I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2021/887 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 20 May 2021

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,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee [1],

Acting in accordance with the ordinary legislative procedure [2],

Whereas:

(1) The majority of the population of the Union is connected to the internet. The daily lives of people and economies are becoming increasingly dependent on digital technologies. Citizens and businesses are becoming increasingly exposed to serious cybersecurity incidents and many businesses in the Union experience at least one cybersecurity incident every year. This highlights the need for resilience, for enhancing technological and industrial capabilities and for the use of high cybersecurity standards and holistic cybersecurity solutions which involve people, products, processes and technology in the Union, as well as the need for Union leadership in the areas of cybersecurity and digital autonomy. Cybersecurity can also be improved by raising the awareness of cybersecurity threats and by developing competencies, capacities and capabilities throughout the Union, while thoroughly taking into account societal and ethical implications and concerns.

(2) The Union has steadily increased its activities to address growing cybersecurity challenges following the cybersecurity strategy put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative) in their Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 7 February 2013 entitled 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' (the '2013 Cybersecurity Strategy'). The 2013 Cybersecurity Strategy aimed to foster a reliable, safe, and open cyber ecosystem. In 2016, the Union adopted the first measures in the area of cybersecurity with Directive (EU) 2016/1148 of the European Parliament and of the Council [3] on security of network and information systems.

[1] OJ C 159, 10.5.2019, p. 63.
[2] Position of the European Parliament of 17 April 2019 (not yet published in the Official Journal) and position of the Council at first reading of 20 April 2021 (not yet published in the Official Journal). Position of the European Parliament of 19 May 2021 (not yet published in the Official Journal).
[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

(3) In September 2017, the Commission and the High Representative presented a Joint communication to the European Parliament and the Council entitled 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' to further reinforce the Union's resilience, deterrence and response to cyber-attacks.

(4) The Heads of State and Government at the Tallinn Digital Summit, in September 2017, called for the Union to become a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of citizens, consumers and enterprises online and to enable a free, safer and law-governed internet and declared their intention to make more use of open source solutions and open standards when (re)building Information and Communication Technology (ICT) systems and solutions, in particular avoiding vendor lock-ins, including those developed or promoted by Union programmes for interoperability and standardisation, such as ISA[2].

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

(6) The substantial disruption of network and information systems can affect individual Member States and the Union as a whole. A high level of security of network and information systems throughout the Union is therefore essential for society and the economy alike. At the moment, the Union depends on non-European cybersecurity providers. However, it is in the Union's strategic interest to ensure that it retains and develops essential cybersecurity research and technological capacities to secure the network and information systems of citizens and businesses, and in particular to protect critical network and information systems and provide key cybersecurity services.

(7) 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 the effective protection of networks and systems in that domain. Such efforts and expertise need to be pooled, networked and used in an efficient manner to reinforce and complement existing research, technology and industrial capacities and skills at Union and national level. Although the ICT sector faces important challenges, such as fulfilling its demand for skilled workers, it can benefit from representing the diversity of society at large, achieving a balanced representation of genders, ethnic diversity, and non-discrimination against persons with disabilities, as well as facilitating access to knowledge and training for future cybersecurity experts, including the education of such experts in non-formal contexts, for example in free and open source software projects, civic technology projects, start-ups and microenterprises.

(8) Small and medium-sized enterprises (SMEs) are crucial stakeholders in the Union's cybersecurity sector and can provide cutting-edge solutions due to their agility. However, SMEs that are not specialised in cybersecurity are also prone to be more vulnerable to cybersecurity incidents due to high investment and knowledge requirements for the establishment of effective cybersecurity solutions. It is therefore necessary that the Competence Centre and the Network of National Coordination Centres (the 'Network') provide support for SMEs by facilitating the access of SMEs to knowledge and tailoring access to the results of research and development, in order to allow SMEs to make themselves sufficiently secure and to allow SMEs that are active in cybersecurity to be competitive and contribute to the Union's leadership in the area of cybersecurity.

(9) Expertise exists outside 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.

(10) The area of cybersecurity is diverse. Relevant stakeholders include stakeholders from public entities, Member States and the Union, as well as from industry, civil society, such as trade unions, consumer associations, the free and open source software community and the academic and research community, and other entities.

(11) 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 and a European cybersecurity research and competence centre, and to propose by mid-2018 the relevant legal instrument for the creation of such a network and such a centre.

(12) The Union still lacks sufficient technological and industrial capacities and capabilities to autonomously make its economy and critical infrastructures secure and become a global leader in the area of cybersecurity. There is an insufficient level of strategic and sustainable coordination and cooperation between industries, cybersecurity research communities and governments. The Union suffers from insufficient investment and limited access to cybersecurity knowhow, skills and facilities, and few Union cybersecurity research and innovation outcomes are translated into marketable solutions or widely deployed across the economy.

(13) Establishing the Competence Centre and the Network, with a mandate to pursue measures in support of industrial technologies and in the domain of research and innovation, is the best way to fulfil the objectives of this Regulation while offering the highest economic, societal and environmental impact and safeguarding the Union's interests.

(14) 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 Network. The Competence Centre should manage cybersecurity-related financial support from Horizon Europe – the Framework Programme for Research and Innovation (Horizon Europe) established by Regulation (EU) 2021/695 of the European Parliament and of the Council ([4]) and the Digital Europe Programme established by Regulation (EU) 2021/694 of the European Parliament and of the Council ([5]) and should be open to other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to Union initiatives in the area of cybersecurity research and development, innovation, technology and industrial development and should avoid unnecessary duplication.

(15) It is important to ensure respect for fundamental rights and ethical conduct in cybersecurity research projects supported by the Competence Centre.

(16) The Competence Centre should not carry out operational cybersecurity tasks, such as tasks associated with Computer Security Incident Response Teams (CSIRTs), including the monitoring and handling of cybersecurity incidents. However, the Competence Centre should be able to facilitate the development of ICT infrastructures at the service of industries, in particular SMEs, research communities, civil society and the public sector, consistently with the mission and objectives laid down in this Regulation. Where CSIRTs and other stakeholders seek to promote the reporting and disclosing of vulnerabilities, the Competence Centre and members of the Cybersecurity Competence Community (the 'Community') should be able to support those stakeholders at their request within the limits of their respective tasks and while avoiding any duplication with the European Union Agency for Cybersecurity (ENISA) as established by Regulation (EU) 2019/881 of the European Parliament and of the Council ([6]).

(17) The Competence Centre, the Community and the Network are intended to benefit from the experience and the broad representation of relevant stakeholders built through the contractual public-private partnership on cybersecurity between the Commission and the European Cyber Security Organisation (ECSO) for the duration of Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) established by Regulation (EU) No 1291/2013 of the European Parliament and of the Council ([7]), from the lessons learnt from four pilot projects launched in early 2019 under Horizon 2020, namely CONCORDIA, ECHO, SPARTA and CyberSec4Europe, and from the pilot project and the preparatory action on Free and Open Source Software Audits (EU FOSSA), for the management of the Community and the representation of the Community in the Competence Centre.

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

([4]) Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (OJ L 170, 12.5.2021, p. 1).

([5]) Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1).

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

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

(19) In order to foster the Union's competitiveness and high cybersecurity standards internationally, the Competence Centre and the Community should seek the exchange of developments in cybersecurity, including in products and processes, in standards and in technical standards, with the international community, where relevant to the Competence Centre's mission, objectives and tasks. Relevant technical standards could include, for the purpose of this Regulation, the creation of reference implementations, including those published under open standard licences.

(20) The seat of the Competence Centre is in Bucharest.

(21) When preparing its annual work programme (annual work programme), the Competence Centre should inform the Commission of its co-funding needs on the basis of the Member States' planned co-funding contributions to joint actions, so that the Commission is able to take into account the matching Union contribution in the preparation of the draft general budget of the Union for the following year.

(22) Where the Commission prepares the work programme of Horizon Europe for matters related to cybersecurity, including in the context of its stakeholder consultation process, and especially before the adoption of that work programme, the Commission should take into account the input of the Competence Centre and should share that input with the Programme Committee of Horizon Europe.

(23) In order to enable the Competence Centre to perform its role in the area of cybersecurity, to facilitate the involvement of the Network and to provide a strong governance role for the Member States, the Competence Centre should be established as a Union body with legal personality to which Commission Delegated Regulation (EU) 2019/715 ([8]) is to apply. The Competence Centre should perform a dual role, undertaking specific tasks in the area of cybersecurity industry, technology and research as laid down in this Regulation and managing cybersecurity-related funding from several programmes at the same time, in particular from Horizon Europe and the Digital Europe Programme, and possibly also from other Union programmes. Such management would have to be in accordance with the rules applicable to those programmes. Nevertheless, considering that the funding for the functioning of the Competence Centre would originate primarily from Horizon Europe and the Digital Europe Programme, it is necessary that the Competence Centre be considered as a partnership for the purpose of budget implementation, including during the programming phase.

(24) As a result of Union contribution, access to the results of the Competence Centre's activities and projects is to be as open as possible and as closed as necessary, and re-use of such results is to be possible where appropriate.

(25) The Competence Centre should facilitate and coordinate the work of the Network. The Network should be made up of one national coordination centre from each Member State. National coordination centres which have been recognised by the Commission as having the necessary capacity to manage funds to fulfil the mission and objectives laid down in this Regulation should receive direct Union financial support, including grants awarded without a call for proposals, in order to carry out their activities in relation to this Regulation.

(26) National coordination centres should be public sector entities, or entities with a majority of public participation, performing public administrative functions under national law, including by means of delegation, and they should be selected by Member States. It should be possible for the functions of a national coordination centre in a given Member State to be carried out by an entity that carries out other functions arising under Union law, such as those of a national competent authority, a single point of contact within the meaning of Directive (EU) 2016/1148 or any other Union Regulation, or a digital innovation hub within the meaning of Regulation (EU) 2021/694. Other public sector entities or entities performing public administrative functions in a Member State should be able to assist the national coordination centre in that Member State in carrying out its functions.

(27) National coordination centres should have the necessary administrative capacity, should possess or have access to cybersecurity industrial, technological and research expertise and should be in a position to effectively engage and coordinate with the industry, the public sector and the research community.

(28) Education in the Member States should reflect the importance of having adequate cybersecurity awareness and skills. To that end, taking into account the role of ENISA and without prejudice to the competences of Member States in education, the national coordination centres, alongside relevant public authorities and stakeholders, should contribute to promoting and disseminating cybersecurity educational programmes.

([8]) Commission Delegated Regulation (EU) 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (OJ L 122, 10.5.2019, p. 1).

(29) National coordination centres should be able to receive grants from the Competence Centre in order to provide financial support to third parties in the form of grants. The direct cost incurred by the national coordination centres for the provision and administration of financial support to third parties should be eligible for funding under the relevant programmes.

(30) The Competence Centre, the Network and the Community should help advance and disseminate the latest cybersecurity products, services and processes. At the same time, the Competence Centre and the Network should promote the cybersecurity capabilities of the demand-side industry, in particular by supporting developers and operators in sectors such as transport, energy, health, finance, government, telecommunications, manufacturing and space, in order to help such developers and operators solve their cybersecurity challenges, such as by implementing security by \design. The Competence Centre and the Network should also support the standardisation and deployment of cybersecurity products, services and processes while promoting, where possible, the implementation of the European cybersecurity certification framework as established by Regulation (EU) 2019/881.

(31) Due to the fast-changing nature of cyber threats and cybersecurity, the Union needs to be able to adapt quickly and continuously to new developments in the area. Hence, the Competence Centre, the Network and the Community should be flexible enough to ensure the required ability to respond to such developments. They should facilitate projects that help entities to be able to constantly build capabilities to enhance their own and the Union's resilience.

(32) The Competence Centre should support the Community. The Competence Centre should implement cybersecurity relevant parts of Horizon Europe and the Digital Europe Programme in accordance with the multiannual work programme of the Competence Centre (multiannual work programme), the annual work programme and the strategic planning process of Horizon Europe by allocating grants and other forms of funding, primarily following a competitive call for proposals. The Competence Centre should also facilitate the transfer of expertise in the Network and the Community and should support joint investment by the Union, Member States or industry. It should pay particular attention to supporting SMEs in the area of cybersecurity, as well as to actions that help overcome the skills gap.

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

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

(35) The Competence Centre should cooperate and ensure synergies with ENISA and should receive relevant input from ENISA when defining funding priorities.

(36) In order to respond to the needs of both the demand and supply sides of cybersecurity, the Competence Centre's task of providing cybersecurity knowledge and technical assistance to industries should refer to both ICT products, processes and services and to all other technological products and processes in which cybersecurity is to be embedded. Where it so requests, the public sector could also benefit from support from the Competence Centre.

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

(38) Whereas the Competence Centre and the Network should strive to enhance synergies and coordination between the cybersecurity civilian and defence spheres, projects under this Regulation that are financed by Horizon Europe should be implemented in accordance with Regulation (EU) 2021/695, which provides that research and innovation activities carried out under Horizon Europe are to have an exclusive focus on civil applications.

(39) This Regulation applies primarily to civilian matters, but Member States' activities under this Regulation may reflect specificities of Member States in cases when cybersecurity policy is pursued by authorities carrying out both civilian and military tasks, should strive for complementarity and should avoid overlap with defence-related funding instruments.

(40) This Regulation should ensure the liability and transparency of the Competence Centre and those undertakings receiving funding, in line with the relevant programme Regulations.

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

(42) In view of its expertise in cybersecurity and its mandate as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for relevant Union stakeholders, and in view of its collection of input through its tasks, ENISA should play an active part in the activities of the Competence Centre, including the development of the Agenda, avoiding any duplication of their tasks, in particular through its role as permanent observer in the Governing Board of the Competence Centre. Regarding the drafting of the Agenda, the annual work programme and the multiannual work programme, the Executive Director of the Competence Centre and the Governing Board should take into account any relevant strategic advice and input provided by ENISA, in accordance with the rules of procedure of the Governing Board.

(43) 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 Community should publicise the fact that their respective activities are undertaken in the context of this Regulation.

(44) The costs arising from the establishment of the Competence Centre and from the administrative and coordination activities of the Competence Centre should be financed by the Union and by the Member States, in proportion to the voluntary contributions from the Member States to joint actions. In order to avoid double funding, those activities should not benefit simultaneously from a contribution from other Union programmes.

(45) The Governing Board, which should be composed of representatives from the Member States and the Commission, should define the general direction of the Competence Centre's operations and should ensure that the Competence Centre carries out its tasks in accordance with this Regulation. The Governing Board should adopt the Agenda.

(46) The Governing Board should be entrusted with the powers necessary to establish the budget of the Competence Centre. It should verify the execution of the budget, should adopt appropriate financial rules, and should establish transparent working procedures for the Competence Centre's decision-making, including for the adoption, reflecting the Agenda, of the annual work programme and the multiannual work programme. The Governing Board should also adopt its rules of procedure, should appoint the Executive Director and should decide on any extension or termination of the Executive Director's term of office.

(47) The Governing Board should have oversight of the strategic and implementation activities of the Competence Centre and should ensure that those activities are aligned. In its annual report, the Competence Centre should put special emphasis on the strategic goals that it has achieved and, if necessary, propose actions for further improvement of the achievement of those strategic goals.

(48) In order for the Competence Centre to function properly and effectively, the Commission and the Member States should ensure that the 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 the continuity of its work.

(49) In view of the Competence Centre's specific status and its responsibility for the implementation of Union funds, in particular those from Horizon Europe and the Digital Europe Programme, the Commission should have 26 % of the total votes in the Governing Board in respect of decisions involving Union funds, in order to maximise the Union value added of those decisions, while ensuring that those decisions are legal and are aligned with Union priorities.

(50) The smooth functioning of the Competence Centre requires that its Executive Director be appointed in a transparent manner, on the basis of merit, documented administrative and managerial skills and competence and experience relevant to cybersecurity, and that the duties of the Executive Director be carried out with complete independence.

(51) The Competence Centre should have a Strategic Advisory Group as an advisory body. The Strategic Advisory Group should provide advice on the basis of a regular dialogue between the Competence Centre and the Community, which should be formed by the representatives of the private sector, consumers' organisations, academia and other relevant stakeholders. The Strategic Advisory Group should focus on issues relevant to stakeholders and bring them to the attention of the Governing Board and the Executive Director. The tasks of the Strategic Advisory Group should include providing advice regarding the Agenda, the annual work programme and the multiannual work programme. The representation of the different stakeholders in the Strategic Advisory Group should be balanced, with particular attention paid to the representation of SMEs, in order to ensure that stakeholders are appropriately represented in the work of the Competence Centre.

(52) Contributions of the Member States to the resources of the Competence Centre could be financial or in-kind. For example, such financial contributions could consist of a grant given by a Member State to a beneficiary in that Member State that complements Union financial support given to a project under the annual work programme. On the other hand, in-kind contributions would typically be made where a Member State entity is itself the beneficiary of Union financial support. For example, if the Union subsidises an activity of a national coordination centre at a financing rate of 50 %, the remaining costs of the activity would be accounted for as an in-kind contribution. In another example, if a Member State entity receives Union financial support for creating or upgrading infrastructure that is to be shared among stakeholders in line with the annual work programme, the related non-subsidised costs would be accounted for as in-kind contributions.

(53) In accordance with the relevant provisions of Delegated Regulation (EU) 2019/715 on conflicts of interest, the Competence Centre should have in place rules regarding the prevention, identification and resolution and management of conflicts of interest in respect of its members, bodies and staff, the Governing Board, as well as the Strategic Advisory Group and the Community. Member States should ensure the prevention, identification, and resolution of conflicts of interest in respect of the national coordination centres in accordance with national law. The Competence Centre should also apply relevant Union law concerning public access to documents as set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council ([9]). The processing of personal data by the Competence Centre should be subject to Regulation (EU) 2018/1725 of the European Parliament and of the Council ([10]). The Competence Centre should comply with the provisions of Union law that apply to Union institutions, and with national law regarding the handling of information, in particular the handling of sensitive non-classified information and EU classified information.

(54) The financial interests of the Union and of the Member States should be protected by proportionate measures throughout the expenditure cycle, including the prevention, detection and investigation of irregularities, the recovery of lost, wrongly paid or incorrectly used funds and, where appropriate, the application of administrative and financial penalties in accordance with Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council ([11]) (the 'Financial Regulation').

(55) The Competence Centre should operate in an open and transparent way. It should provide all relevant information in a timely manner and should promote its activities, including information and dissemination activities to the wider public. The rules of procedure of the Governing Board of the Competence Centre and of the Strategic Advisory Group should be made publicly available.

([9]) 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).

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

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

(56) The Commission's internal auditor should exercise the same powers over the Competence Centre as those exercised in respect of the Commission.

(57) The Commission, the Court of Auditors and the European Anti-Fraud Office should get access to all necessary information and the premises of the Competence Centre to conduct audits and investigations on the grants, contracts and agreements signed by the Competence Centre.

(58) Since the objectives of this Regulation, namely strengthening the Union's competitiveness and capacities, retaining and developing Union's cybersecurity research technological and industrial capacities, increasing the competitiveness of the Union's cybersecurity industry and turning cybersecurity into a competitive advantage for other Union industries, cannot be sufficiently achieved by the Member States alone, due to the fact that existing, limited resources are dispersed and due to the scale of the investment necessary, but can rather, by reason of avoiding unnecessary duplication of those efforts, helping to achieve critical mass of investment, ensuring that public financing is used in an optimal way and ensuring that a high level of cybersecurity is promoted in all Member States, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions and principles of the Competence Centre and the Network

Article 1

Subject matter and scope

1. This Regulation establishes the European Cybersecurity Industrial, Technology and Research Competence Centre (the 'Competence Centre') and the Network of National Coordination Centres (the 'Network'). It lays down rules for the nomination of national coordination centres as well as rules for the establishment of the Cybersecurity Competence Community (the 'Community').

2. The Competence Centre shall have an essential role in the implementation of the cybersecurity part of the Digital Europe Programme, in particular with regard to actions related to Article 6 of Regulation (EU) 2021/694, and shall contribute to the implementation of Horizon Europe, in particular with regard to Section 3.1.3 of Pillar II of Annex I to Council Decision (EU) 2021/764 ([12]).

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

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

Article 2

Definitions

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

(1) 'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;

(2) 'network and information system' means a network and information system as defined in point (1) of Article 4 of Directive (EU) 2016/1148;

(3) 'cybersecurity products, services and processes' means commercial and non-commercial ICT products, services or processes with the specific purpose of protecting network and information systems or ensuring the confidentiality, integrity and accessibility of data that are processed or stored in network and information systems, as well as the cybersecurity of the users of such systems and other persons affected by cyber threats;

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

([12]) Council Decision (EU) 2021/764 of 10 May 2021 establishing the Specific Programme implementing Horizon Europe – the Framework Programme for Research and Innovation, and repealing Decision 2013/743/EU (OJ L 167 I, 12.5.2021, p. 1).

(5) 'joint action' means an action that is included in the annual work programme and that receives financial support from Horizon Europe, the Digital Europe Programme or other Union programmes as well as financial or in-kind support by one or more Member States, and which is implemented via projects involving beneficiaries that are established in and receive financial or in-kind support from those Member States;

(6) 'in-kind contribution' means eligible costs incurred by national coordination centres and other public entities when they participate in projects funded through this Regulation, where those costs are not financed by a Union contribution or by financial contributions from Member States;

(7) 'European Digital Innovation Hub' means a European Digital Innovation Hub as defined in point (e) of Article 2 of Regulation (EU) 2021/694;

(8) 'Agenda' means a comprehensive and sustainable cybersecurity industrial, technology and research strategy which sets out strategic recommendations for the development and growth of the European cybersecurity industrial, technological and research sector and strategic priorities for the Competence Centre's activities and is not binding with respect to decisions to be taken on the annual work programmes;

(9) 'technical assistance' means assistance by the Competence Centre to the national coordination centres or the Community in the performance of theirs tasks by providing knowledge or facilitating access to expertise in the area of cybersecurity research, technology and industry, facilitating networking, raising awareness and promoting cooperation, or means assistance by the Competence Centre together with the national coordination centres to stakeholders with respect to the preparation of projects in relation to the mission of the Competence Centre and the Network and the objectives of the Competence Centre.

Article 3

Mission of the Competence Centre and the Network

1. The mission of the Competence Centre and the Network is to help the Union to:

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

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

(c) increase the global competitiveness of the Union's cybersecurity industry, ensure high cybersecurity standards throughout the Union and turn cybersecurity into a competitive advantage for other Union industries.

2. The Competence Centre and the Network shall undertake their tasks in collaboration with ENISA and the Community, as appropriate.

3. The Competence Centre shall, in accordance with the legislative acts establishing the relevant programmes, in particular Horizon Europe and the Digital Europe Programme, use relevant Union financial resources in such a way as to contribute to the mission set out in paragraph 1.

Article 4

Objectives of the Competence Centre

1. The Competence Centre shall have the overall objective of promoting research, innovation and deployment in the area of cybersecurity in order to fulfil the mission as set out in Article 3.

2. The Competence Centre shall have the following specific objectives:

(a) enhancing cybersecurity capacities, capabilities, knowledge and infrastructure for the benefit of industry, in particular SMEs, research communities, the public sector and civil society, as appropriate;

(b) promoting cybersecurity resilience, the uptake of cybersecurity best practices, the principle of security by design, and the certification of the security of digital products and services, in a manner that complements the efforts of other public entities;

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

3. The Competence Centre shall implement the specific objectives referred to in paragraph 2 by:

(a) establishing strategic recommendations for research, innovation and deployment in cybersecurity in accordance with Union law and setting out strategic priorities for the Competence Centre's activities;

(b) implementing actions under relevant Union funding programmes in accordance with the relevant work programmes and the Union legislative acts establishing those funding programmes;

(c) fostering cooperation and coordination among the national coordination centres and with and within the Community; and

(d) where relevant and appropriate, acquiring and operating ICT infrastructure and services where necessary to fulfil the tasks set out in Article 5 and in accordance with the respective work programmes set out in point (b) of Article 5(3).

Article 5

Tasks of the Competence Centre

1. In order to fulfil its mission and objectives, the Competence Centre shall have the following tasks:

(a) strategic tasks; and

(b) implementation tasks.

2. The strategic tasks referred to in point (a) of paragraph 1 shall consist of:

(a) developing and monitoring the implementation of the Agenda;

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

(i) establishing priorities for the work of the Competence Centre in relation to:

(1) the enhancement of cybersecurity research and innovation, covering the entire innovation cycle, and the deployment of that research and innovation;

(2) the development of cybersecurity industrial, technological and research capacities, capabilities, and infrastructure;

(3) the reinforcement of cybersecurity and technology skills and competence in industry, technology and research and at all relevant educational levels, supporting gender balance;

(4) the deployment of cybersecurity products, services and processes;

(5) support for the uptake by the market of cybersecurity products, services and processes contributing to the mission set out in Article 3;

(6) support for the adoption and integration of state-of-the-art cybersecurity products, services and processes by public authorities at their request, by demand-side industries and by other users;

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

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

(c) ensuring synergies between and cooperation with relevant Union institutions, bodies, offices and agencies, in particular ENISA, while avoiding any duplication of activities with those Union institutions, bodies, offices and agencies;

(d) coordinating national coordination centres through the Network and ensuring a regular exchange of expertise;

(e) providing expert cybersecurity industrial, technology and research advice to Member States at their request, including with regard to the procurement and deployment of technologies;

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

(g) attending Union, national and international conferences, fairs and forums related to the mission, objectives and tasks of the Competence Centre with the aim of sharing views and exchanging relevant best practices with other participants;

(h) facilitating the use of results from research and innovation projects in actions related to the development of cybersecurity products, services and processes, while seeking to avoid the fragmentation and duplication of efforts and replicating good cybersecurity practices and cybersecurity products, services and processes, in particular those developed by SMEs and those using open source software.

3. The implementation tasks referred to in point (b) of paragraph 1 shall consist of:

(a) coordinating and administrating the work of the Network and the Community in order to fulfil the mission set out in Article 3, in particular by supporting cybersecurity start-ups, SMEs, microenterprises, associations and civic technology projects in the Union and facilitating their access to expertise, funding, investment and markets;

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

(i) the Digital Europe Programme, in particular actions related to Article 6 of Regulation (EU) 2021/694;

(ii) joint actions receiving support under the provisions that relate to cybersecurity in Horizon Europe, in particular with regard to Section 3.1.3 of Pillar II of Annex I to Decision (EU) 2021/764, in accordance with the multiannual work programme and the strategic planning process of Horizon Europe; and

(iii) other programmes where provided for in the relevant legislative acts of the Union;

(c) supporting, where appropriate, the achievement of Specific Objective 4 – 'Advanced Digital Skills' as set out in Article 7 of Regulation (EU) 2021/694, in cooperation with European Digital Innovation Hubs;

(d) providing expert advice on cybersecurity industry, technology and research to the Commission when the Commission prepares draft work programmes pursuant to Article 13 of Decision (EU) 2021/764;

(e) carrying out or enabling the deployment of ICT infrastructure and facilitating the acquisition of such infrastructure, for the benefit of society, industry and the public sector, at the request of Member States, research communities and operators of essential services, by means of, inter alia, contributions from Member States and Union funding for joint actions, in accordance with the Agenda, the annual work programme and the multiannual work programme;

(f) raising awareness of the mission of the Competence Centre and the Network and of the objectives and tasks of the Competence Centre;

(g) without prejudice to the civilian nature of projects to be financed from Horizon Europe, and in accordance with Regulations (EU) 2021/695 and (EU) 2021/694, enhancing synergies and coordination between the cybersecurity civilian and defence spheres, by facilitating the exchange of:

(i) knowledge and information with regard to dual-use technologies and applications;

(ii) results, requirements and best practices; and

(iii) information with regard to the priorities of relevant Union programmes.

4. The Competence Centre shall carry out the tasks set out in paragraph 1 in close cooperation with the Network.

5. In accordance with Article 6 of Regulation (EU) 2021/695 and subject to a contribution agreement as defined in point (18) of Article 2 of the Financial Regulation, the Competence Centre may be entrusted with the implementation of the cybersecurity parts under Horizon Europe that are not co-funded by the Member States, in particular with regard to Section 3.1.3 of Pillar II of Annex I to Decision (EU) 2021/764.

Article 6

Nomination of national coordination centres

1. By 29 December 2021, each Member State shall nominate one entity which fulfils the criteria laid down in paragraph 5 to act as its national coordination centre for the purposes of this Regulation. Each Member State shall notify that entity to the Governing Board without delay. Such entity may be an entity already established in that Member State.

The deadline set out in the first subparagraph of this paragraph shall be extended for the period during which the Commission is to issue the opinion referred to in paragraph 2.

2. At any time, a Member State may ask the Commission for an opinion concerning whether the entity that the Member State has nominated or intends to nominate to act as its national coordination centre has the necessary capacity to manage funds to fulfil the mission and objectives laid down in this Regulation. The Commission shall issue its opinion to that Member State within three months of the Member State's request.

3. On the basis of the notification by a Member State of an entity as referred to in paragraph 1, the Governing Board shall list that entity as a national coordination centre no later than three months after the notification. The Competence Centre shall publish the list of nominated national coordination centres.

4. A Member State may at any time nominate a new entity to act as its national coordination centre for the purposes of this Regulation. Paragraphs 1, 2 and 3 shall apply to the nomination of any new entity.

5. The national coordination centre shall be a public sector entity or an entity, a majority of which is owned by the Member State, which performs public administrative functions under national law, including by means of delegation, and having the capacity to support the Competence Centre and the Network in fulfilling their mission as set out in Article 3 of this Regulation. It shall either possess or have access to research and technological expertise in cybersecurity. It shall have the capacity to engage effectively and coordinate with industry, the public sector, the academic and research community and citizens, as well as with authorities designated pursuant to Directive (EU) 2016/1148.

6. At any time, a national coordination centre may request to be recognised as having the necessary capacity to manage funds to fulfil the mission and objectives laid down in this Regulation, in accordance with Regulations (EU) 2021/695 and (EU) 2021/694. Within three months of such a request, the Commission shall assess whether that national coordination centre has such capacity and shall issue a decision.

Where the Commission has provided a positive opinion to a Member State in accordance with the procedure laid down in paragraph 2, that opinion shall be deemed to be a decision recognising the relevant entity as having the necessary capacity for the purposes of this paragraph.

No later than 29 August 2021, after consulting the Governing Board, the Commission shall issue guidelines on the assessment referred to in the first subparagraph, including a specification of the conditions for recognition and how opinions and assessments are conducted.

Before issuing the opinion referred to in paragraph 2 and the decision referred to in the first subparagraph of this paragraph, the Commission shall take into account any information and documentation provided by the requesting national coordination centre.

Any decision not to recognise a national coordination centre as having the necessary capacity to manage funds to fulfil the mission and objectives laid down in this Regulation shall be duly reasoned, setting out the requirements the requesting national coordination centre has not yet fulfilled that justify the decision to withhold recognition. Any national coordination centre whose request for recognition has been rejected may resubmit its request with additional information at any time.

Member States shall inform the Commission in the event of changes to the national coordination centre, such as the composition of the national coordination centre, the legal form of the national coordination centre or other relevant aspects, that affect its capacity to manage funds to fulfil the mission and objectives laid down in this Regulation. On receiving such information the Commission may review a decision to grant or withhold recognition of the national coordination centre as having the necessary capacity to manage funds accordingly.

7. The Network shall be composed of all the national coordination centres that have been notified to the Governing Board by the Member States.

Article 7

Tasks of the national coordination centres

1. The national coordination centres shall have the following tasks:

(a) acting as points of contact at national level for the Community to support the Competence Centre in fulfilling its mission and objectives, in particular in coordinating the Community through the coordination of Community members in their Member States;

(b) providing expertise and actively contributing to the strategic tasks set out in Article 5(2), taking into account relevant national and regional challenges for cybersecurity in different sectors;

(c) promoting, encouraging and facilitating the participation of civil society, industry, in particular start-ups and SMEs, the academic and research communities and other stakeholders at national level in cross-border projects and in cybersecurity actions funded by relevant Union programmes;

(d) providing technical assistance to stakeholders by supporting them in the application phase for projects managed by the Competence Centre in relation to its mission and objectives, and in full compliance with the rules of sound financial management, especially with regard to conflicts of interest;

(e) seeking to establish synergies with relevant activities at national, regional and local level, such as national policies on research, development and innovation in the area of cybersecurity, in particular those policies stated in the national cybersecurity strategies;

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

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

(h) promoting and disseminating the relevant outcomes of the work of the Network, the Community and the Competence Centre at national, regional or local level;

(i) assessing requests by entities established in the same Member State as the national coordination centre to become part of the Community;

(j) advocating and promoting the involvement of relevant entities in the activities arising from the Competence Centre, the Network and the Community, and monitoring, as appropriate, the level of engagement with and the amount of public financial support awarded for cybersecurity research, developments and deployments.

2. For the purposes of point (f) of paragraph 1 of this Article, the financial support to third parties may be provided in any of the forms of Union contribution specified in Article 125 of the Financial Regulation, including in the form of lump sums.

3. On the basis of a decision as referred to in Article 6(6) of this Regulation, national coordination centres may receive a grant from the Union in accordance with point (d) of the first paragraph of Article 195 of the 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.

Article 8

The Cybersecurity Competence Community

1. The Community shall contribute to the mission of the Competence Centre and the Network set out in Article 3 and shall enhance, share and disseminate cybersecurity expertise across the Union.

2. The Community shall consist of industry, including SMEs, academic and research organisations, other relevant civil society associations as well as, as appropriate, relevant European Standardisation Organisations, public entities and other entities dealing with cybersecurity operational and technical matters and, where relevant, stakeholders in sectors that have an interest in cybersecurity and that face cybersecurity challenges. The Community shall bring together the main stakeholders with regard to cybersecurity technological, industrial, academic and research capacities in the Union. It shall involve national coordination centres, European Digital Innovation Hubs, where relevant, as well as Union institutions, bodies, offices and agencies with relevant expertise, such as ENISA.

3. Only entities which are established within the Member States shall be registered as members of the Community. They shall demonstrate that they are able to contribute to the mission and shall have cybersecurity expertise with regard to at least one of the following domains:

(a) academia, research or innovation;

(b) industrial or product development;

(c) training and education;

(d) information security or incident response operations;

(e) ethics;

(f) formal and technical standardisation and specifications.

4. The Competence Centre shall register entities, at their request, as members of the Community after an assessment made by the national coordination centre of the Member State in which those entities are established to confirm that those entities meet the criteria set out in paragraph 3 of this Article. That assessment shall also take into account any relevant national assessment on security grounds made by the national competent authorities. Such registrations shall not be limited in time but may be revoked by the Competence Centre at any time if the relevant national coordination centre considers that the entity concerned no longer fulfils the criteria set out in paragraph 3 of this Article or falls under Article 136 of the Financial Regulation, or on justified security grounds. Where membership in the Community is revoked on security grounds, the decision to revoke shall be proportional and reasoned. The national coordination centres shall aim to achieve a balanced representation of stakeholders in the Community and actively stimulate participation, in particular of SMEs.

5. National coordination centres shall be encouraged to cooperate through the Network in order to harmonise the way in which they apply the criteria set out in paragraph 3 and the procedures for assessing and registering entities referred to in paragraph 4.

6. The Competence Centre shall register relevant Union institutions, bodies, offices and agencies as members of the Community after carrying out an assessment to confirm that that Union institution, body, office or agency meets the criteria set out in paragraph 3 of this Article. Such registrations shall not be limited in time but may be revoked by the Competence Centre at any time if it considers that the Union institution, body, office or agency no longer fulfils the criteria set out in paragraph 3 of this Article or falls under Article 136 of the Financial Regulation.

7. Representatives of the Union institutions, bodies, offices and agencies may participate in the work of the Community.

8. An entity registered as a member of the Community shall designate its representatives to ensure an efficient dialogue. Those representatives shall have expertise with regard to cybersecurity research, technology or industry. The requirements may be further specified by the Governing Board, without unduly limiting the entities in the designation of their representatives.

9. The Community, through its working groups and in particular through the Strategic Advisory Group, shall provide the Executive Director and the Governing Board with strategic advice on the Agenda, the annual work programme and the multiannual work programme, in accordance with the rules of procedure of the Governing Board.

Article 9

Tasks of the members of the Community

The members of the Community shall:

(a) support the Competence Centre in fulfilling its mission and objectives and, for that purpose, shall work closely with the Competence Centre and the national coordination centres;

(b) where relevant, participate in formal or informal activities and in the working groups referred to in point (n) of Article 13(3) to carry out specific activities as provided by the annual work programme; and

(c) where relevant, support the Competence Centre and the national coordination centres in promoting specific projects.

Article 10

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

1. To ensure consistency and complementarity while avoiding any duplication of effort, the Competence Centre shall cooperate with relevant Union institutions, bodies, offices and agencies, including ENISA, the European External Action Service, the Directorate-General Joint Research Centre of the Commission, the European Research Executive Agency, the European Research Council Executive Agency and the European Health and Digital Executive Agency established by Commission Implementing Decision (EU) 2021/173 ([13]), relevant European Digital Innovation Hubs, the European Cybercrime Centre at the European Union Agency for Law Enforcement Cooperation established by Regulation (EU) 2016/794 of the European Parliament and of the Council ([14]), the European Defence Agency in relation to the tasks set out in Article 5 of this Regulation and other relevant Union entities. The Competence Centre may also cooperate with international organisations, where relevant.

2. Cooperation as referred to in paragraph 1 of this Article may take place within the framework of working arrangements. Those arrangements shall be submitted for the approval of the Governing Board. Any sharing of classified information shall take place within the framework of administrative arrangements concluded in accordance with Article 36(3).

CHAPTER II

Organisation of the Competence Centre

Article 11

Membership and structure

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

2. The structure of the Competence Centre shall ensure the achievement of the objectives set out in Article 4 and the tasks set out in Article 5, and shall comprise:

(a) a Governing Board;

(b) an Executive Director;

(c) a Strategic Advisory Group.

([13]) Commission Implementing Decision (EU) 2021/173 of 12 February 2021 establishing the European Climate, Infrastructure and Environment Executive Agency, the European Health and Digital Executive Agency, the European Research Executive Agency, the European Innovation Council and SMEs Executive Agency, the European Research Council Executive Agency, and the European Education and Culture Executive Agency and repealing Implementing Decisions 2013/801/EU, 2013/771/EU, 2013/778/EU, 2013/779/EU, 2013/776/EU and 2013/770/EU (OJ L 50, 15.2.2021, p. 9).

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

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 two representatives of the Commission who act on behalf of the Union.

2. Each member of the Governing Board shall have an alternate. That alternate shall represent the member in the member's absence.

3. Members of the Governing Board appointed by Member States and their alternates shall be public sector staff in their respective Member State and shall be appointed on the basis of their knowledge in the area of cybersecurity research, technology and industry, their ability to ensure the coordination of actions and positions with their respective national coordination centre, or their relevant managerial, administrative and budgetary skills. The Commission shall appoint its members of the Governing Board and their alternates on the basis of their knowledge in the area of cybersecurity, technology, or their relevant managerial, administrative and budgetary skills and of their ability to ensure coordination, synergies and, as far as possible, joint initiatives between different sectoral or horizontal Union policies involving cybersecurity. The Commission and the Member States shall make efforts to limit the turnover of their representatives in the Governing Board, in order to ensure the continuity of the Governing Board's work. The Commission and the Member States shall aim to achieve a balanced representation between men and women on the Governing Board.

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

5. The members of the Governing Board shall ensure that the Competence Centre's mission, objectives, identity and autonomy are safeguarded and that its actions are consistent with that mission and those objectives, in an independent and transparent way.

6. The Governing Board may invite observers to take part in its meetings as appropriate, including representatives of relevant Union institutions, bodies, offices and agencies, and the members of the Community.

7. A representative from ENISA shall be a permanent observer in the Governing Board. The Governing Board may invite a representative from the Strategic Advisory Group to attend its meetings.

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

Article 13

Tasks of the Governing Board

1. The Governing Board shall have the overall responsibility for the strategic orientation and the operations of the Competence Centre, shall supervise the implementation of its activities and shall be responsible for any task that is not specifically allocated to the Executive Director.

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

3. The Governing Board shall take necessary strategic decisions, in particular with regard to:

(a) the development and adoption of the Agenda and the monitoring of its implementation;

(b) reflecting the Union's policy priorities and the Agenda, the adoption of the multiannual work programme containing common, industrial, technology and research priorities which are based on the needs identified by Member States in cooperation with the Community and which require the focus of Union financial support, including key technologies and domains for developing the Union's own capabilities in cybersecurity;

(c) the adoption of the annual work programme for implementing the relevant Union funds, in particular the cybersecurity parts of Horizon Europe insofar as they are co-financed voluntarily by Member States and of the Digital Europe Programme, in accordance with the Competence Centre's multiannual work programme and the strategic planning process of Horizon Europe;

(d) the adoption of the Competence Centre's annual accounts, balance sheet and annual activity report, on the basis of a proposal from the Executive Director;

(e) the adoption of the specific financial rules of the Competence Centre in accordance with Article 70 of the Financial Regulation;

(f) as part of the annual work programme, the allocation of funds from the Union budget to topics for joint actions between the Union and Member States;

(g) as part of the annual work programme, and in accordance with the decisions referred to in point (f) of this subparagraph and in compliance with Regulations (EU) 2021/695 and (EU) 2021/694, the description of the joint actions referred to in point (f) of this subparagraph and the laying down of conditions for the implementation of such joint actions;

(h) the adoption of a procedure for appointing the Executive Director and the appointment, dismissal, extension of the term of office of, provision of guidance to and the monitoring of the performance of the Executive Director;

(i) the adoption of guidelines for assessing and registering entities as members of the Community;

(j) the adoption of the working arrangements referred to in Article 10(2);

(k) the appointment of the Accounting Officer;

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

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

(n) the establishment of working groups within the Community, where relevant taking into account advice provided by the Strategic Advisory Group;

(o) the appointment of members of the Strategic Advisory Group;

(p) the adoption of rules on the reimbursement of expenses for members for the Strategic Advisory Group;

(q) the setting up of a monitoring mechanism to ensure that the implementation of the respective funds managed by the Competence Centre is done in accordance with the Agenda, the mission, the multiannual work programme and the rules of the programmes that are the source of the relevant funding;

(r) the ensuring of a regular dialogue and the establishment of an effective cooperation mechanism with the Community;

(s) the establishment of the Competence Centre's communications policy on the basis of a recommendation by the Executive Director;

(t) where appropriate, the establishment of rules implementing the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union, laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 ([15]) ('Staff Regulations' and 'Conditions of Employment'), in accordance with Article 30(3) of this Regulation;

(u) where appropriate, the laying down of rules on the secondment of national experts to the Competence Centre and on the use of trainees in accordance with Article 31(2);

(v) the adoption of security rules for the Competence Centre;

(w) the adoption of an anti-fraud and anti-corruption strategy that is proportionate to the fraud and corruption risks, as well as the adoption of comprehensive measures, in accordance with applicable Union legislation, to protect persons who report infringements of Union law, having regard to a cost-benefit analysis of the measures to be implemented;

(x) if necessary, the adoption of the methodology to calculate voluntary financial and in-kind contributions from contributing Member States in accordance with Regulations (EU) 2021/695 and (EU) 2021/694 or with any other applicable legislation;

([15]) OJ L 56, 4.3.1968, p. 1.

(y) in the context of the annual work programme and the multiannual work programme, the ensuring of coherence and synergies with those parts of the Digital Europe Programme and Horizon Europe which are not managed by the Competence Centre, as well as with other Union programmes;

(z) the adoption of the annual report on the implementation of the Competence Centre's strategic goals and priorities, if necessary with a recommendation for the better realisation of those goals and priorities.

Insofar the annual work programme contains joint actions, it shall contain information about Member States' voluntary contributions to joint actions. Where appropriate, proposals, in particular the proposal for the annual work programme, shall assess the need to apply security rules as set out in Article 33 of this Regulation, including the security self-assessment procedure in accordance with Article 20 of Regulation (EU) 2021/695.

4. Regarding the decisions set out in points (a), (b) and (c) of paragraph 3, the Executive Director and the Governing Board shall take into account any relevant strategic advice and input provided by ENISA, in accordance with the rules of procedure of the Governing Board.

5. The Governing Board shall be responsible for ensuring that the recommendations contained in the implementation report and the evaluation referred to in Article 38(2) and (4) are adequately followed up.

Article 14

Chairperson and meetings of the Governing Board

1. The Governing Board shall elect a Chairperson and a Deputy Chairperson from among its members, each for a period of three years. The mandate of the Chairperson and the Deputy Chairperson may be extended once by a decision by the Governing Board. If, however, the membership of the Governing Board of the Chairperson or Deputy Chairperson ends at any time during their terms of office, their terms of office shall automatically expire at that time. The Deputy Chairperson shall replace the Chairperson *ex officio* if the latter is unable to attend to his or her duties. The Chairperson shall take part in the voting.

2. The Governing Board shall hold 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 Chairperson, or at the request of the Executive Director in the fulfilment of his or her tasks.

3. The Executive Director shall take part in the deliberations of the Governing Board, unless decided otherwise by the Governing Board, but shall have no right to vote.

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

5. The Chairperson may invite representatives of the Community to take part in the meetings of the Governing Board, but they shall have no right to vote.

6. The members of the Governing Board and their alternates may be assisted at the meetings by advisers or experts, subject to the rules of procedure of the Governing Board.

7. The Competence Centre shall provide the secretariat for the Governing Board.

Article 15

Voting rules of the Governing Board

1. The Governing Board shall use a consensual approach in its discussions. A vote shall be held if the members of the Governing Board fail to achieve consensus.

2. If the Governing Board fails to achieve consensus on a matter, it shall take its decisions by a majority of at least 75 % of the votes of all its members, the representatives of the Commission constituting a single member for that purpose. An absent member of the Governing Board may delegate his or her vote to his or her alternate or, in the absence of his or her alternate, to another member. No member of the Governing Board shall represent more than one other member.

3. Decisions of the Governing Board on the joint actions and their management as referred to in points (f) and (g) of Article 13(3) shall be taken as follows:

(a) decisions to allocate funds from the Union budget to joint actions as referred to in point (f) of Article 13(3) and decisions to include such joint actions in the annual work programme shall be taken in accordance with paragraph 2 of this Article;

(b) decisions relating to the description of joint actions and laying down conditions for their implementation referred in point (g) of Article 13(3) shall be taken by participating Members States and the Commission, subject to the right to vote of the members being proportional to their respective contributions to that joint action, calculated in accordance with the methodology adopted pursuant to point (x) of Article 13(3).

4. For decisions which are taken under points (b), (c), (d), (e), (f), (k), (l), (p), (q), (t), (u), (w), (x) and (y) of Article 13(3), the Commission shall have 26 % of the total votes within the Governing Board.

5. For decisions other than those referred to in point (b) of paragraph 3 and in paragraph 4, each Member State and the Union shall have one vote. The vote of the Union shall be cast jointly by the two representatives of the Commission.

6. The Chairperson shall take part in the voting.

Section II

Executive Director

Article 16

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

1. The Executive Director shall be a person with expertise and a strong 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 point (a) of Article 2 of the Conditions of Employment.

3. The Executive Director shall be appointed by the Governing Board from a list of candidates proposed by the Commission, following an open, transparent and non-discriminatory selection procedure.

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

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

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

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

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

Article 17

Tasks of the Executive Director

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

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

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

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

(c) after consulting the Governing Board and the Commission and taking into account the input of the national coordination centres and the Community, prepare and submit for adoption to the Governing Board the Agenda, as well as, in accordance with the Agenda, the draft annual work programme and the draft multiannual work programme of the Competence Centre, including the scope of the calls for proposals, calls for expressions of interest and calls for tenders needed to implement the annual work programme and the corresponding expenditure estimates as proposed by the Member States and the Commission;

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

(e) implement the annual work programme and the multiannual work programme and report to the Governing Board with regard thereto;

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

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

(h) prepare an action plan that follows up on the conclusions of the implementation report and the evaluation referred to in Article 38(2) and (4) and, every two years, submit reports on progress to the European Parliament and to the Commission;

(i) prepare and conclude agreements with the national coordination centres;

(j) be responsible for administrative, financial and staff matters, including the implementation of the Competence Centre's budget, taking due account of advice received from the relevant internal audit function, in accordance with the decisions referred to in points (e), (l), (t), (u), (v) and (w) of Article 13(3);

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

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

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

(n) approve the tenders selected for funding;

(o) submit the draft annual accounts and balance sheet to the relevant internal audit function, and subsequently to the Governing Board;

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

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

(r) sign procurement contracts;

(s) prepare an action plan that follows up on the conclusions of internal or external audit reports, as well as investigations by the European Anti-Fraud Office (OLAF) established with Commission Decision 1999/352/EC, ECSC, Euratom [16] and report on progress twice a year to the Commission and regularly to the Governing Board;

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

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

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

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

(w) take any other measures needed to assess the Competence Centre's fulfilment of its mission and objectives;

(x) perform any other tasks entrusted or delegated to him or her by the Governing Board.

Section III

Strategic Advisory Group

Article 18

Composition of the Strategic Advisory Group

1. The Strategic Advisory Group shall consist of no more than 20 members. The members shall be appointed by the Governing Board, acting on a proposal from the Executive Director, from among the representatives of the members of the Community other than representatives of Union institutions, bodies, offices and agencies. Only representatives of members which are not controlled by a third country or by an entity established in a third-country shall be eligible. The appointment shall be made in accordance with an open, transparent, and non-discriminatory procedure. The Governing Board shall aim for the composition of the Strategic Advisory Group to achieve a balanced representation of the Community between scientific, industrial and civil society entities, demand and supply-side industries, large enterprises and SMEs, as well as balanced representation in terms of geographical provenance and gender. It shall also aim to achieve an intra sectorial balance, having regard to the cohesion of the Union and all of the Member States in the area of cybersecurity research, industry and technology. The Strategic Advisory Group shall be composed so as to enable a comprehensive, ongoing and permanent dialogue between the Community and the Competence Centre.

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

3. Procedures concerning the appointment of the members of the Strategic Advisory Group and the operation of the Strategic Advisory Group shall be specified in the rules of procedure of the Governing Board and shall be made public.

4. The terms of office of members of the Strategic Advisory Group shall be two years. Those terms shall be renewable once.

5. Representatives of the Commission and of other Union institutions, bodies, offices and agencies, in particular ENISA, may be invited by the Strategic Advisory Group to participate in and support its work. The Strategic Advisory Group may invite additional representatives from the Community in the capacity of observer, adviser, or expert, as appropriate on a case-by-case basis, to take into account the dynamic of developments in the area of cybersecurity. Members of the Governing Board may participate as observers in the meetings of the Strategic Advisory Group.

Article 19

Functioning of the Strategic Advisory Group

1. The Strategic Advisory Group shall meet at least three times a year.

2. The Strategic Advisory Group shall provide advice to the Governing Board on the establishment of working groups within the Community, in accordance with point (n) of Article 13(3) on specific issues relevant to the work of the Competence Centre, whenever those issues directly relate to the tasks and areas of competence set out in Article 20. Where necessary, such working groups shall be subject to the overall coordination of one or more members of the Strategic Advisory Group.

3. The Strategic Advisory Group shall elect its Chair by a simple majority of its members.

4. The secretariat of the Strategic Advisory Group shall be provided by the Executive Director and the staff of the Competence Centre, using existing resources, with due regard to the overall workload of the Competence Centre. The resources assigned to the support of the Strategic Advisory Group shall be indicated in the draft annual budget.

5. The Strategic Advisory Group shall adopt its rules of procedure by a simple majority of its members.

Article 20

Tasks of the Strategic Advisory Group

The Strategic Advisory Group shall regularly advise the Competence Centre in respect of the performance of the Competence Centre's activities and shall ensure communication with the Community and other relevant stakeholders. The Strategic Advisory Group shall also:

(a) taking into account contributions from the Community and the working groups referred to in point (n) of Article 13(3) where relevant, provide and update on an ongoing basis strategic advice and input to the Executive Director and the Governing Board with regard to the Agenda, the annual work programme and the multiannual work programme within the deadlines set by the Governing Board;

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

(c) subject to approval by the Governing Board, decide on and organise public consultations open to all public and private stakeholders who have an interest in the area of cybersecurity, in order to collect input for the strategic advice referred to in point (a).

CHAPTER III

Financial provisions

Article 21

Union and Member States' financial contributions

1. The Competence Centre shall be funded by the Union, while joint actions shall be funded by the Union and by voluntary contributions by the Member States.

2. The administrative and operational costs of joint actions shall be covered by the Union and by the Member States contributing to the joint actions, in accordance with Regulations (EU) 2021/695 and (EU) 2021/694.

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

(a) up to EUR 1 649 566 000 from the Digital Europe Programme, including up to EUR 32 000 000 for administrative costs;

(b) an amount from Horizon Europe, including for administrative costs, for joint actions, such amount being equal to the amount contributed by Member States pursuant to paragraph 7 of this Article but not exceeding the amount determined in the strategic planning process of Horizon Europe to be carried out pursuant to Article 6(6) of Regulation (EU) 2021/695, in the annual work programme or in the multiannual work programme;

(c) an amount from the other relevant Union programmes, as needed for the implementation of the tasks or the achievement of the objectives of the Competence Centre, subject to decisions taken in accordance with the legal acts of the Union establishing those programmes.

4. The maximum Union contribution shall be paid from the appropriations in the general budget of the Union allocated to Digital Europe Programme, the specific programme implementing Horizon Europe established by Decision (EU) 2021/764 and other programmes and projects falling within the scope of the Competence Centre or the Network.

5. The Competence Centre shall implement cybersecurity actions of the Digital Europe Programme and Horizon Europe in accordance with point (c)(iv) of the first subparagraph of Article 62(1) of the Financial Regulation.

6. Contributions from Union programmes other than those referred to in paragraphs 3 and 4 that are part of the Union co-financing to a programme implemented by one of the Member States shall not be accounted for in the calculation of the Union maximum financial contribution referred to in those paragraphs.

7. Member States shall voluntarily take part in joint actions by means of voluntary financial and/or in-kind contributions. If a Member State takes part in a joint action, the financial contribution by that Member State shall cover administrative costs in proportion to its contribution to that joint action. The administrative costs of joint actions shall be met by financial contributions. The operational costs of joint actions may be met by financial or in-kind contributions, as provided for by Horizon Europe and the Digital Europe Programme. Contributions from each Member State may take the form of support that the Member State provides in a joint action to beneficiaries established in that Member State. In-kind contributions by Member States consist of the eligible costs incurred by

national coordination centres and other public entities when participating in projects funded through this Regulation, less any Union contribution to those costs. In the case of projects funded by Horizon Europe, eligible costs shall be calculated in accordance with Article 36 of Regulation (EU) 2021/695. In the case of projects funded by the Digital Europe Programme, eligible costs shall be calculated in accordance with the Financial Regulation.

The envisaged amount of total Member State voluntary contributions to joint actions under Horizon Europe, including financial contributions for administrative costs, shall be determined in order to be taken into account in the strategic planning process of Horizon Europe to be carried out pursuant to Article 6(6) of Regulation (EU) 2021/695, with input from the Governing Board. For actions under the Digital Europe Programme, notwithstanding Article 15 of Regulation (EU) 2021/694, the Member States may make a contribution to the costs of the Competence Centre that are co-financed from the Digital Europe Programme that is lower than the amounts specified in point (a) of paragraph 3 of this Article.

8. Member States' national co-funding of actions supported by Union programmes other than Horizon Europe and the Digital Europe Programme shall be considered to be Member States' national contributions insofar as those contributions are parts of joint actions and are included in the Competence Centre's work programme.

9. For the purpose of assessing the contributions referred to in paragraph 3 of this Article and in point (b) of Article 22(2), costs shall be determined in accordance with the usual cost accounting practices of the Member State concerned, the applicable accounting standards of the Member State concerned, and the applicable international accounting standards and international financial reporting standards. 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 if there is any uncertainty arising from the certification.

10. If any Member State is in default of its commitments concerning its financial or in-kind contributions to joint actions, the Executive Director shall notify the Member State concerned thereof in writing and shall set a reasonable period within which such default is to be remedied. If the situation is not remedied within that period, the Executive Director shall convene a meeting of the Governing Board to decide whether the defaulting participating Member State's right to vote is to be revoked or whether any other measures are to be taken until that Member State has met its obligations. The defaulting Member State's right to vote concerning joint actions shall be suspended until the default of its commitments is remedied.

11. The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to joint actions if the contributing Member States do not contribute, contribute only partially or contribute late with regard to the contributions referred to in point (b) of paragraph 3. The termination, reduction or suspension of the Union's financial contribution by the Commission shall be proportionate in amount and time to the Member State's failure to contribute, partial contribution or late contribution.

12. The contributing Member States shall report by 31 January of each year to the Governing Board on the value of the contributions referred to in paragraph 7 for joint action with the Union made in each of the previous financial year.

Article 22

Costs and resources of the Competence Centre

1. The administrative costs of the Competence Centre shall in principle be covered by means of financial contributions from the Union on an annual basis. Additional financial contributions shall be made by contributing Member States in proportion to their voluntary contributions to joint actions. If part of the contribution for administrative costs is not used, it may be made available to cover the operational costs of the Competence Centre.

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

(a) the Union's financial contribution;

(b) voluntary financial or in-kind contributions from the contributing Member States in the case of joint actions.

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

(a) the Union's financial contributions to operational and administrative costs;

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

(c) contributing Member States' voluntary financial contributions to operational costs in the case of joint actions;

(d) any revenue generated by the Competence Centre;

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

4. Any interest yielded by the contributions paid to the Competence Centre by the contributing Member States shall be considered to be the revenue of the Competence Centre.

5. All resources of the Competence Centre and its activities shall be used to achieve its objectives.

6. The Competence Centre shall own all assets that are generated by it or are transferred to it for the fulfilment of its objectives. Without prejudice to the applicable rules of the relevant funding programme, the ownership of assets that are generated or acquired in joint actions shall be decided in accordance with point (b) of Article 15(3).

7. Except when the Competence Centre is wound up, any excess revenue over expenditure shall continue to be owned by the Competence Centre and shall not be paid to the contributing members of the Competence Centre.

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

Article 23

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 24

Financial year

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

Article 25

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 the draft establishment plan referred to in point (l) of Article 13(3). Revenue and expenditure shall be in balance. The expenditure of the Competence Centre shall include the staff, administrative, infrastructure and operational expenses. Administrative expenses shall be kept to a minimum, including by means of redeployment of staff or posts.

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

3. The Governing Board shall, by 31 January of each year, send the statement of estimates referred to in paragraph 2 of this Article, which shall be part of the draft single programming document referred to in Article 32(1) of Delegated Regulation (EU) 2019/715, to the Commission.

4. On the basis of the statement of estimates referred to in paragraph 2 of this Article, the Commission shall enter in the draft budget of the Union the estimates it deems to be necessary for the establishment plan referred to in point (l) of Article 13(3) of this Regulation and the amount of the contribution to be charged to the general budget, which it shall submit to the European Parliament and the Council in accordance with Articles 313 and 314 of the Treaty on the Functioning of the European Union (TFEU).

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

6. The European Parliament and the Council shall adopt the establishment plan referred to in point (l) of Article 13(3).

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

Article 26

Presentation of the Competence Centre's accounts and discharge

The presentation of the Competence Centre's provisional and final accounts and the discharge shall comply with the rules and timetable of the Financial Regulation and of the financial rules of the Competence Centre.

Article 27

Operational and financial reporting

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

2. Within two months of the end of each financial year, the Executive Director shall submit to the Governing Board for approval an annual activity report on the progress made by the Competence Centre in the previous calendar year, in particular in relation to the annual work programme for that year and the fulfilment of its strategic goals and priorities. That report shall include 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) the fulfilment of the mission and objectives laid down in this Regulation and proposals for further necessary work to fulfil that mission and those objectives;

(e) the consistency of the implementation tasks with the Agenda and the multiannual work programme.

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

Article 28

Financial rules

The Competence Centre shall adopt its specific financial rules in accordance with Article 70 of the Financial Regulation.

Article 29

Protection of financial interests of the Union

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 penalties.

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

3. 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 ([17]) and Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council ([18]) 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, contracts and grant agreements resulting from the implementation of this Regulation shall contain provisions expressly empowering the Commission, the Competence Centre, the Court of Auditors and OLAF to conduct such audits and investigations in accordance with their respective competences. Where the implementation of an action is outsourced or sub-delegated, in whole or in part, or where it requires the award of a procurement contract or financial support to a third party, the contract or grant agreement shall include the contractor's or beneficiary's obligation to impose on any third party involved explicit acceptance of those powers of the Commission, the Competence Centre, the Court of Auditors and OLAF.

CHAPTER IV

Competence Centre staff

Article 30

Staff

1. The Staff Regulations and Conditions of Employment and the rules adopted jointly by the institutions of the Union for the purpose of applying the Staff Regulations and Conditions of Employment shall apply to the staff of the Competence Centre.

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

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

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

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

6. The staff resources shall be determined in the establishment plan referred to in point (l) of Article 13(3), indicating the number of temporary posts by function group and by grade and the number of contract staff expressed in full-time equivalents, in line with the annual budget of the Competence Centre.

7. The human resources required by the Competence Centre shall be met in the first instance by redeployment of staff or posts from Union institutions, bodies, offices and agencies, and additional human resources through recruitment. The staff of the Competence Centre may consist of temporary staff and contract staff.

([17]) 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).

([18]) 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).

8. All costs related to staff shall be borne by the Competence Centre.

Article 31

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 32

Privileges and immunities

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

CHAPTER V

Common provisions

Article 33

Security rules

1. Article 12 Regulation (EU) 2021/694 shall apply to participation in all actions funded by the Competence Centre.

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

(a) for the purposes of Article 38(1) of Regulation (EU) 2021/695, when provided for in the annual work programme, the grant of non-exclusive licences may be limited to third parties that are established or deemed to be established in a Member State and are controlled by that Member State or by nationals of that Member State;

(b) for the purposes of point (b) of the first subparagraph of Article 40(4) of Regulation (EU) 2021/695, the transfer or license to a legal entity established in an associated country or established in the Union but controlled from third countries shall be grounds for objecting to transfers of ownership of results or to grants of an exclusive license regarding results;

(c) for the purposes of point (a) of the first subparagraph of Article 41(7) of Regulation (EU) 2021/695, when provided for in the annual work programme, the granting of access rights, as defined in point (9) of Article 2 of that Regulation, may be limited to a legal entity that is established or deemed to be established in a Member State and is controlled by that Member State or by nationals of that Member State.

Article 34

Transparency

1. The Competence Centre shall carry out its activities with a high level of transparency.

2. The Competence Centre shall ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information in a timely manner, in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Article 43. Those requirements shall also apply to the national coordination centres, the Community and the Strategic Advisory Group in accordance with relevant law.

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 the rules of procedure of the Governing Board of the Competence Centre and of the Strategic Advisory Group the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2 of this Article. For actions funded by Horizon Europe, those rules and arrangements shall take account of Regulation (EU) 2021/695.

Article 35

Gender balance

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

Article 36

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

1. After approval by the Commission, the Governing Board shall adopt the security rules of the Competence Centre. Those security rules shall apply the security principles and rules laid down in Commission Decisions (EU, Euratom) 2015/443 ([19]) and (EU, Euratom) 2015/444 ([20]).

2. Members of the Governing Board, the Executive Director, external experts participating in ad hoc working groups, and members of the staff of the Competence Centre shall comply with the confidentiality requirements under Article 339 TFEU, even after their duties have ceased.

3. The Competence Centre may take the 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 institutions, bodies, offices and agencies. Any administrative arrangements concluded to that end with regard to the sharing of EU classified information (EUCI) or, in the absence of such arrangements, any exceptional ad hoc release of EUCI, shall have received the Commission's prior approval.

Article 37

Access to documents

1. Regulation (EC) No 1049/2001 shall apply to documents held by the Competence Centre.

2. The Governing Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001 by 29 December 2021.

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 TFEU or of an action before the Court of Justice of the European Union under Article 263 TFEU.

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 the implementation and results of the Union funding programmes referred to in point (b) of Article 4(3) are collected efficiently, effectively, and in a timely manner, and shall impose proportionate reporting requirements on recipients of Union funds and Member States. The conclusions of that evaluation shall be made public.

2. Once there is sufficient information available about the implementation of this Regulation, and in any event no later than 30 months after the date provided for in Article 46(4), the Commission shall prepare an implementation report on the activities of the Competence Centre, taking into account the preliminary input of the Governing Board, the national coordination centres and the Community. The Commission shall submit that implementation report to the European Parliament and to the Council by 30 June 2024. The Competence Centre and Member States shall provide the Commission with the information necessary for the preparation of that report.

3. The implementation report referred to in paragraph 2 shall include assessments of:

(a) the working capacity of the Competence Centre with regard to its mission, objectives, mandate and tasks and the cooperation and coordination with other stakeholders, in particular the national coordination centres, the Community and ENISA;

([19]) Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).
([20]) 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).

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

(c) the consistency of implementation tasks with the Agenda and the multiannual work programme;

(d) the coordination and cooperation of the Competence Centre with the Programme Committees of Horizon Europe and the Digital Europe Programme, in particular with a view to increasing consistency and synergies with the Agenda, the annual work programme, the multiannual work programme, Horizon Europe and the Digital Europe Programme;

(e) joint actions.

4. After submission of the implementation report referred to in paragraph 2 of this Article, the Commission shall carry out an evaluation of the Competence Centre, taking into account the preliminary input from the Governing Board, the national coordination centres and the Community. That evaluation shall refer to or update, as necessary, the assessments referred to in paragraph 3 of this Article and shall be carried out before expiry of the period specified in Article 47(1), in order to determine in a timely manner whether it is appropriate to extend the duration of the mandate of the Competence Centre beyond that period. That evaluation shall assess legal and administrative aspects regarding the mandate of the Competence Centre and the potential to create synergies and avoid fragmentation with other Union institutions, bodies, offices and agencies.

If the Commission considers that the continuation of the Competence Centre is justified with regard to its mission, objectives, mandate and tasks, it may make a legislative proposal to extend the duration of the mandate of the Competence Centre set out in Article 47.

5. On the basis of the conclusions of the implementation report referred to in paragraph 2, the Commission may take appropriate actions.

6. The monitoring, evaluation, phasing out and renewal of the contribution from Horizon Europe shall be carried out in accordance with Articles 10, 50 and 52 of Regulation (EU) 2021/695 and agreed implementation arrangements.

7. The monitoring, reporting and evaluation of the contribution from the Digital Europe Programme shall be carried out in accordance with Articles 24 and 25 of Regulation (EU) 2021/694.

8. In the event of a winding-up of the Competence Centre, the Commission shall conduct a final evaluation of the Competence Centre within six months of the winding-up of the Competence Centre, and in any event no later than two years after the triggering of the winding-up procedure referred to in Article 47. The results of that final evaluation shall be submitted to the European Parliament and to the Council.

Article 39

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 party to legal proceedings.

Article 40

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 make good any damage caused by its staff in the performance of their duties, in accordance with the general principles common to the laws of the Member States.

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 41

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

1. The Court of Justice of the European Union shall have jurisdiction:

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

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

(c) in any dispute between the Competence Centre and its staff within the limits of and under the conditions laid down in the Staff Regulations.

2. Regarding any matter not covered by this Regulation or by other legal acts of the Union, the law of the Member State where the seat of the Competence Centre is located shall apply.

Article 42

Liability of the Union and the Member States and insurance

1. The financial liability of the Union and the Member States 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 43

Conflicts of interest

The Governing Board shall adopt rules for the prevention, identification and resolution of conflicts of interest in respect of its members, bodies and staff, including the Executive Director. Those rules shall contain the provisions intended to avoid a conflict of interest in respect of the representatives of the members serving in the Governing Board as well as the Strategic Advisory Group, in accordance with the Financial Regulation, including provisions on any declarations of interest. The national coordination centres shall be subject to national law with regard to conflicts of interest.

Article 44

Protection of Personal Data

1. The processing of personal data by the Competence Centre shall be subject to Regulation (EU) 2018/1725.

2. The Governing Board shall adopt implementing measures as referred to in Article 45(3) of Regulation (EU) 2018/1725. The Governing Board may adopt additional measures necessary for the application of that Regulation by the Competence Centre.

Article 45

Support from the host Member State

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

CHAPTER VI

Final provisions

Article 46

Initial actions

1. The Commission shall be responsible for the establishment and initial operation of the Competence Centre until it has the operational capacity to implement its own budget. The Commission shall carry out, in accordance with Union law, all necessary actions with the involvement of the competent bodies of the Competence Centre.

2. For the purpose of paragraph 1 of this Article, the Commission may designate an interim Executive Director until the Executive Director takes up his or her duties following his or her appointment by the Governing Board in accordance with Article 16. The interim Executive Director shall exercise the duties of the Executive Director and may be assisted by a limited number of members of staff of the Commission. The Commission may assign a limited number of its members of staff to the Competence Centre 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 it has been adopted by the Governing Board and may conclude agreements and contracts, including staff contracts, and adopt decisions, following the adoption of the establishment plan referred to in point (l) of Article 13(3).

4. The interim Executive Director shall determine, in common accord with the Executive Director and subject to the approval of the Governing Board, the date from 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 47

Duration

1. The Competence Centre shall be established for the period from 28 June 2021 to 31 December 2029.

2. Unless the mandate of the Competence Centre is extended in accordance with Article 38(4), the winding-up procedure shall be triggered automatically at the end of the period referred to in paragraph 1 of this Article.

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

Article 48

Entry into force

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

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

Done at Brussels, 20 May 2021.

For the European Parliament	*For the Council*
The President	*The President*
D.M. SASSOLI	A.P. ZACARIAS