list of the Cybersecurity Competence Community members and should make public the declarations of interest made by them in accordance with Article 42.*** The rules of procedure of the bodies of the Competence Centre should be made publicly available. **[Am. 41]**

(31a) It is advisable that both the Competence Centre and the National Coordination Centres monitor and follow the international standards as much as possible, in order to encourage development towards global best practices. **[Am. 42]**

(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.

(33a) The power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of defining the elements of contractual agreements between the Competence Centre and National Coordination Centres, and in respect of specifying criteria for assessing and accrediting entities as members of the Cybersecurity Competence Community. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[12]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. **[Am. 43]**

12 ***OJ L 123, 12.5.2013, p. 1.***

(34) ~~Since~~ The objectives of this Regulation, namely ***strengthening the Union's competitiveness and capacities in cybersecurity through, and reducing its digital dependence by increasing the uptake of cybersecurity products, processes and services developed within the Union,*** retaining and developing Union's cybersecurity technological and industrial capacities, increasing the competitiveness of the Union's cybersecurity industry and turning cybersecurity into a competitive advantage of other Union industries, cannot be sufficiently achieved by the Member States due the fact that existing, limited resources are dispersed as well as due to the scale of the investment necessary, but can rather by reason of avoiding unnecessary duplication of these efforts, helping to achieve critical mass of investment and ensuring that public financing is used in an optimal way be better achieved at Union level***. In addition, only actions at Union level can ensure the highest level of cybersecurity in all Member States and thus close security gaps existing in some Member States that create security gaps for the whole Union. 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. **[Am. 44]**

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")***. ***The Competence Centre and the Network shall contribute to the overall resilience and awareness in the Union towards cybersecurity threats, thoroughly taking into account societal implications.*** **[Am. 45]**

2. The Competence Centre shall contribute to the implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX[13] and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] thereof and of the Horizon Europe Programme established by Regulation No XXX[14] 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].

---

13 [add full title and OJ reference]

14 [add full title and OJ reference]

~~3. The seat of the Competence Centre shall be located in [Brussels, Belgium.]~~ **[Am. 46]**

~~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.~~ **[Am. 47]**

Article 2

Definitions

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

(1) 'cybersecurity' means ~~the protection of~~ ***all activities necessary to protect*** network and information systems, their users, and ~~other~~ ***affected*** persons ~~against~~ ***from*** cyber threats; **[Am. 48]**

(1a) 'cyber defence' and 'defence dimensions of cybersecurity' means exclusively defensive and reactive cyber defence technology which aims to protect critical infrastructures, military networks and information systems, their users, and affected persons, against cyber threats including situational awareness, threat detection and digital forensics; **[Am. 183]**

(2) '~~cybersecurity~~ products and ~~solutions~~ ***processes***' means ***commercial and non-commercial*** ICT products, services or ~~process~~ ***processes*** with the specific purpose of protecting ***data,*** network and information systems, their users and ~~affected~~ ***other*** persons from ~~cyber~~ ***cybersecurity*** threats; **[Am. 49]**

(2a) 'cyber threat' means any potential circumstance, event or action that may damage, disrupt or otherwise adversely impact network and information systems, their users and affected persons; **[Am. 50]**

(3) 'public authority' means any government or other public administration, including public advisory bodies, at national, regional or local level or any natural or legal person performing public administrative functions under ***Union and*** national law, including specific duties; **[Am. 51]**

(4) '~~participating~~ ***contributing*** Member State' means a Member State which voluntarily contributes financially to the administrative and operational costs of the Competence Centre***;*** **[Am. 52]**

(4a) 'European Digital Innovation Hubs' means a legal entity as defined in Regulation (EU) 2019/XXX of the European Parliament and of the Council[15]. **[Am. 53]**

---

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)).***

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 cybersecurity technological***,*** ~~and~~ industrial***, societal, academic and research expertise*** capacities ***and capabilities*** necessary to secure its Digital Single Market ***and further the protection of data of Union citizens, companies and public administrations***; **[Am. 54]**

(aa) increase the resilience and reliability of the infrastructure of network and information systems, including critical infrastructure, the internet and commonly used hardware and software in the Union; **[Am. 55]**

(b) increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into ***a*** competitive advantage of other Union industries***;*** **[Am. 56]**

(ba) raise the awareness for cybersecurity threats, and related societal and ethical implications and concerns and reduce the skills gap in cybersecurity in the Union; **[Am. 57]**

(bb) develop the Union's leadership in cybersecurity and ensure the highest cybersecurity standards throughout the Union; **[Am. 58]**

(bc) strengthen the Union's competitiveness and capacities while reducing its digital dependence by increasing the uptake of cybersecurity products, processes and services developed within the Union; **[Am. 59]**

(bd) reinforce the trust of citizens, consumers and businesses in the digital world, and therefore contribute to the goals of the Digital Single Market strategy. **[Am. 60]**

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

Article 4

Objectives and Tasks of the Centre

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

1. ***create, manage and*** 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; **[Am. 61]**

2. ~~contribute to~~ ***coordinate*** 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] ***and contribute to the implementation of the actions funded by the European Defence Fund established by Regulation (EU) 2019/XXX***; **[Am. 62]**

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

3. enhance cybersecurity ***resilience, capacities,*** capabilities, knowledge and infrastructures at the service of ***society,*** industries, the public sector and research communities, by carrying out the following tasks***, having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services***: **[Am. 63]**

   (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~~ ***the Competence Centre's facilities*** and related services ***in a fair, open and transparent way*** to a wide range of users across the Union from industry ~~including~~ ***in particular*** SMEs, the public sector and the research and scientific community; **[Am. 64]**

   (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~~ ***facilities*** and related services to a wide range of users across the Union from industry***,*** ~~including~~ ***in particular*** SMEs, the public sector and the research and scientific community; **[Am. 65]**

(ba) providing financial support and technical assistance to cybersecurity start-ups, SMEs, microenterprises, associations, individual experts and to civic tech projects; **[Am. 66]**

(bb) financing software security code audits and related improvements for Free and Open Source Software projects, commonly used for infrastructure, products and processes; **[Am. 67]**

(c) ~~providing~~ ***facilitating the sharing*** cybersecurity knowledge and technical assistance ***among others*** to ***civil society, the*** industry and public authorities***, and the academic and research community***, in particular by supporting actions aimed at facilitating access to the expertise available in the Network and the Cybersecurity Competence Community ***with the aim of improving cyber resilience within the Union***; **[Am. 68]**

(ca) promoting "security by design" as 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 including the commitment of producer or provider to make available updates remedying new vulnerabilities or threats, without delay, and beyond the estimated product lifetime, or enabling a third party to create and provide such updates; **[Am. 69]**

(cb) assisting source code contribution policies and their development, in particular for public authorities where Free and Open Source Software projects are used; **[Am. 70]**

(cc) bringing together stakeholders from industry, trade unions, academia, research organisations and public entities to ensure long-term cooperation on developing and implementing cybersecurity products and processes, including pooling and sharing of resources and information regarding such products and processes if appropriate; **[Am. 71]**

4. contribute to the wide deployment of state-of-the-art ***and sustainable*** cyber security products and ~~solutions~~ ***processes*** across the ~~economy~~ ***the Union***, by carrying out the following tasks: **[Am. 72]**

(a) stimulating cybersecurity research, development and the uptake of Union cybersecurity products and ~~solutions by~~ ***holistic processes throughout the entire innovation cycle, by, inter alia,*** public authorities***,*** ~~and user industries~~ ***the industry and the market***; **[Am. 73]**

(b) assisting public authorities, demand side industries and other users in ***increasing their resilience by*** adopting and integrating ~~the latest cyber security solutions~~ ***state-of-the-art cybersecurity products and processes***; **[Am. 74]**

(c) supporting in particular public authorities in organising their public procurement, or carrying out procurement of state-of-the-art cybersecurity products and ~~solutions~~ ***processes*** on behalf of public authorities***, including by providing support for procurement, to increase the security of and the benefits from public investment***; **[Am. 75]**

(d) providing financial support and technical assistance to cybersecurity start-ups and SMEs***,*** ~~to~~ ***micro-enterprises, individual experts, commonly used Free and Open Source Software projects, and civic tech projects, to enhance expertise on cybersecurity,*** connect to potential markets and ***deployment opportunities, and*** to attract investment; **[Am. 76]**

5. improve the understanding of cybersecurity and contribute to reducing skills gaps ***and strengthening the level of skills*** in the Union related to cybersecurity by carrying out the following tasks: **[Am. 77]**

(-a) 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; **[Am. 78]**

(a) supporting further development***, pooling, and sharing*** of cybersecurity skills ***and competences at all relevant educational levels, supporting the objective of achieving gender balance, facilitating a common high level of cybersecurity knowledge and contributing to the resilience of users and infrastructures throughout the Union in cooperation with the Network and***, where appropriate***,*** ~~together~~ ***aligning*** with relevant EU agencies and bodies including ENISA***;*** **[Am. 79]**

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~~ ***plan referred to in Article 13***; **[Am. 80]**

(b) ~~support~~ ***supporting*** large-scale research and demonstration projects in next generation cybersecurity technological capabilities, in collaboration with the industry***,*** ~~and~~ ***the academic and research community, public sector and authorities, including*** the Network ***and the Community***; **[Am. 81]**

(ba) ensuring respect for fundamental rights and ethical conduct in cybersecurity research projects supported by the Competence Centre; **[Am. 82]**

(bb) monitoring reports of vulnerabilities discovered by the Community and facilitating the disclosure of vulnerabilities, the development of patches, fixes and solutions, and the distribution of those; **[Am. 83]**

(bc) monitoring research results regarding self-learning algorithms used for malicious cyber activities in collaboration with ENISA and supporting the implementation of Directive (EU) 2016/1148; **[Am. 84]**

(bd) supporting research in the field of cybercrime; **[Am. 85]**

(be) supporting the research and development of products and processes that can be freely studied, shared, and built upon, in particular in the field of verified and verifiable hardware and software, in close cooperation with the industry, the Network and the Community; **[Am. 86]**

(c) support research and innovation for ***formal and non-formal*** standardisation ***and certification*** in cybersecurity technology***, linking to the existing work and where appropriate in close cooperation with the European Standardisation Organisations, certification bodies and ENISA;*** **[Am. 87]**

(ca) provide special support to SMEs by facilitating their access to knowledge and training through tailored access to the deliverables of research and development reinforced by the Competence Centre and the Network in order to increase competitiveness; **[Am. 88]**

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***, which shall be reactive and defensive cyber defence technology, applications and services***: **[Am. 184]**

(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***, which shall be reactive and defensive cyber defence technology, applications and services***: **[Am. 185]**

(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].

(ba) assisting and providing advice to the Commission with regard to the implementation of Regulation (EU) 2019/XXX [recast of Regulation (EC) No 428/2009 as proposed by COM(2016)0616]. **[Am. 89]**

8a. contribute to the Union's efforts to enhance international cooperation with regard to cybersecurity by:

(a) facilitating the participation of the Competence Centre in international conferences and governmental organisations as well as the contribution to international standardisation organisations;

(b) cooperating with third countries and international organisations within relevant international cooperation frameworks. **[Am. 90]**

Article 5

Investment in and use of infrastructures, capabilities, products or ~~solutions~~ ***processes*** **[Am. 91]**

1. Where the Competence Centre provides funding for infrastructures, capabilities, products or ~~solutions~~ ***processes*** pursuant to Article 4(3) and (4) in the form of a ***procurement,*** grant or a prize, the work plan of the Competence Centre may specify in particular: **[Am. 92]**

   (a) ***specific*** rules governing the operation of an infrastructure or capability, including where relevant entrusting the operation to a hosting entity based on criteria that the Competence Centre shall define; **[Am. 93]**

   (b) rules governing access to and use of an infrastructure or capability;

   (ba) specific rules governing different phases of implementation; **[Am. 94]**

   (bb) that as a result of Union contribution, access is as open as possible and as closed as necessary, and re-use is possible. **[Am. 95]**

2. The Competence Centre may be responsible for the overall execution of relevant joint procurement actions including pre-commercial procurements on behalf of members of the Network~~, members of the cybersecurity Competence Community, or other third parties representing the users of cybersecurity products and solutions~~. For this purpose, the Competence Centre may be assisted by one or more National Coordination Centres or members of the Cybersecurity Competence Community ***or relevant European Digital Innovation Hubs***. **[Am. 96]**

Article 6

Nomination of National Coordination Centres

-1. ***A single National Coordination Centre shall be set up in each Member State.*** **[Am. 97]**

1. By [date], each Member State shall nominate the entity to act as the National Coordination Centre for the purposes of this Regulation and notify it to the Commission.

2. On the basis of an assessment concerning the compliance of that entity with 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 entity as a National Coordination Centre or rejecting the nomination. The list of National Coordination Centres shall be published by the Commission.

3. Member States may at any time nominate a new entity as the National Coordination Centre for the purposes of this Regulation. Paragraphs 1 and 2 shall apply to nomination of any new entity.

4. The nominated National Coordination Centre shall have the capability to support the Competence Centre and the Network in fulfilling their mission laid out in Article 3 of this Regulation. They shall possess or have direct access to technological expertise in cybersecurity and be in a position to effectively engage and coordinate with industry, the public sector***,*** ~~and the~~ ***the academic and*** research community***, and citizens***. ***The Commission shall issue guidelines further detailing the assessment procedure and explaining the application of the criteria.*** **[Am. 98]**

5. The relationship between the Competence Centre and the National Coordination Centres shall be based on a ***standard*** contractual agreement signed between the Competence Centre and each of the National Coordination Centres. The agreement shall ~~provide for~~ ***consist of the same set of harmonised general conditions providing*** the rules governing the relationship and division of tasks between the Competence Centre and each National Coordination Centre ***and special conditions tailored to the particular National Coordination Centre***. **[Am. 99]**

5a. The Commission shall adopt delegated acts in accordance with Article 45a in order to supplement this Regulation by establishing the harmonised general conditions of the contractual agreements referred to in paragraph 5 of this Article, including their format. **[Am. 100]**

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 Competence Centre in achieving its objectives and in particular in ***establishing and*** coordinating the Cybersecurity Competence Community; **[Am. 101]**

(b) ***promoting, encouraging and*** facilitating the participation of ***civil society,*** industry***, in particular start-ups and SMEs, academic and research community*** and other actors at the Member State level in cross-border projects; **[Am. 102]**

(ba) in cooperation with other entities with similar tasks, operating as a one-stop-shop for cybersecurity products and processes financed through other Union programmes like InvestEU or the Single Market Programme, in particular for SMEs; **[Am. 103]**

(c) contributing, together with the Competence Centre, to identifying and addressing sector-specific cyber security ~~industrial~~ challenges; **[Am. 104]**

(ca) cooperating closely with National Standardisation Organisations to promote the uptake of existing standards and to involve all relevant stakeholders, particularly SMEs, in setting new standards; **[Am. 105]**

(d) acting as contact point at the national level for the Cybersecurity Competence Community and the Competence Centre;

(e) seeking to establish synergies with relevant activities at the national***,*** ~~and~~ regional ***and local*** level; **[Am. 106]**

(f) implementing specific actions for which grants have been awarded by the Competence Centre, including through provision of financial support to third parties in line with Article 204 of Regulation XXX [new Financial Regulation] under conditions specified in the concerned grant agreements;

(fa) promoting and disseminating a common minimal cybersecurity educational curricula in cooperation with the relevant bodies in the Member States; **[Am. 107]**

(g) promoting and disseminating the relevant outcomes of the work by the Network, the Cybersecurity Competence Community and the Competence Centre at national***,*** ~~or~~ regional ***or local*** level; **[Am. 108]**

(h) assessing requests by entities ***and individuals*** established in the same Member State as the Coordination Centre for becoming part of the Cybersecurity Competence Community. **[Am. 109]**

2. For the purposes of point (f), the financial support to third parties may be provided in any of the forms specified in Article 125 of Regulation XXX [new Financial Regulation] including in the form of lump sums.

3. National Coordination Centres may receive a grant from the Union in accordance with Article 195 (d) of Regulation XXX [new Financial Regulation] in relation to carrying out the tasks laid down in this Article.

4. National Coordination Centres shall, where relevant, cooperate through the Network ***and with the relevant European Digital Innovation Hubs*** for the purpose of implementing tasks referred to in ~~points (a), (b), (c), (e) and (g) of~~ paragraph 1. **[Am. 110]**

Article 8

The Cybersecurity Competence Community

1. The Cybersecurity Competence Community ~~shall contribute~~ ***contributes*** to the mission of the Competence Centre as laid down in Article 3 and ~~enhance~~ and ***enhances, pools, shares,*** and disseminate cybersecurity expertise across the Union ***and provides technical expertise***. **[Am. 111]**

2. The Cybersecurity Competence Community shall consist of ***civil society,*** industry ***from the demand and supply-side, including SMEs***, academic and ~~non-profit~~ research ***community, associations of users, individual experts, relevant European Standardisation*** Organisations, and ***other*** associations as well as public entities and other entities dealing with operational and technical matters ***in the area of cybersecurity***. It shall bring together the main stakeholders with regard to cybersecurity technological***,*** ~~and~~ industrial***, academic and research, and societal*** capacities ***and capabilities*** in the Union~~. It~~ ***and*** shall involve National Coordination Centres***, European Digital Innovation Hubs*** as well as Union institutions and bodies with relevant expertise ***as referred to in Article 10 of this Regulation***. **[Am. 112]**

3. Only entities which are established ***and individuals resident*** within the Union***, the European Economic Area (EEA) or the European Free Trade Association (EFTA)*** may be accredited as members of the Cybersecurity Competence Community. ~~They~~ ***Applicants*** shall demonstrate that they ~~have~~ ***can provide*** cybersecurity expertise with regard to at least one of the following domains: **[Am. 113]**

(a) ***academia or*** research; **[Am. 114]**

(b) industrial development;

(c) training and education;

(ca) ethics; **[Am. 115]**

(cb) formal and technical standardisation and specifications. **[Am. 116]**

4. The Competence Centre shall accredit entities established under national law***, or individuals,*** as members of the Cybersecurity Competence Community after ~~an~~ ***a harmonised*** assessment made by ***the Competence Centre,*** the National Coordination Centre of the Member State where the entity is established***, or the individual is a resident***, on whether that entity meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it or the relevant National Coordination Centre considers that the entity ***or individual*** does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation]. ***The National Coordination Centres of the Member States shall aim to achieve a balanced representation of stakeholders in the Community, actively stimulating participation from under-represented categories, especially SMEs, and groups of individuals***. **[Am. 117]**

4a. The Commission shall adopt delegated acts in accordance with Article 45a in order to supplement this Regulation by detailing the criteria provided for in paragraph 3 of this Article according to which applicants are selected, and the procedures for assessing and accrediting entities that meet the criteria referred to in paragraph 4 of this Article. **[Am. 118]**

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

6. The representatives of the Commission may participate in the work of the Community.

Article 9

Tasks of the members of the Cybersecurity Competence Community

The members of the Cybersecurity Competence Community shall:

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

(2) participate in activities promoted by the Competence Centre and National Coordination Centres;

(3) where relevant, participate in working groups established by the Governing Board of the Competence Centre to carry out specific activities as provided by the Competence Centre's work plan;

(4) where relevant, support the Competence Centre and the National Coordination Centres in promoting specific projects;

(5) promote and disseminate the relevant outcomes of the activities and projects carried out within the community;

(5a) support the Competence Centre by reporting and disclosing vulnerabilities, helping to mitigate them and providing advice on how to reduce such vulnerabilities including through certification under the schemes adopted in conformity with Regulation (EU) 2019/XXX [the Cybersecurity Act]. **[Am. 119]**

Article 10

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

1. ***To ensure coherence and complementarity,*** the Competence 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, Innovation and Networks Executive Agency, ***relevant European Digital Innovation Hubs,*** European Cybercrime Centre at Europol as well as the European Defence Agency ***as regards dual-use projects, services and competences***. **[Am. 120]**

2. Such cooperation shall take place within the framework of working arrangements. Those arrangements shall be ~~submitted to the~~ ***adopted by the Governing Board after*** prior approval of the Commission. **[Am. 121]**

CHAPTER II

ORGANISATION OF THE COMPETENCE CENTRE

Article 11

Membership and structure

1. The members of the Competence Centre shall be the Union, represented by the Commission, and the Member States.

2. The structure of the Competence Centre shall comprise:

   (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;

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

SECTION I

GOVERNING BOARD

Article 12

Composition of the Governing Board

1. The Governing Board shall be composed of one representative of each Member State, ~~and~~ ~~five~~ ***one representative nominated by the European Parliament as an observer, and four*** representatives of the Commission, on behalf of the Union***, aiming to achieve gender balance among board members and their alternates***. **[Am. 122]**

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

3. Members of the Governing Board and their alternates shall be appointed in light of their knowledge in the field of ~~technology~~ ***cybersecurity*** as well as of relevant managerial, administrative and budgetary skills. The Commission and the Member States shall make efforts to limit the turnover of their representatives in the Governing Board, in order to ensure continuity of the Board's work. The Commission and the Member States shall aim to achieve a balanced representation between men and women on the Governing Board. **[Am. 123]**

4. The term of office of members of the Governing Board and of their alternates shall be four years. That term shall be renewable.

5. The Governing Board members shall act in the interest of the Competence Centre, safeguarding its goals and mission, identity, autonomy and coherence, in an independent and transparent way.

6. The ~~Commission~~ ***Governing Board*** 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. **[Am. 124]**

7. ~~The European Agency for Network and Information Security (~~ENISA***,*** ~~)~~ ***and the Industrial and Scientific Advisory Board,*** shall be ~~a~~ permanent ~~observer~~ ***observers*** in the Governing Board***, in an advisory role without voting rights***. ***The Governing Board shall have the utmost regard to the views expressed by the permanent observers.*** **[Am. 125]**

Article 13

Tasks of the Governing Board

1. The Governing Board shall have the overall responsibility for the strategic orientation and the operations of the Competence Centre and shall supervise the implementation of its activities.

2. The Governing Board shall adopt its rules of procedure. These rules shall include specific procedures for identifying and avoiding conflicts of interest and ensure the confidentiality of any sensitive information.

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

   (a) adopt a multi-annual strategic plan, containing a statement of the major priorities and planned initiatives of the Competence Centre, including an estimate of financing needs and sources***, taking into account advice provided by ENISA***; **[Am. 126]**

   (b) adopt the Competence Centre's work plan, annual accounts and balance sheet and annual activity report, on the basis of a proposal from the Executive Director***, taking into account advice provided by ENISA***; **[Am. 127]**

   (c) adopt the specific financial rules of the Competence Centre in accordance with [Article 70 of the FR];

(d) adopt a procedure for appointing the Executive Director;

(e) adopt the ~~criteria and~~ procedures for assessing and accrediting the entities as members of the ~~Cybersecurity Competence~~ Community; **[Am. 128]**

(ea) adopt the working arrangements referred to in Article 10(2); **[Am. 129]**

(f) appoint, dismiss, extend the term of office of, provide guidance to and monitor the performance of the Executive Director, and appoint the Accounting Officer;

(g) adopt the annual budget of the Competence Centre, including the corresponding staff establishment plan indicating the number of temporary posts by function group and by grade, the number of contract staff and seconded national experts expressed in full-time equivalents;

(ga) adopt transparency rules for the Competence Centre; **[Am. 130]**

(h) adopt rules regarding conflicts of interest;

(i) establish working groups with members of the ~~Cybersecurity Competence~~ Community***, taking into account advice provided by the permanent observers***; **[Am. 131]**

(j) appoint members of the Industrial and Scientific Advisory Board;

(k) set up an Internal Auditing Function in accordance with Commission Delegated Regulation (EU) No 1271/2013[18];

(l) promote ***the cooperation of*** the Competence Centre ~~globally, so as to raise its attractiveness and make it a world-class body for excellence in cybersecurity~~ ***with global actors***; **[Am. 132]**

(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);

[18] 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).

(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 having regard to a cost-benefit analysis of the measures to be implemented***, as well as adopt comprehensive protection measures for persons reporting on breaches of Union law in accordance with applicable Union legislation***; **[Am. 133]**

(s) adopt ~~the~~ ***an extensive definition of financial contributions from Member States and a*** methodology to calculate the ~~financial contribution from~~ ***amount of*** Member States***' voluntary contributions that can be accounted for as financial contributions in accordance with that definition, such a calculation being executed at the end of every financial year***; **[Am. 134]**

(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;

Article 14

Chairperson and Meetings of the Governing Board

1. The Governing Board shall elect a Chairperson and a Deputy Chairperson from among the members with voting rights, for a period of two years***, aiming to achieve gender balance***. 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. **[Am. 135]**

2. The Governing Board shall hold its ordinary meetings at least three times a year. It may hold extraordinary meetings at the request of the Commission, at the request of one third of all its members, at the request of the chair, or at the request of the Executive Director in the fulfilment of his/her tasks.

3. The Executive Director shall take part in the deliberations, unless decided otherwise by the Governing Board, but shall have no voting rights. ~~The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers.~~ **[Am. 136]**

~~4. Members of the Industrial and Scientific Advisory Board may take part, upon invitation from the Chairperson, in the meetings of the Governing Board, without voting rights.~~ **[Am. 137]**

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. The Union shall hold 50 % of the voting rights. The voting rights of the Union shall be indivisible.~~

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

~~3. The Governing Board shall take its decisions by a majority of at least 75% of all votes, including the votes of the members who are absent, representing at least 75% of the total financial contributions to the Competence Centre. The financial contribution will be calculated based on the estimated expenditures proposed by the Member States referred to in point c of Article 17(2) and based on the report on the value of the contributions of the participating Member States referred to in Article 22(5).~~

~~4. Only the representatives of the Commission and the representatives of the participating Member States shall hold voting rights.~~

~~5. The Chairperson shall take part in the voting.~~ **[Am. 138]**

Article 15a

Voting rules of the Governing Board

1. Decisions subject to vote may concern:

(a) governance and organisation of the Competence Centre and the Network;

(b) allocation of budget for the Competence Centre and the Network;

(c) joint actions by several Member States, possibly complemented by Union budget further to decision allocated in accordance with point (b).

2. The Governing Board shall adopt its decisions on the basis of at least 75 % of the votes of all members. The voting rights of the Union shall be represented by the Commission and shall be indivisible.

3. For decisions under point (a) of paragraph 1, each Member States shall be represented and have the same equal rights of vote. For the remaining votes available up to 100 %, the Union should have at least 50 % of the voting rights corresponding to its financial contribution.

4. For decisions falling under point (b) or (c) of paragraph 1, or any other decision not falling under any other category of paragraph 1, the Union shall hold at least 50 % of the voting rights corresponding to its financial contribution. Only contributing Member States shall have voting rights and they will correspond to its financial contribution.

5. If the Chairperson has been elected from among the representatives of the Member States, the Chairperson shall take part in the voting as a representative of his or her Member State. **[Am. 139]**

SECTION II

EXECUTIVE DIRECTOR

Article 16

Appointment, dismissal or 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, ***including nominations aiming to achieve gender balance from the Member States,*** following an open***,*** ~~and~~ transparent ***and non-discriminatory*** selection procedure. **[Am. 140]**

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~~ ***five*** 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. **[Am. 141]**

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~~ ***five*** years. **[Am. 142]**

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 ***proposal from its members or on*** a proposal from the Commission. **[Am. 143]**

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 its work, provide the secretariat for their meetings and supply all information necessary for the performance of their duties;

   (c) after consultation with the Governing Board***, the Industrial and Scientific Advisory Board, ENISA,*** and the Commission, prepare and submit for adoption to the Governing Board the draft multiannual strategic plan and the draft annual work plan of the Competence Centre including the scope of the calls for proposals, calls for expressions of interest and calls for tenders needed to implement the work plan and the corresponding expenditure estimates as proposed by the Member States and the Commission; **[Am. 144]**

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

(e) implement the work plan and report to the Governing Board thereon;

(f) prepare the draft annual activity report on the Competence Centre, including the information on corresponding expenditure;

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

(h) prepare an action plan following-up on the conclusions of the retrospective evaluations and reporting on progress every two years to the Commission ***and the European Parliament;*** **[Am. 145]**

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

(j) be responsible for administrative, financial and staff matters, including the implementation of the Competence Centre budget, taking due account of advice received from the Internal Auditing Function, within the limits of the delegation by the Governing Board;

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

(l) ***after consulting the Industrial and Scientific Advisory Board and ENISA,*** approve the list of actions selected for funding on the basis of the ranking list established by a panel of independent experts; **[Am. 146]**

(m) approve and manage the launch of calls for tenders, in accordance with the work plan and administer the contracts;

(n) approve the tenders selected for funding;

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

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

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

(r) sign procurement contracts;

(s) prepare an action plan following-up conclusions of internal or external audit reports, as well as investigations by the European Anti-Fraud Office (OLAF) and reporting on progress twice a year to the Commission and ***the European Parliament and*** regularly to the Governing Board; **[Am. 147]**

(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 request, to the European Parliament and to the Council***; **[Am. 148]**

(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.

SECTION III

INDUSTRIAL AND SCIENTIFIC ADVISORY BOARD

Article 18

Composition of the Industrial and Scientific Advisory Board

1. The Industrial and Scientific Advisory Board shall consist of no more than ~~16~~ ***25*** members. The members shall be appointed by the Governing Board from among the representatives of the entities of the ~~Cybersecurity Competence~~ Community***, or its individual members. Only representatives of entities which are not controlled by a third country or a third-country entitiy except from EEA and EFTA countries shall be eligible. The appointment shall be made in accordance with an open, transparent and non-discriminatory procedure. The Board composition shall aim to achieve gender balance, and include a balanced representation of the stakeholder groups from industry, academic community and civil society.*** **[Am. 149]**

2. Members of the Industrial and Scientific Advisory Board shall have expertise either with regard to cybersecurity research, industrial development, ***offering, implementing, or deploying*** professional services or ~~the deployment thereof~~ ***products***. The requirements for such expertise shall be further specified by the Governing Board. **[Am. 150]**

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

4. The term of office of members of the Industrial and Scientific Advisory Board shall be three years. That term shall be renewable.

5. Representatives of the Commission and of the ~~European Network and Information Security Agency may~~ ***ENISA shall be invited to*** participate in and support the works of the Industrial and Scientific Advisory Board. ***The Board may invite additional representatives from the Community in an observer, adviser, or expert capacity as appropriate, on a case-by-case basis.*** **[Am. 151]**

Article 19

Functioning of the Industrial and Scientific Advisory Board

1. The Industrial and Scientific Advisory Board shall meet at least ~~twice~~ ***three times*** a year. **[Am. 152]**

2. The Industrial and Scientific Advisory Board ~~may advise~~ ***shall provide suggestions to*** the Governing Board on the establishment of working groups 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 Advisory Board. **[Am. 153]**

3. The Industrial and Scientific Advisory Board shall elect its chair.

4. The Industrial and Scientific Advisory Board shall adopt its rules of procedure, including the nomination of the representatives that shall represent the Advisory Board where relevant and the duration of their nomination.

Article 20

Tasks of the Industrial and Scientific Advisory Board

The Industrial and Scientific Advisory Board shall ***regularly*** advise the Competence Centre in respect of the performance of its activities and shall: **[Am. 154]**

(1) provide to the Executive Director and the Governing Board strategic advice and input for ***deployment by, orientation and operations of the Competence Centre as far as industry and research is concerned, and*** drafting the work plan and multi-annual strategic plan within the deadlines set by the Governing Board; **[Am. 155]**

(1a) advise the Governing Board on the establishment of working groups on specific issues relevant to the work of the Competence Centre; **[Am. 156]**

(2) organise public consultations open to all public and private stakeholders having an interest in the field of cybersecurity, in order to collect input for the strategic advice referred to in paragraph 1;

(3) promote and collect feedback on the work plan and multi-annual strategic plan of the Competence Centre ***and advise the Governing Board on how to improve the Competence Centre's strategic orientation and operation***. **[Am. 157]**

CHAPTER III

FINANCIAL PROVISIONS

Article 21

Union financial contribution

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

(a) ~~EUR 1 981 668 000~~ ***EUR 1 780 954 875 in 2018 prices (EUR 1 998 696 000 in current prices)*** from the Digital Europe Programme, including up to ***EUR 21 385 465 in 2018 prices (***EUR 23 746 000 ***in current prices)*** for administrative costs; **[Am. 158]**

(b) An amount from the Horizon Europe Programme, including for administrative costs, to be determined taking into account the strategic planning process to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation];

(ba) an amount from the European Defence Fund for defence-related actions of the Competence Centre, including for all related administrative costs such as costs that the Competence Centre may incur when acting as a project manager for actions carried out under the European Defence Fund. **[Am. 159]**

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***, to the European Defence Fund and to other programmes and projects falling within the scope of the Competence Centre or the Network***. **[Am. 160]**

3. The Competence Centre shall implement cybersecurity actions of [Digital Europe Programme] and [Horizon Europe Programme] in accordance with point (c) (iv) of Article 62 of Regulation (EU, Euratom) XXX[19] [the financial regulation].

4. The Union financial contribution ***from Digital Europe Programme and from Horizon Europe Programme*** shall not cover the tasks referred to in Article 4(8)(b)***. These may be covered by financial contributions from the European Defence Fund.*** **[Am. 161]**

---

19 [add full title and OJ reference]

Article 22

Contributions of participating Member States

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

2. For the purpose of assessing the contributions referred to in paragraph 1 and in point (b)ii of Article 23(3), the costs shall be determined in accordance with the usual cost accounting practices of the Member States concerned, the applicable accounting standards of the Member State, and the applicable International Accounting Standards and International Financial Reporting Standards. The costs shall be certified by an independent external auditor appointed by the Member State concerned. The valuation method may be verified by the Competence Centre should there be any uncertainty arising from the certification.

3. Should any participating Member State be in default of its commitments concerning its financial contribution, the Executive Director shall put this in writing and shall set a reasonable period within which such default shall be remedied. If the situation is not remedied within that period, the Executive Director shall convene a meeting of the Governing Board to decide whether the defaulting participating Member State’s right to vote is to be revoked or whether any other measures are to be taken until its obligations have been met. The defaulting Member State's voting rights shall be suspended until the default of its commitments is remedied.

4. The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to the Competence Centre if the participating Member States do not contribute, ***or*** contribute only partially ~~or contribute late~~ with regard to the contributions referred to in 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.*** **[Am. 162]**

5. The participating Member States shall report by 31 January each year to the Governing Board on the value of the contributions referred to in paragraphs 1 made in each of the previous financial year.

Article 23

Costs and resources of the Competence Centre

1. The Competence Centre shall be jointly funded by the Union and Member States through financial contributions paid in instalments and contributions consisting of costs incurred by National Coordination Centres and beneficiaries in implementing actions that are not reimbursed by the Competence Centre.

2. The administrative costs of the Competence Centre shall not exceed EUR [number] and shall be covered by means of financial contributions divided equally on an annual basis between the Union and the participating Member States. If part of the contribution for administrative costs is not used, it may be made available to cover the operational costs of the Competence Centre.

3. The operational costs of the Competence Centre shall be covered by means of:

   (a) the Union's financial contribution;

   (b) contributions from the participating Member States in the form of:

      (i) Financial contributions; and

      (ii) where relevant, in-kind contributions by the participating Member States of the costs incurred by National Coordination Centres and beneficiaries in implementing indirect actions less the contribution of the Competence Centre and any other Union contribution to those costs;

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

(a) ***the Union's and*** participating Member States' financial contributions to the administrative costs; **[Am. 163]**

(b) ***the Union's and*** participating Member States' financial contributions to the operational costs; **[Am. 164]**

(c) any revenue generated by Competence Centre;

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

5. Any interest yielded by the contributions paid to the Competence Centre by the participating Member States shall be considered to be its revenue.

6. All resources of the Competence Centre and its activities shall be aimed to achieve to the objectives set out in Article 4.

7. The Competence Centre shall own all assets generated by it or transferred to it for the fulfilment of its objectives.

8. Except when the Competence Centre is wound up, any excess revenue over expenditure shall not be paid to the participating members of the Competence Centre.

8a. ***The Competence Centre shall cooperate closely with other Union institutions, agencies, and bodies in order to benefit from synergies and, where appropriate, to reduce administrative costs.*** **[Am. 165]**

Article 24

Financial commitments

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

Article 25

Financial year

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

Article 26

Establishment of the budget

1. Each year, the Executive Director shall draw up a draft statement of estimates of the Competence Centre's revenue and expenditure for the following financial year, and shall forward it to the Governing Board, together with a draft establishment plan. Revenue and expenditure shall be in balance. The expenditure of the Competence Centre shall include the staff, administrative, infrastructure and operational expenses. Administrative expenses shall be kept to a minimum.

2. Each year, the Governing Board shall, on the basis of the draft statement of estimates of revenue and expenditure referred to in paragraph 1, produce a statement of estimates of revenue and expenditure for the Competence Centre for the following financial year.

3. The Governing Board shall, by 31 January each year, send the statement of estimates referred to in paragraph 2, which shall be part of the draft single programming document, to the Commission.

4. On the basis of that statement of estimates, the Commission shall enter in the draft budget of the Union the estimates it deems necessary for the establishment plan and the amount of the contribution to be charged to the general budget, which it shall submit to the European Parliament and the Council in accordance with Article 313 and 314 TFEU.

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

6. The European Parliament and the Council shall adopt the establishment plan for the Competence Centre.

7. Together with the Work Plan, the Governing Board shall adopt the Centre's budget. It shall become final following definitive adoption of the general budget of the Union. Where appropriate, the Governing Board shall adjust the Competence Centre's budget and Work Plan in accordance with the general budget of the Union.

Article 27

Presentation of the Competence Centre's accounts and discharge

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

Article 28

Operational and financial reporting

1. The Executive Director shall report annually to the Governing Board on the performance of his/her duties in accordance with the financial rules of the Competence Centre.

2. Within two months of the closure of each financial year, the Executive Director shall submit to the Governing Board for approval an annual activity report on the progress made by the Competence Centre in the previous calendar year, in particular in relation to the work plan for that year. That report shall include, inter alia, information on the following matters:

   (a) operational actions carried out and the corresponding expenditure;

   (b) the actions submitted, including a breakdown by participant type, including SMEs, and by Member State;

   (c) the actions selected for funding, including a breakdown by participant type, including SMEs, and by Member State and indicating the contribution of the Competence Centre to the individual participants and actions;

   (d) progress towards the achievement of the objectives set out in Article 4 and proposals for further necessary work to achieve these objectives.

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

Article 29

Financial rules

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

Article 30

Protection of financial interests

1. The Competence Centre shall take appropriate measures to ensure that, when actions financed under this Regulation are implemented, the financial interests of the Union are protected by the application of preventive measures against fraud, corruption and any other illegal activities, by ***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. **[Am. 166]**

2. The Competence Centre shall grant Commission staff and other persons authorised by the Commission, as well as the Court of Auditors, access to its sites and premises and to all the information, including information in electronic format that is needed in order to conduct their audits.

3. The European Anti-Fraud Office (OLAF) may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Council Regulation (Euratom, EC) No 2185/96[20] and Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council[21] 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.

---

20 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).

21 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[22] ('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').

---

22 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).

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

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

5. The Governing Board shall adopt implementing rules as regards the Staff Regulations and the Conditions of Employment in accordance with Article 110 of the Staff Regulations.

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

7. ~~The staff of~~ The Competence Centre ***shall aim to achieve gender balance among its staff. The staff*** shall consist of temporary staff and contract staff. **[Am. 167]**

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) Regulation (EU) No XXX [Digital Europe Programme] shall apply to participation in all actions funded by the Competence Centre.

2. The following specific security rules shall apply to actions funded from Horizon Europe:

   (a) for the purposes of Article 34(1) [Ownership and protection] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan, the grant of non-exclusive licenses may be limited to third parties established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States;

   (b) for the purposes of Article 36(4)(b) [Transfer and licensing] of Regulation (EU) No XXX [Horizon Europe], the transfer or license to a legal entity established in an associated country or established in the Union but controlled from third countries shall also be a ground to object to transfers of ownership of results, or to grants of an exclusive license regarding results;

(c) for the purposes of Article 37(3)(a) [Access rights] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan, granting of access to results and background may be limited only to a legal entity established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States;

(ca) Articles 22 [Ownership of results], 23 [Ownership of results] and 30 [Application of the rules on classified information] of Regulation (EU) 2019/XXX [European Defence Fund] shall apply to participation in all defence-related actions by the Competence Centre, when provided for in the work plan, and 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. **[Am. 168]**

Article 35

Transparency

1. The Competence Centre shall carry out its activities with ~~a high~~ ***the highest*** level of transparency. **[Am. 169]**

2. The Competence Centre shall ensure that the public and any interested parties are ~~given~~ ***provided with comprehensive,*** appropriate, objective, reliable and easily accessible information ***in due time***, in particular with regard to the results of ~~its work~~ ***the work of the Competence Centre, the Network, the Industry and Scientific Advisory Board and the Community***. It shall also make public the declarations of interest made in accordance with Article ~~41~~ ***42***. **[Am. 170]**

3. The Governing Board, acting on a proposal from the Executive Director, may authorise interested parties to observe the proceedings of some of the Competence Centre's activities.

4. The Competence Centre shall lay down, in its rules of procedure, the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2. For actions funded from Horizon Europe this will take due account of the provisions in Annex III of the Horizon Europe Regulation.

Article 36

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

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

2. Members of the Governing Board, the Executive Director, the members of the Industrial and Scientific Advisory Board, external experts participating in ad hoc Working Groups, and members of the staff of the Centre shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union, even after their duties have ceased.

3. The Governing Board of the Competence Centre shall adopt the Competence Centre's security rules, following approval by the Commission, based on the principles and rules laid down in the Commission's security rules for protecting European Union classified information (EUCI) and sensitive non-classified information including inter alia provisions for the processing and storage of such information as set out in Commission Decisions (EU, Euratom) 2015/443[23] and 2015/444[24].

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.

---

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

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

Article 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 timely manner and proportionate reporting requirements shall be imposed on recipients of Union funds and Member States. The outcomes of the evaluation shall be made public.

2. Once there is sufficient information available about the implementation of this Regulation, but no later than three and a half years after the start of the implementation of this Regulation, the Commission shall carry out an interim evaluation of the Competence Centre. The Commission shall prepare a report on that evaluation and shall submit that report to the European Parliament and to the Council by 31 December 2024. The Competence Centre and Member States shall provide the Commission with the information necessary for the preparation of that report.

3. The evaluation referred to in paragraph 2 shall include an assessment of the results achieved by the Competence Centre, having regard to its objectives, mandate and tasks**,** ***effectiveness, and efficiency***. If the Commission considers that the continuation of the Competence Centre is justified with regard to its assigned objectives, mandate and tasks, it may propose that the duration of the mandate of the Competence Centre set out in Article 46 be extended. **[Am. 171]**

4. On the basis of the conclusions of the interim evaluation referred to in paragraph 2 the Commission may act in accordance with [Article 22(5)] or take any other appropriate actions.

5. The monitoring, evaluation, phasing out and renewal of the contribution from Horizon Europe will follow the provisions of articles 8, 45 and 47 and Annex III of the Horizon Europe Regulation and agreed implementation modalities.

6. The monitoring, reporting and evaluation of the contribution from Digital Europe will follow the provisions of articles 24, 25 of the Digital Europe programme.

7. In case of a winding up of the Competence Centre, the Commission shall conduct a final evaluation of the Competence Centre within six months after the winding-up of the Competence Centre, but no later than two years after the triggering of the winding-up procedure referred to in Article 46 of this Regulation. The results of that final evaluation shall be presented to the European Parliament and to the Council.

Article 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. **[Am. 172]**

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***,*** ~~and management~~ ***identification, and resolution*** of conflicts of interest in respect of its members, bodies and staff***,*** ~~.~~ ~~Those rules shall contain the provisions intended to avoid a conflict of interest in respect of the representatives of the members serving in~~ ***including the Executive Director,*** the Governing Board***,*** as well as the Scientific and Industrial Advisory Board***,*** ~~in accordance with Regulation XXX [new Financial Regulation]~~ ***and the Community***. **[Am. 173]**

Member States shall ensure the prevention, identification, and resolution of conflicts of interest in respect of the National Coordination Centres. **[Am. 174]**

The rules referred to in the first paragraph shall comply with Regulation (EU, Euratom) 2018/1046. **[Am. 175]**

Article 43

Protection of Personal Data

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

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

Article 44

Seat and support from the host Member State **[Am. 176]**

The seat of the Competence Centre shall be determined in a democratically accountable procedure, using transparent criteria and in accordance with Union law. **[Am. 177]**

The host Member State shall provide the best possible conditions to ensure the proper functioning of the Competence Centre, including a single location, and further conditions such as the accessibility of the adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and partners. **[Am. 178]**

An administrative agreement ~~may~~ ***shall*** 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. **[Am. 179]**

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, until the Executive Director takes up his duties following his/her appointment by the Governing Board in accordance with Article 16, the Commission may designate an interim Executive Director and exercise the duties assigned to the Executive Director who may be assisted by a limited number of Commission officials. The Commission may assign a limited number of its officials on an interim basis.

3. The interim Executive Director may authorise all payments covered by the appropriations provided in the annual budget of the Competence Centre once approved by the Governing Board and may conclude agreements, decisions and contracts, including staff contracts following the adoption of the Competence Centre's staff establishment plan.

4. The interim Executive Director shall determine, in common accord with the Executive Director of the Competence Centre and subject to the approval of the Governing Board, the date on which the Competence Centre will have the capacity to implement its own budget. From that date onwards, the Commission shall abstain from making commitments and executing payments for the activities of the Competence Centre.

Article 45a

Exercise of the delegation

1. *The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.*

2. *The power to adopt delegated acts referred to in Article 6(5a) and Article 8(4b) shall be conferred on the Commission for an indeterminate period of time from ... [date of entry into force of this Regulation].*

3. *The delegation of power referred to in Article 6(5a) and Article 8(4b) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.*

4. *Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.*

5. ***As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.***

6. ***A delegated act adopted pursuant to Article 6(5a) and Article 8(4b) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.*** **[Am. 180]**

Article 46

Duration

1. The Competence Centre shall be established for the period from 1 January 2021 to 31 December 2029.

2. At the end of this period, unless decided otherwise through a review of this Regulation, the winding-up procedure shall be triggered. The winding-up procedure shall be automatically triggered if the Union or all participating Member States withdraw from the Competence Centre.

3. For the purpose of conducting the proceedings to wind up the Competence Centre, the Governing Board shall appoint one or more liquidators, who shall comply with the decisions of the Governing Board.

4. When the Competence Centre is being wound up, its assets shall be used to cover its liabilities and the expenditure relating to its winding-up. Any surplus shall be distributed among the Union and the participating Member 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 …,

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