



Council of the
European Union

Brussels, 26 October 2020
(OR. en)

12293/20

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

LIMITE

**CYBER 200
TELECOM 195
COPEN 292
CODEC 1058
COPS 351
COSI 160
CSC 276
CSCI 65
IND 190
RECH 419
ESPACE 57**

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	8625/20, 9745/20, 10781/20, 11234/20
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres: four column document

Delegations will find attached the four column document regarding the above-mentioned Regulation as it results from the technical meetings held on 9 and 21 October 2020.

Regulation establishing the European Cybersecurity Competence Centre and the Network of Coordination Centres
2018/0328(COD)
Version [Version for trilogue on 29 Oct 2020]
25-10-2020 at 19h27

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Formula				
G 1	2018/0328 (COD)	2018/0328 (COD)	2018/0328 (COD)	2018/0328 (COD) Text Origin: Commission Proposal
Proposal Title				
Y 2	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018 use of 'Competence' Text Origin: EP Mandate

Formula				
G	3	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, Text Origin: Commission Proposal
Citation 1				
G	4	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 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 Treaty on the Functioning of the European Union, and in particular Article 173(3) and the first paragraph of Article 188 thereof, Text Origin: Commission Proposal
Citation 2				
G	5	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission,	Having regard to the proposal from the European Commission, Text Origin: Commission Proposal

Citation 3				
6	Having regard to the opinion of the European Economic and Social Committee ¹ , <u>1. OJ C</u> , p. .	Having regard to the opinion of the European Economic and Social Committee ¹ , <u>1. OJ C</u> , p. .	Having regard to the opinion of the European Economic and Social Committee ¹ , <u>1. OJ C</u> , <u>p.</u> .	Having regard to the opinion of the European Economic and Social Committee ¹ , <u>1. OJ C</u> , p. . Text Origin: Commission Proposal
Citation 4				
7	Having regard to the opinion of the Committee of the Regions ¹ , <u>1. OJ C</u> , , p. .	Having regard to the opinion of the Committee of the Regions ¹ , <u>1. OJ C</u> , , p. .	Having regard to the opinion of the Committee of the Regions ¹ , <u>1. OJ C</u> , , p. .	Deleted
Citation 5				
8	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure,	Acting in accordance with the ordinary legislative procedure, Text Origin: Commission Proposal
Formula				
9	Whereas:	Whereas:	Whereas:	Whereas: Text Origin: Commission Proposal

Recital 1				
Y	10	<p>(1) Our daily lives and economies become increasingly dependent on digital technologies, citizens become more and more exposed to serious cyber incidents. Future security depends, among others, on enhancing technological and industrial ability to protect the Union against cyber threats, as both civilian infrastructure and military capacities rely on secure digital systems.</p>	<p>(1) Our <u>More than 80 % of the population of the Union is connected to the internet and our</u> daily lives and economies <u>are becoming</u> become increasingly dependent on digital technologies, citizens become <u>with citizens becoming</u> more and more exposed to serious cyber incidents. Future security depends, among others, on <u>contributing to overall resilience, on enhancing technological and industrial ability to protect the Union against constantly evolving</u> cyber threats, as both civilian infrastructure and military <u>security</u> capacities rely on secure digital systems. <u>Such security can be achieved by raising the awareness for cybersecurity threats, by developing competences, capacities, capabilities throughout the Union, thoroughly taking into account the interplay of hardware and software infrastructure, networks, products and processes, and the societal and ethical implications and concerns.</u></p>	<p>(1) Our daily lives and economies become <u>are becoming</u> increasingly dependent on digital technologies, <u>and</u> citizens become more and more exposed to serious cyber incidents. Future security depends, among others <u>other things</u>, on enhancing technological and industrial ability to protect the Union against cyber threats, as both civilian infrastructure and military capacities rely on secure digital systems.</p> <p>EP to make new proposal, merger with recital 10a. "awareness" to be put in square brackets (link recital 60a)</p>

Recital 1a						
Y	10a	<p><u><i>(1a) Cybercrime is a fast growing threat to the Union, its citizens and its economy. In 2017, 80 % of the European companies experienced at least one cyber incident. The Wannacry-attack in May 2017 affected more than 150 countries and 230 000 IT-systems and had significant impacts on critical infrastructures, such as hospitals. This underlines the necessity for the highest cybersecurity standards and holistic cybersecurity solutions, involving people, products, processes and technology in the Union, as well as for the Union's leadership in the matter, and for digital autonomy.</i></u></p>		<p>EP to make new proposal, merger with recital 10. "Cybercrime" possibly replaced by "Cyber incidents" Deletion of sentences with data</p>	Y	
Recital 2						
G	11	<p>(2) The Union has steadily increased its activities to address growing cybersecurity challenges following the 2013 Cybersecurity Strategy¹ aimed to foster a reliable, safe, and open cyber ecosystem. In 2016 the Union adopted the first measures in the area of cybersecurity through Directive (EU) 2016/1148 of the European Parliament and of the Council² on security of network and information systems.</p> <p>1. Joint Communication to the European Parliament and the Council:: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013) 1 final.</p> <p>2. Directive (EU) 2016/1148 of the European Parliament and of the Council of</p>	<p>(2) The Union has steadily increased its activities to address growing cybersecurity challenges following the 2013 Cybersecurity Strategy¹ aimed to foster a reliable, safe, and open cyber ecosystem. In 2016 the Union adopted the first measures in the area of cybersecurity through Directive (EU) 2016/1148 of the European Parliament and of the Council² on security of network and information systems.</p> <p>1. Joint Communication to the European Parliament and the Council:: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013) 1 final.</p> <p>2. Directive (EU) 2016/1148 of the European Parliament and of the Council of</p>	<p>(2) The Union has steadily increased its activities to address growing cybersecurity challenges following the <u>Cybersecurity Strategy put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy ("High Representative") in their Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" ("the 2013 Cybersecurity Strategy"</u>). <u>The 2013 Cybersecurity Strategy</u> aimed to foster a reliable, safe, and open cyber ecosystem. In 2016 the Union adopted the first measures in the</p>	<p>(2) The Union has steadily increased its activities to address growing cybersecurity challenges following the <u>Cybersecurity Strategy put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy ("High Representative") in their Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" ("the 2013 Cybersecurity Strategy"</u>). <u>The 2013 Cybersecurity Strategy</u> aimed to foster a reliable, safe, and open cyber ecosystem. In 2016 the Union adopted the first measures in the</p>	G

	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).	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).	area of cybersecurity through Directive (EU) 2016/1148 of the European Parliament and of the Council ^{2L} on security of network and information systems. 1. Joint Communication to [1] Directive (EU) 2016/1148 of the European Parliament and of the Council Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013)-I final of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1). 2. 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).	area of cybersecurity through Directive (EU) 2016/1148 of the European Parliament and of the Council ^{2L} on security of network and information systems. 1. Joint Communication to [1] Directive (EU) 2016/1148 of the European Parliament and of the Council Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013)-I final of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1). 2. 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). reference to be updated in case of a new Cybersecurity Strategy Text Origin: Council Mandate
--	--	--	--	---

Recital 3				
G	12	<p>(3) In September 2017, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a Joint Communication¹ on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" to further reinforce the Union's resilience, deterrence and response to cyber-attacks.</p> <p>1. Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017) 450 final.</p>	<p>(3) In September 2017, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a Joint Communication¹ on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" to further reinforce the Union's resilience, deterrence and response to cyber-attacks.</p> <p>1. Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017) 450 final.</p>	<p>(3) In September 2017, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a Joint Communication¹ on <u>presented a Joint Communication to the European Parliament and the Council entitled</u> "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" to further reinforce the Union's resilience, deterrence and response to cyber-attacks.</p> <p>1. Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017) 450 final.</p> <p>Text Origin: Council Mandate</p>
Recital 4				
Y	13	<p>(4) The Heads of State and Government at the Tallinn Digital Summit, in September 2017, called for the Union to become "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."</p>	<p>(4) The Heads of State and Government at the Tallinn Digital Summit, in September 2017, called for the Union to become "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free, <u>safer</u> and law-governed internet-"<u>"</u>, and <u>declared to "make more use of open source solutions and/or open standards when (re)building Information and Communication Technology (ICT) systems and solutions (among else, to avoid vendor lock-ins), including those</u></p>	<p>(4) The Heads of State and Government at the Tallinn Digital Summit, in September 2017, called for the Union to become "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free, <u>safer</u> and law-governed internet-"<u>"</u>, and <u>declared to "make more use of open source solutions and/or open standards when (re)building Information and Communication Technology (ICT) systems and solutions (among else, to avoid vendor lock-ins), including those</u></p>

		<u><i>developed and/or promoted by EU programmes for interoperability and standardisation, such as ISA².</i></u>		<u><i>developed and/or promoted by EU programmes for interoperability and standardisation, such as ISA².</i></u> Proivisional OK. Council to check with MS Text Origin: EP Mandate
	Recital 4a			
Y	13a	<u><i>(4a) The European Cybersecurity Industrial, Technology and Research Competence Centre (the 'Competence Centre') should help to increase the resilience and reliability of the infrastructure of network and information systems, including the internet and other critical infrastructure for the functioning of society such as transport, health, and banking systems.</i></u>		COM to propose new text
	Recital 4b			
Y	13b	<u><i>(4b) The Competence Centre and its actions should take into account the implementation of Regulation (EU) 2019/XXX [recast of Regulation (EC) No 428/2009 as proposed by COM(2016)0616]¹.</i></u> <u><i>1. Regulation (EU) 2019/... of the European Parliament and of the Council of ... setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (OJ L ..., ..., p. ...).</i></u>		Possible deletion: EP to check

Recital 5						
Y	14	<p>(5) Substantial disruption of network and information systems can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market. At the moment, the Union depends on non-European cybersecurity providers. However, it is in the Union's strategic interest to ensure that it retains and develops essential cybersecurity technological capacities to secure its Digital Single Market, and in particular to protect critical networks and information systems and to provide key cybersecurity services.</p>	<p>(5) Substantial disruption of network and information systems can affect individual Member States and the Union as a whole. The <u>highest level of</u> security of network and information systems <u>throughout the Union</u> is therefore essential for the smooth functioning of the internal market <u>society and economy alike</u>. At the moment, the Union depends on non-European cybersecurity providers. However, it is in the Union's strategic interest to ensure that it retains and develops essential cybersecurity technological capacities <u>and capabilities</u> to secure <u>the protection of data and critical networks and information systems of European citizens and companies, including its Digital Single Market, and in particular to protect critical networks and information systems</u><u>infrastructures for the functioning of society such as transport systems, health systems and banking, and the Digital Single Market</u>, and to provide key cybersecurity services.</p>	<p>(5) Substantial disruption of network and information systems can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market. At the moment, the Union depends on non-European cybersecurity providers. However, it is in the Union's strategic interest to ensure that it retains and develops essential cybersecurity <u>research and</u> technological capacities to secure its Digital Single Market <u>as outlined by the Commission in its Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled "A Digital Single Market Strategy for Europe"</u>, and in particular to protect critical networks<u>network</u> and information systems and to provide key cybersecurity services.</p> <p>COM to propose new text Council reluctant on reference to "protection of data", which should be in square brackets. Wording "highest level" and deletion of reference to "the smooth functioning of the internal market" to be examined.</p>	Y	
Recital 6						
Y	15	<p>(6) A wealth of expertise and experience in cybersecurity research, technology and industrial development exists in the Union but the efforts of industrial and research communities are fragmented, lacking alignment and a common mission, which hinders competitiveness in this domain. These efforts and expertise need to be pooled, networked and used in an efficient</p>	<p>(6) A wealth of expertise and experience in cybersecurity research, technology and industrial development exists in the Union but the efforts of industrial and research communities are fragmented, lacking alignment and a common mission, which hinders competitiveness <u>and effective protection of critical data, networks and systems</u> in this domain. These efforts and</p>	<p>(6) A wealth of expertise and experience in cybersecurity research, technology and industrial development exists in the Union, but the efforts of industrial and research communities are fragmented, lacking alignment and a common mission, which hinders competitiveness in this domain. These efforts and expertise need to be pooled, networked and used in an efficient</p>	<p>(6) A wealth of expertise and experience in cybersecurity research, technology and industrial development exists in the Union but the efforts of industrial and research communities are fragmented, lacking alignment and a common mission, which hinders competitiveness <u>and effective protection of [critical data], networks and systems</u> in this domain. These efforts and</p>	Y

	manner to reinforce and complement existing research, technology and industrial capacities at Union and national levels.	expertise need to be pooled, networked and used in an efficient manner to reinforce and complement existing research, technology, <u>skills</u> and industrial capacities at Union and national levels. <u>Whereas ICT sector faces important challenges, such as fulfilling its demand for skilled workers, it can benefit from representing the diversity of society at large, and from achieving a balanced representation of genders, ethnic diversity, and non-discrimination against disabled persons, as well as from facilitating the access to knowledge and training for future cybersecurity experts, including their education in non-formal contexts, for example in Free and Open Source Software projects, civic tech projects, start-ups and microenterprises.</u>	manner to reinforce and complement existing research, technology and industrial capacities at Union and national levels.	expertise need to be pooled, networked and used in an efficient manner to reinforce and complement existing research, technology, <u>skills</u> and industrial capacities at Union and national levels. <u>Whereas ICT sector faces important challenges, such as fulfilling its demand for skilled workers, it can benefit from representing the diversity of society at large, and from achieving a balanced representation of genders, ethnic diversity, and non-discrimination against disabled persons, as well as from facilitating the access to knowledge and training for future cybersecurity experts, including their education in non-formal contexts, for example in Free and Open Source Software projects, civic tech projects, start-ups and microenterprises.</u>
Recital 6a				
15a		<u>(6a) Small and medium-sized enterprises (SMEs) are crucial actors in the Union's cybersecurity sector, which can provide cutting-edge solutions due to their agility. SMEs that are not specialised in cybersecurity are, however, also prone to be more vulnerable to cyber incidents due to high investment and knowledge requirements to establish effective cybersecurity solutions. It is therefore necessary that the Competence Centre and the Cybersecurity Competence Network (the 'Network') provide special support for SMEs by facilitating their access to knowledge and training in order</u>		<u>(6a) Small and medium-sized enterprises (SMEs) are crucial actors in the Union's cybersecurity sector, which can provide cutting-edge solutions due to their agility. SMEs that are not specialised in cybersecurity are, however, also prone to be more vulnerable to cyber incidents due to high investment and knowledge requirements to establish effective cybersecurity solutions. It is therefore necessary that the Competence Centre and the Cybersecurity Competence Network (the 'Network') provide special support for SMEs by facilitating their access to knowledge and training in order</u>

Council to check EP text.
"Data" in square brackets.

Text Origin: EP Mandate

		<u>to allow them to secure themselves sufficiently and to allow those who are active in cybersecurity to contribute to the Union's leadership in the field.</u>		<u>to allow them to secure themselves sufficiently and to allow those who are active in cybersecurity to contribute to the Union's leadership in the field.</u> Council to check EP text. Wording last sentence too prescriptive. Text Origin: EP Mandate
Recital 6b				
Y	15b	<u>(6b) Expertise exists beyond industrial and research contexts. Non-commercial and pre-commercial projects, referred to as “civic tech” projects, make use of open standards, Open Data, and Free and Open Source Software, in the interest of society and the public good. They contribute to the resilience, awareness and development of competence in cybersecurity matters and play an important role in building capacities for industry and research in the field.</u>		<u>(6b) [Expertise exists beyond industrial and research contexts. Non-commercial and pre-commercial projects, referred to as “civic tech” projects, make use of open standards, Open Data, and Free and Open Source Software, in the interest of society and the public good]</u> To be included in a compatible recital Text Origin: EP Mandate
Recital 6c				
Y	15c	<u>(6c) The term ‘stakeholders’, when used in the context of this Regulation, refers to, inter alia, industry, public entities and other entities which deal with operational and technical matters in the area of cybersecurity, as well as to civil society, inter alia trade unions, consumer associations, the Free and Open Source Software community, and the academic and research community.</u>		Council reluctant. EP to propose new text.

	Recital 7					
Y	16	(7) The Council Conclusions adopted in November 2017 called on the Commission to provide rapidly an impact assessment on the possible options to create a network of cybersecurity competence centres with the European Research and Competence Centre and propose by mid-2018 the relevant legal instrument.	(7) The Council Conclusions adopted in November 2017 called on the Commission to provide rapidly an impact assessment on the possible options to create a network of cybersecurity competence centres with the European Research and Competence Centre and propose by mid-2018 the relevant legal instrument.	(7) The Council Conclusions adopted in November 2017 called on the Commission to provide rapidly an impact assessment on the possible options to create a Network of Cybersecurity Competence Centres, <u>together with a</u> with the European <u>Cybersecurity</u> Research and Competence Centre and propose by mid-2018 the relevant legal instrument.	(7) The Council Conclusions adopted in November 2017 called on the Commission to provide rapidly an impact assessment on the possible options to create a Network of Cybersecurity Competence Centres, <u>together with a</u> with the European <u>Cybersecurity</u> Research and Competence Centre and propose by mid-2018 the relevant legal instrument. use of 'Competence' Text Origin: Council Mandate	Y
	Recital 7a					
G	16a			<u>(7a) The Union still lacks sufficient technological and industrial capacities and capabilities to autonomously secure its economy and critical infrastructures and to become a global leader in cybersecurity field. There is an insufficient level of strategic and sustainable coordination and cooperation between industries, cybersecurity research communities and governments; the EU suffers from subscale investment and limited access to cybersecurity know- how, skills and facilities across Europe; and few European cybersecurity research and innovation outcomes are translated into marketable solutions and widely deployed across the economy.</u>	<u>(7a) The Union still lacks sufficient technological and industrial capacities and capabilities to autonomously secure its economy and critical infrastructures and to become a global leader in cybersecurity field. There is an insufficient level of strategic and sustainable coordination and cooperation between industries, cybersecurity research communities and governments; the EU suffers from subscale investment and limited access to cybersecurity know- how, skills and facilities across Europe; and few European cybersecurity research and innovation outcomes are translated into marketable solutions and widely deployed across the economy.</u> Text Origin: Council Mandate	G

Recital 7b						
Y	16b		<p><u>(7b) The option of creating a network of national coordination centres, together with a European Cybersecurity Industrial, Technology and Research Centre, with a dual mandate to pursue measures in support of industrial technologies, as well as in the domain of research and innovation, is best suited to achieve the goals of this Regulation, while offering the highest economic, societal, and environmental impact and safeguarding the Union's interests.</u></p>	<p><u>(7b) The option of creating a network of national coordination centres, together with a European Cybersecurity Industrial, Technology and Research Centre, with a [dual] mandate to pursue measures in support of industrial technologies, as well as in the domain of research and innovation, is best suited to achieve the goals of this Regulation, while offering the highest economic, societal, and environmental impact and safeguarding the Union's interests.</u></p> <p>word "dual" in square brackets: EP to check</p> <p>use of 'Competence'</p> <p>Text Origin: Council Mandate</p>	Y	
Recital 8						
Y	17	<p>(8) The Competence Centre should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with the Cybersecurity Competence Network. It should deliver cybersecurity-related financial support from the Horizon Europe and Digital Europe programmes, and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to cybersecurity research, innovation, technology and industrial development and avoiding duplication.</p>	<p>(8) The Competence Centre should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with the Cybersecurity Competence Network. It should deliver cybersecurity-related financial support from the Horizon Europe and Digital Europe programmes, <u>as well as from the European Defence Fund for actions and administrative costs related to defence</u>, and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial</p>	<p>(8) The Competence Centre should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with <u>a Network of National Coordination Centre ("the the Cybersecurity Competence</u> Network"). <u>The Centre</u> it should deliver cybersecurity-related financial support from <u>Horizon Europe - the Framework Programme for Research and Innovation established by Regulation 2020/... of the European Parliament and of the Council</u> ('<u>the the Horizon Europe programme</u>') <u>and the and Digital Europe programmes</u> <u>programme established by</u></p>	<p>(8) The Competence Centre should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with <u>a Network of National Coordination Centre ("the the Cybersecurity Competence</u> Network"). <u>The Centre</u> it should deliver cybersecurity-related financial support from <u>Horizon Europe - the Framework Programme for Research and Innovation established by Regulation 2020/... of the European Parliament and of the Council</u> ('<u>the the Horizon Europe programme</u>') <u>and the and Digital Europe programmes</u> <u>programme established by</u></p>	Y

		<p>support related to <u>Union initiatives in the field of</u> cybersecurity research <u>and development</u>, innovation, technology and industrial development and avoiding duplication.</p>	<p><u>Regulation 2020/... of the European Parliament and of the Council² ('the Digital Europe programme</u> and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial^{fin}'), ancial support related to cybersecurity research, innovation, technology and industrial development and avoiding <u>unnecessary</u> duplication.</p> <p><u>1. Regulation 2020/... of the European Parliament and of the Council, of establishing Horizon Europe - the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination (OJ ...) [2018/0224(COD)]</u>.</p> <p><u>2. Regulation 2020/... of the European Parliament and of the Council, of establishing the Digital Europe programme for the period 2021-2027 (OJ ...) [2018/0227(COD)]</u>.</p>	<p><u>Regulation 2020/... of the European Parliament and of the Council² ('the Digital Europe programme)</u> [as well as <u>from the European Defence Fund for actions and administrative costs related to defence]</u> and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to <u>Union initiatives in the field of</u> cybersecurity research <u>and development</u>, innovation, technology and industrial development and avoiding <u>unnecessary</u> duplication.</p> <p><u>1. Regulation 2020/... of the European Parliament and of the Council, of establishing Horizon Europe - the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination (OJ ...) [2018/0224(COD)]</u>.</p> <p><u>2. Regulation 2020/... of the European Parliament and of the Council, of establishing the Digital Europe programme for the period 2021-2027 (OJ ...) [2018/0227(COD)]</u>.</p> <p>merger EP - Council text. Reference to Defence in square brackets</p> <p>use of 'Competence' Defence/dual use aspect</p> <p>Text Origin: Council Mandate</p>
--	--	---	--	---

Recital 8a				
Y	17a		<p><u>(8a) The Centre should not play an operational role nor provide operational technical assistance. Upon request from a Member State the Centre, within the scope of its mandate, should be able to provide expert cybersecurity industrial, technological, and research advice to that Member State.</u></p>	<p><u>(8a) The Competence Centre should not carry out operational cybersecurity tasks, such as tasks associated with Computer Security Incident Response Teams (CSIRTs), including monitoring and responding to Cybersecurity incidents. [However, the Competence Centre could acquire and operate cyber security infrastructures at the service of industries, in particular SMEs, research communities, civil society, and the public sector in line with the mission and objectives laid down in this Regulation.]</u></p> <p>Council to check with MS</p> <p>Concrete formulation to be in line with 63g, 87aa</p>
Recital 8a				
Y	17b		<p><u>(8a) “Security by design” as a principle established in Commission Joint Communication of 13 September 2017 entitled “Resilience, Deterrence and Defence: Building strong cybersecurity for the EU” includes state-of-the-art methods by which to increase security, at all stages of the lifecycle of a product or service, starting with secure design and development methods, reducing the attack surface, and incorporating adequate security testing and security audits. For the duration of operation and maintenance, producers or providers need to make available updates remedying new</u></p>	<p>EP to provide new text</p>

		<u>vulnerabilities or threats without delay, for the estimated lifetime of a product and beyond. This can also be achieved by enabling third parties to create and provide such updates. The provision of updates is especially necessary in the case of commonly used infrastructures, products and processes.</u>		
Recital 8aa				
Y	17c		<p><u>(8aa) The Centre would benefit from the experience and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity between the Commission and European Cyber Security Organisation ECSO Association during the duration of the Framework Programme for Research and Innovation (2014-2020) ("Horizon 2020"), established by Regulation (EU) No 1291/2013 of the European Parliament and of the Council¹, and the lessons learned from four pilot projects² launched in early 2019 under Horizon 2020, for the management of the Cybersecurity Competence Community, and the representation of the Cybersecurity Competence Community in the Centre.</u></p> <p><u>1. 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).</u></p> <p><u>2. CONCORDIA, ECHO, SPARTA and CyberSec4Europe are the four winning</u></p>	COM to provide new text

			<u>pilot projects of the 2018 Horizon 2020 cybersecurity call "establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap".</u>	
	Recital 8b			
Y	17d		<u>(8b) In view of the extent of the cybersecurity challenge and in view of the investments made in cybersecurity capacities and capabilities in other parts of the world, the Union and its Member States should step up their financial support to research, development and deployment in this area. In order to realise economies of scale and achieve a comparable level of protection across the union, the Member States should put their efforts into a European framework by investing through the Competence Centre mechanism where relevant.</u>	Council sceptical, to check with MS.

Recital 8c				
Y	17e		<p><u>(8c) The Competence Centre and the Cybersecurity Competence Community should, in order to foster the Union's competitiveness and the highest cybersecurity standards internationally, seek the exchange on cybersecurity products and processes, standards and technical standards with the international community. Technical standards include the creation of reference implementations, published under open standard licences. The secure design of, in particular, reference implementations is crucial for the overall reliability and resilience of commonly used network and information system infrastructure like the internet and critical infrastructures.</u></p>	<p>Council sceptical, to check with MS.</p>
Recital 9				
Y	18	<p>(9) Taking into account that the objectives of this initiative can be best achieved if all Member States or as many Member States as possible participate, and as an incentive for Member States to take part, only Member States who contribute financially to the administrative and operational costs of the Competence Centre should hold voting rights.</p>	<p>(9) Taking into account that the objectives of this initiative can be best achieved if all Member States or as many Member States as possible participate <u>contribute</u>, and as an incentive for Member States to take part, only Member States who contribute financially to the administrative and operational costs of the Competence Centre should hold voting rights.</p>	<p>(9) Taking into account that the objectives of this initiative can be best achieved if all Member States or as many Member States as possible participate, and as an incentive for Member States to take part, only Member States who contribute financially to the administrative and operational costs <u>The Centre would benefit from the experience and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity between the Commission and European Cyber Security Organisation ECSO Association during the duration of the Framework Programme for Research and Innovation</u></p> <p>To be rediscussed depending outcome voting/financing.</p> <p>Link voting/financing</p>

(2014-2020) ("Horizon 2020"), established by Regulation (EU) No 1291/2013 of the European Parliament and of the Council¹, and the lessons learned from four pilot projects² launched in early 2019 under Horizon 2020, for the management of the Cybersecurity Competence ~~Centre should hold voting rights~~ Community, and the representation of the Cybersecurity Competence Community in the Centre.

1. 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).

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

Recital 9a					
Y	18a		<p><u>(9a) When the Centre is preparing its annual work programme ("annual work programme"), it should inform the Commission on its co-funding needs based on the Member States' planned co-funding contributions to joint actions, in order for the Commission to take into account the Union matching contribution in the preparation of the draft general budget for the following year.</u></p>	<p>COM new text awaited</p> <p>Link voting/financing</p>	Y
Recital 9b					
Y	18b		<p><u>(9b) Where the Commission prepares the work programme of the Horizon Europe programme for matters related to cyber security, including in the context of its stakeholder consultation process and particularly before the adoption of that work programme, the Commission should take into account the input of the Centre and share that input with the Programme Committee of the Horizon Europe programme.</u></p>	<p>COM new text awaited.</p> <p>Link voting/financing</p>	Y

Recital 9c				
Y	18c		<p><u>(9c) In order to support its role in the area of cybersecurity and the involvement of the Network and to provide a strong governance role for the Member States, the Centre should be established as a Union body with legal personality. The Centre should perform a dual role by undertaking specific tasks in the area of cybersecurity industry, technology and research as laid down in this Regulation and by managing cybersecurity related funding from several programmes at the same time – notably the Horizon Europe programme and the Digital Europe programme, and possibly even further Union programmes. Such management is to be in accordance with the rules applicable to those programmes. Nevertheless, considering that the funding for the functioning of the Centre would originate primarily from the Digital Europe programme and the Horizon Europe programme, it is necessary that the Centre is considered as a partnership for the purpose of budget implementation, including the programming phase.</u></p>	<p><u>(9c) In order to support its role in the area of cybersecurity and the involvement of the Network and to provide a strong governance role for the Member States, the Centre should be established as a Union body with legal personality. The Centre should perform a [dual] role by undertaking specific tasks in the area of cybersecurity industry, technology and research as laid down in this Regulation and by managing cybersecurity related funding from several programmes at the same time – notably the Horizon Europe programme and the Digital Europe programme, and possibly even further Union programmes. Such management is to be in accordance with the rules applicable to those programmes. Nevertheless, considering that the funding for the functioning of the Centre would originate primarily from the Digital Europe programme and the Horizon Europe programme, it is necessary that the Centre is considered as a partnership for the purpose of budget implementation, including the programming phase.</u></p> <p>reference to "dual" in square brackets.</p> <p>Text Origin: Council Mandate</p>

Recital 10				
Y	19	(10) The participating Member States' financial participation should be commensurate to the Union's financial contribution to this initiative.	(10) The participating Member States' financial participation should be commensurate to the Union's financial contribution to this initiative.	<div>deleted</div> <div>Link voting/financing</div>
Recital 11				
Y	20	(11) The Competence Centre should facilitate and help coordinate the work of the Cybersecurity Competence Network (“the Network”), made up of National Coordination Centres in each Member State. National Coordination Centres should receive direct Union financial support, including grants awarded without a call for proposals, in order to carry out activities related to this Regulation.	(11) The Competence Centre should facilitate and help coordinate the work of the Cybersecurity Competence Network (“the Network”), made up of National Coordination Centres in each Member State. National Coordination Centres should receive direct Union financial support, including grants awarded without a call for proposals, in order to carry out activities related to this Regulation.	<div>(11) The <u>Competence</u> Centre should facilitate and <u>help</u> coordinate the work of the <u>Network, which should be Cybersecurity Competence Network (“the Network”)</u>; made up of National Coordination Centres, <u>one from</u> each Member State. National Coordination Centres should receive direct Union financial support, including grants awarded without a call for proposals, in order to carry out <u>their</u> activities related to this Regulation.</div> <div>Council and EP to check "their".</div> <div>use of 'Competence'</div> <div>Text Origin: Council Mandate</div>

Recital 12				
21	<p>(12) National Coordination Centres should be selected by Member States. In addition to the necessary administrative capacity, Centres should either possess or have direct access to cybersecurity technological expertise in cybersecurity, notably in domains such as cryptography, ICT security services, intrusion detection, system security, network security, software and application security, or human and societal aspects of security and privacy. They should also have the capacity to effectively engage and coordinate with the industry, the public sector, including authorities designated pursuant to the Directive (EU) 2016/1148 of the European Parliament and of the Council¹, and the research community.</p> <p>1. 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).</p>	<p>(12) National Coordination Centres should be selected by Member States. In addition to the necessary administrative capacity, Centres should either possess or have direct access to cybersecurity technological expertise in cybersecurity, notably in domains such as cryptography, ICT security services, intrusion detection, system security, network security, software and application security, or human, <u>ethical, societal and environmental</u> and societal aspects of security and privacy. They should also have the capacity to effectively engage and coordinate with the industry, the public sector, including authorities designated pursuant to the Directive (EU) 2016/1148 of the European Parliament and of the Council¹, and the research community <u>in order to establish a continuous public-private dialogue on cybersecurity. In addition, awareness should be raised among the general public about cybersecurity through appropriate means of communication.</u></p> <p>1. 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).</p>	<p>(12) National Coordination Centres should be selected by Member States. In addition to the necessary <u>public sector entities, or entities with a majority of public participation, performing public administrative</u> capacity, Centres <u>functions under national law, including by means of delegation, and they</u> should either possess or have direct access to cybersecurity technological expertise in cybersecurity, notably in domains such as cryptography, ICT security services, intrusion detection, system security, network security, software and application security <u>be selected by Member States. The functions of a National Coordination Centre in a given Member State can be carried out by an entity that carries out other functions arising under Union law, such as those of a national competent authority, a single point of contact in the meaning of Directive (EU) 2016/1148, any other EU Regulation, or a digital innovation hub in the meaning of the Digital Europe programme. Other-or</u> human and societal aspects of security and privacy. They should also have the capacity to effectively engage and coordinate with the industry, the public sector, including authorities designated pursuant to the Directive (EU) 2016/1148 of the European Parliament and of the Council¹, and the research community <u>entities or entities performing public administrative functions in a Member State could assist the National Coordination Centre in that Member</u></p>	

			<p><u>State, in carrying out its functions.</u></p> <p>1. 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).</p>	
Recital 12a				
21a			<p><u>(12a) The National Coordination Centres should have the necessary administrative capacity and should possess or have access to cybersecurity industrial, technological and research expertise and be in a position to effectively engage and coordinate with the industry, the public sector, and the research community.</u></p>	
Recital 13				
22	<p>(13) Where financial support is provided to National Coordination Centres in order to support third parties at the national level, this shall be passed on to relevant stakeholders through cascading grant agreements.</p>	<p>(13) Where financial support is provided to National Coordination Centres in order to support third parties at the national level, this shall be passed on to relevant stakeholders through cascading grant agreements.</p>	<p>(13) Where financial support is provided to National Coordination Centres <u>The National Coordination Centres may receive grants from the Centre</u> in order to <u>provide financial</u> support <u>to</u> third parties at <u>in the form of grants. The direct cost incurred by</u> the National level, this shall be passed on to relevant stakeholders through cascading grant agreements <u>Coordination Centres for the provision and administration of financial support to third parties shall be eligible for funding.</u></p>	

Recital 14				
23	<p>(14) Emerging technologies such as artificial intelligence, Internet of Things, high-performance computing (HPC) and quantum computing, blockchain and concepts such as secure digital identities create at the same time new challenges for cybersecurity as well as offer solutions. Assessing and validating the robustness of existing or future ICT systems will require testing security solutions against attacks run on HPC and quantum machines. The Competence Centre, the Network and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity solutions. At the same time the Competence Centre and the Network should be at the service of developers and operators in critical sectors such as transport, energy, health, financial, government, telecom, manufacturing, defence, and space to help them solve their cybersecurity challenges.</p>	<p>(14) Emerging technologies such as artificial intelligence, Internet of Things, high-performance computing (HPC) and quantum computing, as well as blockchain and concepts such as secure digital identities create at the same time new challenges for cybersecurity as well as offer products and processes solutions. Assessing and validating the robustness of existing or future ICT systems will require testing security products and processes solutions against attacks run on HPC and quantum machines. —The Competence Centre, the Network, <u>the European Digital Innovation Hubs</u> and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity products and processes, <u>including dual use, in particular those that help organisations to be in a constant state of building capacity, resilience and appropriate governance. The Competence Centre and the Network should stimulate the whole innovation cycle and contribute to bridging the valley of death of innovation of cybersecurity technologies and services</u> solutions. At the same time the Competence Centre, <u>the Network</u> and the Network <u>Community</u> should be at the service of developers and operators in critical sectors such as transport, energy, health, financial, government, telecom, manufacturing, defence, and space to help them solve their cybersecurity challenges, <u>and research the various motivations of attacks on the integrity of networks and information systems, such as crime,</u></p>	<p>(14) Emerging technologies such as artificial intelligence, Internet of Things, high-performance computing (HPC) and quantum computing, blockchain and concepts such as secure digital identities create <u>The Centre, the Network and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity products and solutions.</u> At the same time new challenges for cybersecurity as well as offer solutions. Assessing and validating the robustness of existing or future ICT systems will require testing security solutions against attacks run on HPC and quantum machines. The Competence Centre, the Network and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity solutions. At the same time the Competence Centre and the Network should be at the service of developers and operators in critical sectors such as transport, energy, health, financial, government, telecom, manufacturing, defence, and space to help them solve their cybersecurity <u>challenges</u> the Centre and the Network should promote the cybersecurity capability of the demand side industry, in particular by supporting developers and operators in sectors such as transport, energy, health, finance, government, telecom, manufacturing, and space to help them solve their cybersecurity <u>challenges, for example in order to achieve security-by-design. They should also support the deployment of</u></p>	<p>(14) Emerging technologies such as artificial intelligence, Internet of Things, high-performance computing (HPC) and quantum computing, blockchain and concepts such as secure digital identities create <u>The Centre, the Network and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity products and solutions.</u> At the same time new challenges for cybersecurity as well as offer solutions. Assessing and validating the robustness of existing or future ICT systems will require testing security solutions against attacks run on HPC and quantum machines. The Competence Centre, the Network and the <u>the Centre and the Network should promote the cybersecurity capability of the demand side industry, in particular by supporting developers and operators in sectors such as transport, energy, health, finance, government, telecom, manufacturing, and space to help them solve their</u> cybersecurity Competence Community should help advance and disseminate the latest cybersecurity solutions. At the same time the Competence Centre and the Network should be at the service of developers and operators in critical sectors such as transport, energy, health, financial, government, telecom, manufacturing, defence, and space to help them solve their cybersecurity <u>challenges, for example in order to achieve security-by-design. They should also support the standardisation and deployment of cybersecurity products</u></p>

		<u>industrial espionage, defamation, and disinformation.</u>	<u>cybersecurity products and solutions while promoting, where possible, the implementation of the European cybersecurity certification framework as defined by Regulation (EU) 2019/881 of the European Parliament and of the Council¹.</u> <u>1. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ 151, 7.6.2019, p. 15).</u>	<u>and solutions while promoting, where possible, the implementation of the European cybersecurity certification framework as defined by Regulation (EU) 2019/881 of the European Parliament and of the Council¹.</u> <u>(“Standardisation” added in view of EP line 80)</u> COM text proposal, not yet discussed in technical meeting
Recital 14a				
23a		<u>(14a) Due to the fast changing nature of cyber threats and cybersecurity, the Union needs to be able to adapt fast and continuously to new developments in the field. Hence, the Competence Centre, the Network and the Cybersecurity Competence Community should be flexible enough to ensure the required reactivity. They should facilitate solutions that help entities to be able to constantly build capability to enhance their and the Union's resilience.</u>		

Recital 14b				
23b		<p><u>(14b) The Competence Centre should have the objectives to establish the Union's leadership and expertise in cybersecurity, and by that guarantee the highest security standards in the Union, ensure the protection of data, information systems, networks and critical infrastructures in the Union, create new high-quality jobs in the area, prevent brain drain from the European cybersecurity experts to third countries, and add European value to the already existing national cybersecurity measures.</u></p>		
Recital 15				
24	<p>(15) The Competence Centre should have several key functions. First, the Competence Centre should facilitate and help coordinate the work of the European Cybersecurity Competence Network and nurture the Cybersecurity Competence Community. The Centre should drive the cybersecurity technological agenda and facilitate access to the expertise gathered in the Network and the Cybersecurity Competence Community. Secondly, it should implement relevant parts of Digital Europe and Horizon Europe programmes by allocating grants, typically following a competitive call for proposals. Thirdly, the Competence Centre should facilitate joint investment by the Union, Member States and/or industry.</p>	<p>(15) The Competence Centre should have several key functions. First, the Competence Centre should facilitate and help coordinate the work of the European Cybersecurity Competence Network and nurture the Cybersecurity Competence Community. The Centre should drive the cybersecurity technological agenda and <u>pool, share and</u> facilitate access to the expertise gathered in the Network and the Cybersecurity Competence Community. <u>and to cybersecurity infrastructure.</u> Secondly, it should implement relevant parts of Digital Europe and Horizon Europe programmes by allocating grants, typically following a competitive call for proposals. Thirdly, the Competence Centre should facilitate joint investment by the Union, Member States and/or industry <u>as well as joint training opportunities and</u></p>	<p>(15) The Competence Centre should have several key functions. First, the Competences <u>support the Cybersecurity Competence Community. The</u> Centre should facilitate and help coordinate the work <u>implement cybersecurity relevant parts</u> of the European Cybersecurity Competence Network and nurture the Cybersecurity Competence Community. The Centre should drive the cybersecurity technological agenda and facilitate access to the expertise gathered in the Network <u>Digital Europe programme and the Horizon Europe programme in accordance with the Centre's multiannual work programme ("multiannual work programme")</u> and the Cybersecurity Competence Community. Secondly, it should implement relevant parts of Digital Europe and <u>annual work programme and</u></p>	

		<u>awareness raising programmes in line with the Digital Europe Programme for citizens and businesses to overcome the skill gap. It should pay special attention to the enabling of SMEs in the area of cybersecurity.</u>	<u>the strategic planning process of the</u> Horizon Europe programmes <u>programme</u> by allocating grants, typically <u>and other forms of funding, primarily</u> following a competitive call for proposals. Thirdly , <u>facilitate transfer of expertise in the Network and the Cybersecurity Competence Community and support the</u> Competence Centre should facilitate joint investment by the Union, Member States and/or <u>or</u> industry.	
Recital 16				
25	(16) The Competence Centre should stimulate and support the cooperation and coordination of the activities of the Cybersecurity Competence Community, which would involve a large, open, and diverse group of actors involved in cybersecurity technology. That Community should include in particular research entities, supply-side industries, demand side industries, and the public sector. The Cybersecurity Competence Community should provide input to the activities and work plan of the Competence Centre and it should also benefit from the community-building activities of the Competence Centre and the Network, but otherwise should not be privileged with regard to calls for proposals or calls for tender.	(16) The Competence Centre should stimulate and support the <u>long-term strategic</u> cooperation and coordination of the activities of the Cybersecurity Competence Community, which would involve a large, open, <u>interdisciplinary</u> and diverse group of <u>European</u> actors involved in cybersecurity technology. That Community should include in particular research entities, <u>including those working on cybersecurity ethics</u> , supply-side industries, <u>demand-side industries including SMEs</u> demand side industries , and the public sector. The Cybersecurity Competence Community should provide input to the activities and work plan of the Competence Centre and it should also benefit from the community-building activities of the Competence Centre and the Network, but otherwise should not be privileged with regard to calls for proposals or calls for tender.	(16) The Competence Centre should stimulate and support the cooperation and coordination of the activities of the Cybersecurity Competence Community, which would involve a large, open, and diverse group of actors involved in cybersecurity technology. That Community should include in particular research entities, supply side industries, demand side industries, and the public sector. The Cybersecurity Competence Community should provide input to the activities and <u>multiannual work programme and the annual work programme</u> work plan of the Competence Centre and it should also benefit from the community-building activities of the Competence Centre and the Network, but otherwise should not be privileged with regard to calls for proposals or calls for tender.	

Recital 16a				
25a		<p><u>(16a) The Competence Centre should provide the appropriate support to the European Network and Information Security Agency (ENISA) in its tasks defined by Directive (EU) 2016/1148 ("NIS Directive") and Regulation (EU) 2019/XXX of the European Parliament and of the Council ("Cybersecurity Act"). Therefore, ENISA should provide relevant inputs to the Competence Centre in its task of defining funding priorities.</u></p> <p><u>1. Regulation (EU) 2019/... of the European Parliament and of the Council of ... on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L ...) (2017/0225(COD)).</u></p>		
Recital 17				
26	<p>(17) In order to respond to the needs of both demand and supply side industries, the Competence Centre's task to provide cybersecurity knowledge and technical assistance to industries should refer to both ICT products and services and all other industrial and technological products and solutions in which cybersecurity is to be embedded.</p>	<p>(17) In order to respond to the needs of <u>the public sector and</u> both demand and supply side industries, the Competence Centre's task to provide cybersecurity knowledge and technical assistance to <u>the public sector and</u> industries should refer to both ICT products, <u>processes</u> and services and all other industrial and technological products and solutions <u>processes</u> in which cybersecurity is to be embedded. <u>In particular, the Competence Centre should facilitate the deployment of dynamic</u></p>	<p>(17) In order to respond to the needs of both demand and supply side industries, the <u>Centre and the Network should</u> Competence Centre's task to provide cybersecurity knowledge and technical assistance to industries should refer to both ICT <u>access to cybersecurity knowledge in both information and communications technology (ICT)</u> products and services and all other industrial and technological products and solutions in which cybersecurity is to be</p>	

		<u>enterprise-level solutions focused on building capabilities of entire organisations, including people, processes and technology, in order to effectively protect the organizations against constantly changing cyber threats.</u>	embedded.	
Recital 17a				
26a		<u>(17a) The Competence Centre should contribute to the wide deployment of state-of-the-art cybersecurity products and solutions, in particular those that are internationally recognised.</u>		
Recital 18				
27	(18) Whereas the Competence Centre and the Network should strive to achieve synergies between the cybersecurity civilian and defence spheres, projects financed by the Horizon Europe Programme will be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe shall have a focus on civil applications.	(18) Whereas the Competence Centre and the Network should strive to achieve synergies <u>and coordination</u> between the cybersecurity civilian and defence spheres, projects financed by the Horizon Europe Programme will be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe shall have a focus on civil applications.	(18) Whereas the Competence Centre and the Network should strive to achieve synergies <u>and exchange of knowledge</u> between the cybersecurity civilian and defence spheres, projects <u>under this Regulation</u> financed by the Horizon Europe Programme will <u>should</u> be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe shall have a <u>are to have an exclusive</u> focus on civil applications.	(18) Whereas the Competence Centre and the Network should strive to achieve synergies <u>coordination and exchange of knowledge</u> between the cybersecurity civilian and defence spheres, projects <u>under this Regulation</u> financed by the Horizon Europe Programme will <u>should</u> be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe shall have a <u>are to have an exclusive</u> focus on civil applications. Commission compromise proposal. EP to provide updated text. Need to coordinate with DEP and EDF files. Defence/dual use aspect

Recital 18a				
27a			<u>(18a) The enhancement of dual use application of cybersecurity technologies for cybersecurity purposes is without prejudice to the civilian nature of this Regulation and should therefore reflect specificities of Member States in cases when cybersecurity policy is pursued by civil-military or military authorities, and ensure complementarity but not overlap to the cyber defence related funding instruments.</u>	<u>(18a) Without prejudice to the civilian nature of this Regulation, Member States' activities under this Regulation may reflect specificities of Member States in cases when cybersecurity policy is pursued by civil-military or military authorities, and ensure complementarity and avoid overlap with defence related funding instruments.</u> Commission compromise proposal. Defence/dual use aspect
Recital 19				
28	(19) In order to ensure structured and sustainable collaboration, the relation between the Competence Centre and the National Coordination Centres should be based on a contractual agreement.	(19) In order to ensure structured and sustainable collaboration, the relation between the Competence Centre and the National Coordination Centres should be based on a contractual agreement <u>that should be harmonised at Union level.</u>	(19) In order to ensure structured and sustainable collaboration, the relation between the Competence Centre and the National Coordination Centres should be based on a contractual agreement.	
Recital 20				
29	(20) Appropriate provisions should be made to guarantee the liability and transparency of the Competence Centre.	(20) Appropriate provisions should be made to guarantee the liability and transparency of the Competence Centre <u>and those undertakings receiving funding.</u>	(20) Appropriate provisions should be made to guarantee the liability and transparency of the Competence Centre.	

Recital 20a				
29a		<u>(20a) The implementation of deployment projects, in particular those relating to infrastructures and capabilities deployed at European level or in joint procurement, can be divided into different phases of implementation, such as separate tenders for the architecture of hard- and software, their production and their operation and maintenance, whereas companies may only participate in one of the phases each and requiring that the beneficiaries in one or several of those phases meet certain conditions in terms of European ownership or control.</u>		
Recital 20b				
29b		<u>(20b) With ENISA being the dedicated Union cybersecurity agency, the Competence Centre should seek the greatest possible synergies with it and the Governing Board should consult ENISA due to its experience in the field in all matters regarding cybersecurity, in particular on research-related projects.</u>		
Recital 20c				
29c		<u>(20c) In the process of the nomination of the representative to the Governing Board, the European Parliament should include details of the mandate, including the obligation to report regularly to the European Parliament, or the committees responsible.</u>		

Recital 21				
30	<p>(21) In view of their respective expertise in cybersecurity, the Joint Research Centre of the Commission as well as the European Network and Information Security Agency (ENISA) should play an active part in the Cybersecurity Competence Community and the Industrial and Scientific Advisory Board.</p>	<p>(21) In view of their respective expertise in cybersecurity <u>and in order to ensure greatest possible synergies</u>, the Joint Research Centre of the Commission as well as the European Network and Information Security Agency (ENISA) should play an active part in the Cybersecurity Competence Community and the Industrial and Scientific Advisory Board. <u>ENISA should continue to fulfil its strategic objectives especially in the field of cybersecurity certification as defined in Regulation (EU) 2019/XXX [Cybersecurity Act]¹ while the Competence Centre should act as an operational body in cybersecurity.</u></p> <p><u>1. Regulation (EU) 2019/... of the European Parliament and of the Council of ... on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L ...) (2017/0225(COD)).</u></p>	<p>(21) In view of their respective<u>its</u> expertise in cybersecurity, the Joint Research Centre of the Commission and its mandate as a reference point for advice and expertise on cybersecurity for Union institutions, agencies and bodies, as well as <u>for relevant Union stakeholders, and in view of its collection of input through its tasks,</u> the European Network and Information Security Agency (Union Agency for Cybersecurity as established by Regulation (EU) 2019/881 ("ENISA")) should play an active part in the Cybersecurity Competence Community<u>activities of the Centre including the development of the Agenda, avoiding any duplication of their tasks in particular through its role as permanent observer in the Governing Board of the Centre ("Governing Board"). Regarding the drafting of the Agenda, the annual work programme and the Industrial and Scientific Advisory multiannual work programme, the Executive Director of the Centre ("Executive Director") and the Governing Board should take into account any relevant strategic advice and input provided by ENISA, according to the rules of procedure set by the Governing</u> Board.</p>	

Recital 22				
31	(22) Where they receive a financial contribution from the general budget of the Union, the National Coordination Centres and the entities which are part of the Cybersecurity Competence Community should publicise the fact that the respective activities are undertaken in the context of the present initiative.	(22) Where they receive a financial contribution from the general budget of the Union, the National Coordination Centres and the entities which are part of the Cybersecurity Competence Community should publicise the fact that the respective activities are undertaken in the context of the present initiative.	(22) Where they receive a financial contribution from the general budget of the Union, the National Coordination Centres and the entities which are part of the Cybersecurity Competence Community should publicise the fact that the respective activities are undertaken in the context of the present initiative <u>this Regulation</u> .	
Recital 23				
32	(23) The Union contribution to the Competence Centre should finance half of the costs arising from the establishment, administrative and coordination activities of the Competence Centre, In order to avoid double funding, those activities should not benefit simultaneously from a contribution from other Union programmes.	(23) The Union contribution to the Competence Centre should finance half of the costs arising from the establishment, administrative and coordination activities of the Competence Centre, In order to avoid double funding, those activities should not benefit simultaneously from a contribution from other Union programmes.	(23) The Union contribution to the Competence Centre should finance half of the costs arising from the establishment, administrative and coordination activities of the Competence Centre, In order to avoid double funding, those activities should not benefit simultaneously from a contribution from other Union programmes.	
Recital 24				
Y 33	(24) The Governing Board of the Competence Centre, composed of the Member States and the Commission, should define the general direction of the Competence Centre's operations, and ensure that it carries out its tasks in accordance with this Regulation. The Governing Board should be entrusted with the powers necessary to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for	(24) The Governing Board of the Competence Centre, composed of the Member States and the Commission, should define the general direction of the Competence Centre's operations, and ensure that it carries out its tasks in accordance with this Regulation. The Governing Board should be entrusted with the powers necessary to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for	(24) The Governing Board of the Competence Centre , composed of <u>representatives from</u> the Member States and the Commission, should define the general direction of the Competence Centre's operations, and ensure that it <u>the Centre</u> carries out its tasks in accordance with this Regulation. The Governing Board should be entrusted with the powers necessary to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working	Y (24) The Governing Board of the Competence Centre , composed of <u>representatives from</u> the Member States and the Commission, should define the general direction of the Competence Centre's operations, and ensure that it <u>the Centre</u> carries out its tasks in accordance with this Regulation. The Governing Board should be entrusted with the powers necessary to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working

	<p>decision making by the Competence Centre, adopt the Competence Centre's work plan and multiannual strategic plan reflecting the priorities in achieving the objectives and tasks of the Competence Centre, adopt its rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof.</p>	<p>decision making by the Competence Centre, adopt the Competence Centre's work plan and multiannual strategic plan reflecting the priorities in achieving the objectives and tasks of the Competence Centre, adopt its rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof. <u>In order to benefit from synergies, ENISA should be a permanent observer in the Governing Board and contribute the work of the Competence Centre, including by being consulted on the multi-annual strategic plan and on the work plan and on the list of actions selected for funding.</u></p>	<p>procedures for decision making <u>Agenda consisting of strategic goals that have to be fulfilled</u> by the Competence-Centre, adopt the Competence Centre's work plan and multiannual strategic plan reflecting the priorities in achieving the objectives and tasks of the Competence Centre, adopt its rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof.</p>	<p>procedures for decision making by the Competence Centre, adopt the Competence Centre's work plan and multiannual strategic plan reflecting the priorities in achieving the objectives and tasks of the Competence Centre, adopt its rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof <u>Agenda</u>.</p> <p>modified Council text</p>
Recital 24a				
Y	33a		<p><u>(24a) The Governing Board should be entrusted with the powers necessary to establish the budget of the Centre, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Centre, adopt the annual work programme and the multiannual work programme reflecting the priorities set in the Agenda in achieving the objectives and tasks of the Centre, adopt its rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof.</u></p>	<p><u>(24a) odThe Governing Board should be entrusted with the powers necessary to establish the budget of the Centre, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Centre, adopt the annual work programme and the multiannual work programme based on the Agenda, adopt its rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof.</u></p> <p>modified Council text</p>

Recital 24a				
33b		<u>(24a) The Governing Board should aim to promote the Competence Centre globally, so as to raise its attractiveness and make it a world-class body for excellence in cybersecurity.</u>		
Recital 24c				
33c			<u>(24c) The Governing Board should have an oversight of the strategic and implementation activities of the Centre and ensure the synergy between them. In its annual report the Centre should put special emphasis on the achieved realisation of its strategic goals and, if necessary, propose actions for further improvement of such realisation.</u>	
Recital 25				
34	(25) In order for the Competence Centre to function properly and effectively, the Commission and the Member States should ensure that persons to be appointed to the Governing Board have appropriate professional expertise and experience in functional areas. The Commission and the Member States should also make efforts to limit the turnover of their respective Representatives on the Governing Board in order to ensure continuity in its work.	(25) In order for the Competence Centre to function properly and effectively, the Commission and the Member States should ensure that persons to be appointed to the Governing Board have appropriate professional expertise and experience in functional areas. The Commission and the Member States should also make efforts to limit the turnover of their respective Representatives on the Governing Board in order to ensure continuity in its work <u>and aim to achieve gender balance.</u>	(25) In order for the Competence Centre to function properly and effectively, the Commission and the Member States should ensure that persons to be appointed to the Governing Board have appropriate professional expertise and experience in functional areas. The Commission and the Member States should also make efforts to limit the turnover of their respective representatives on the Governing Board in order to ensure continuity in its work.	

Recital 25a				
34a		<u>(25a) The weight of the Commission vote in the decisions of the Governing Board should be in line with the contribution of the Union budget to the Competence Centre, according to the Commission responsibility to ensure proper management of the Union budget in the Union interest, as set in the Treaties.</u>	<u>(25a) In view of the Centre's specific status and responsibility for the implementation of Union funds, in particular those from Horizon Europe and Digital Europe programmes, in the Governing Board, the Commission should have a right of veto on decisions concerning only the implementation of Union funds with the sole aim of ensuring the legality of those decisions. Therefore such a right of veto should be exercised only to ensure that Union funds are implemented in compliance with Union law including the rules and the objectives of the relevant programmes set out in other Union legal acts. In particular decisions taken when implementing tasks specified in Article 13(3) (a), (d), (f), (h), (i), (la), (m), (p), (q), (sa), (u) should not be regarded as decisions concerning the implementation of Union funds.</u>	
Recital 26				
35	(26) The smooth functioning of the Competence Centre requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for cybersecurity, and that the duties of the Executive Director be carried out with complete independence.	(26) The smooth functioning of the Competence Centre requires that its Executive Director be appointed <u>in a transparent manner on the</u> on the grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for cybersecurity, and that the duties of the Executive Director be carried out with complete independence.	(26) The smooth functioning of the Competence <u>Centre</u> requires that its <u>the</u> Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for cybersecurity, and that the duties of the Executive Director be carried out with complete independence.	

Recital 27				
36	<p>(27) The Competence Centre should have an Industrial and Scientific Advisory Board as an advisory body to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The Industrial and Scientific Advisory Board should focus on issues relevant to stakeholders and bring them to the attention of the Competence Centre's Governing Board. The composition of the Industrial and Scientific Advisory Board and the tasks assigned to it, such as being consulted regarding the work plan, should ensure sufficient representation of stakeholders in the work of the Competence Centre.</p>	<p>(27) The Competence Centre should have an Industrial and Scientific Advisory Board as an advisory body to ensure regular <u>and appropriately transparent</u> dialogue with the private sector, consumers' organisations and other relevant stakeholders. <u>It should also provide the Executive Director and the Governing Board with independent advice on deployment and procurement.</u> The Industrial and Scientific Advisory Board should focus on issues relevant to stakeholders and bring them to the attention of the Competence Centre's Governing Board. The composition of the Industrial and Scientific Advisory Board and the tasks assigned to it, such as being consulted regarding the work plan, should ensure sufficient representation of stakeholders in the work of the Competence Centre. <u>A minimum number of seats should be allocated to each category of industry stakeholders, with particular attention paid to the representation of SMEs.</u></p>	<p>(27) <u>The Cybersecurity</u> The Competence Centre <u>Community</u> should have an Industrial and Scientific Advisory Board as an advisory body to ensure <u>act also as a source of advice through</u> regular dialogue between the Centre and <u>with</u> the private sector, consumers' organisations, <u>academia</u> and other relevant stakeholders. The Industrial and Scientific Advisory Board should focus on issues relevant to stakeholders and bring them to the attention of the Competence Centre's Governing Board. The composition of the Industrial and Scientific Advisory Board <u>Cybersecurity Competence Community</u> and the tasks assigned to it, such as <u>providing advice regarding the annual work programme and the multiannual work programme</u> being consulted regarding the work plan, should ensure sufficient representation of stakeholders in the work of the Competence <u>Centre</u>.</p>	

Recital 28				
37	(28) The Competence Centre should benefit from the particular expertise and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity during the duration of Horizon2020, through its Industrial and Scientific Advisory Board.	(28) The Competence Centre <u>and its activities</u> should benefit from the particular expertise and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity during the duration of Horizon2020, <u>and the pilot projects under Horizon2020 on the Cybersecurity Competence Network,</u> through its Industrial and Scientific Advisory Board. <u>The Competence Centre and Industrial and Scientific Advisory Board should, if appropriate, consider replications of existing structures, for example as working groups.</u>	deleted	

Recital 28a				
37a			<p><u>(28a) Contributions of the Member States to the resources of the Centre can be financial and/or in-kind. Financial contributions could for example consist of a grant given by a Member State to a beneficiary in that Member State complementing Union financial support to a project under the annual work programme. On the other hand, in-kind contributions would typically accrue where a Member State entity is itself the beneficiary of a Union financial support. For example, if the Union subsidised an activity of a National Coordination Centre at the financing rate of 50%, the remaining cost would be accounted for as in-kind contribution. In another example, where a Member State entity received Union financial support for creating or upgrading an infrastructure to be shared among stakeholders in line with the annual work programme, the related non-subsidised costs would be accounted for as in-kind contributions.</u></p>	

Recital 28a				
37b		<u>(28a) The Competence Centre and its bodies should make use of the experience and contributions of past and current initiatives, such as the contractual public-private partnership (cPPP) on cybersecurity, the European Cyber Security Organisation (ECSO), and the pilot project and preparatory action on Free and Open Source Software Audits (EU FOSSA).</u>		
Recital 29				
38	<p>(29) The Competence Centre should have in place rules regarding the prevention and the management of conflict of interest. The Competence Centre should also apply the relevant Union provisions concerning public access to documents as set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council¹. Processing of personal data by the Competence Centre will be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council. The Competence Centre should comply with the provisions applicable to the Union institutions, and with national legislation regarding the handling of information, in particular sensitive non classified information and EU classified information.</p> <p>1. 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</p>	<p>(29) The Competence Centre should have in place rules regarding the prevention, <u>identification and resolution of conflicts of interest in respect of its members, bodies and staff, the Governing Board, as well as the Scientific and Industrial Advisory Board, and the Community Member States should ensure the prevention, identification, and resolution of conflicts</u> and the management of conflict of interest <u>in respect of the National Coordination Centres</u>. The Competence Centre should also apply the relevant Union provisions concerning public access to documents as set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council¹. Processing of personal data by the Competence Centre will be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council. The Competence Centre should comply with the provisions applicable to the Union institutions, and with national</p>	<p>(29) The Competence Centre should have in place rules regarding the prevention and the management of conflict of interest. The Competence Centre should also apply the relevant Union provisions concerning public access to documents as set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council¹. Processing of personal data by the Competence Centre will be subject to Regulation (EU) No XXX/2018 <u>No 1725/2018</u> of the European Parliament and of the Council². The Competence Centre should comply with the provisions applicable to the Union institutions, and with national legislation <u>law</u> regarding the handling of information, in particular sensitive non classified information and EU classified information.</p> <p>1. Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May <u>30 May</u> 2001 regarding public</p>	

	Commission documents (OJ L 145, 31.5.2001, p. 43).	legislation regarding the handling of information, in particular sensitive non classified information and EU classified information. 1. 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).	access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43). <u>2. Regulation (EU) No 1725/2018 of the European Parliament and of the Council, of 23 October 2018, on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).</u>	
Recital 30				
39	(30) The financial interests of the Union and of the Member States should be protected by proportionate measures throughout the expenditure cycle, including the prevention, detection and investigation of irregularities, the recovery of lost, wrongly paid or incorrectly used funds and, where appropriate, the application of administrative and financial penalties in accordance with Regulation XXX (EU, Euratom) of the European Parliament and of the Council ¹ [the Financial Regulation]. 1. [add title and OJ reference]	(30) The financial interests of the Union and of the Member States should be protected by proportionate measures throughout the expenditure cycle, including the prevention, detection and investigation of irregularities, the recovery of lost, wrongly paid or incorrectly used funds and, where appropriate, the application of administrative and financial penalties in accordance with Regulation XXX (EU, Euratom) of the European Parliament and of the Council ¹ [the Financial Regulation]. 1. [add title and OJ reference]	(30) The financial interests of the Union and of the Member States should be protected by proportionate measures throughout the expenditure cycle, including the prevention, detection and investigation of irregularities, the recovery of lost, wrongly paid or incorrectly used funds and, where appropriate, the application of administrative and financial penalties in accordance with Regulation XXX (EU, Euratom) <u>2018/1046</u> of the European Parliament and of the Council ¹ [the Financial Regulation] . 1. [add title and OJ reference] <u>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</u>	

			<u>(OJ L 193, 30.7.2018, p. 1).</u>	
Recital 31				
40	(31) The Competence Centre should operate in an open and transparent way providing all relevant information in a timely manner as well as promoting its activities, including information and dissemination activities to the wider public. The rules of procedure of the bodies of the Competence Centre should be made publicly available.	(31) The Competence Centre should operate in an open and transparent way providing all relevant <u>comprehensively providing</u> information in a timely manner as well as promoting its activities, including information and dissemination activities to the wider public. <u>It should provide the public and any interested parties with a list of the Cybersecurity Competence Community members and should make public the declarations of interest made by them in accordance with Article 42.</u> The rules of procedure of the bodies of the Competence Centre should be made publicly available.	(31) The Competence Centre should operate in an open and transparent way providing all relevant information in a timely manner as well as promoting its activities, including information and dissemination activities to the wider public. The rules of procedure of the bodies of the Competence Centre should be made publicly available.	
Recital 31a				
40a		<u>(31a) It is advisable that both the Competence Centre and the National Coordination Centres monitor and follow the international standards as much as possible, in order to encourage development towards global best practices.</u>		
Recital 32				
41	(32) The Commission's internal auditor should exercise the same powers over the Competence Centre as those exercised in respect of the Commission.	(32) The Commission's internal auditor should exercise the same powers over the Competence Centre as those exercised in respect of the Commission.	(32) The Commission's internal auditor should exercise the same powers over the Competence Centre as those exercised in respect of the Commission.	

Recital 33				
42	(33) The Commission, the Competence Centre, the Court of Auditors and the European Anti-Fraud Office should get access to all necessary information and the premises to conduct audits and investigations on the grants, contracts and agreement signed by the Competence Centre.	(33) The Commission, the Competence Centre, the Court of Auditors and the European Anti-Fraud Office should get access to all necessary information and the premises to conduct audits and investigations on the grants, contracts and agreement signed by the Competence Centre.	(33) The Commission, the Competence Centre, the Court of Auditors and the European Anti-Fraud Office should get access to all necessary information and the premises to conduct audits and investigations on the grants, contracts and agreement signed by the Competence Centre.	
Recital 33a				
42a		<u>(33a) The power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission in respect of defining the elements of contractual agreements between the Competence Centre and National Coordination Centres, and in respect of specifying criteria for assessing and accrediting entities as members of the Cybersecurity Competence Community. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making¹. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of</u>		

		<u><i>Commission expert groups dealing with the preparation of delegated acts.</i></u> <u><i>1. OJ L 123, 12.5.2013, p. 1.</i></u>		
Recital 34				
43	<p>(34) Since the objectives of this Regulation, namely retaining and developing Union's cybersecurity technological and industrial capacities, increasing the competitiveness of the Union's cybersecurity industry and turning cybersecurity into a competitive advantage of other Union industries, cannot be sufficiently achieved by the Member States due the fact that existing, limited resources are dispersed as well as due to the scale of the investment necessary, but can rather by reason of avoiding unnecessary duplication of these efforts, helping to achieve critical mass of investment and ensuring that public financing is used in an optimal way be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.</p>	<p>(34) Since The objectives of this Regulation, namely <u>strengthening the Union's competitiveness and capacities in cybersecurity through, and reducing its digital dependence by increasing the uptake of cybersecurity products, processes and services developed within the Union,</u> retaining and developing Union's cybersecurity technological and industrial capacities, increasing the competitiveness of the Union's cybersecurity industry and turning cybersecurity into a competitive advantage of other Union industries, cannot be sufficiently achieved by the Member States due the fact that existing, limited resources are dispersed as well as due to the scale of the investment necessary, but can rather by reason of avoiding unnecessary duplication of these efforts, helping to achieve critical mass of investment and ensuring that public financing is used in an optimal way be better achieved at Union level. <u>In addition, only actions at Union level can ensure the highest level of cybersecurity in all Member States and thus close security gaps existing in some Member States that create security gaps for the whole Union. Hence,</u> the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to</p>	<p>(34) Since the objectives of this Regulation, namely retaining and developing Union's cybersecurity <u>research,</u> technological and industrial capacities, increasing the competitiveness of the Union's cybersecurity industry and turning cybersecurity into a competitive advantage of other Union industries, cannot be sufficiently achieved by the Member States <u>alone due to</u> due the fact that existing, limited resources are dispersed as well as due to the scale of the investment necessary, but can rather by reason of avoiding unnecessary duplication of these efforts, helping to achieve critical mass of investment and ensuring that public financing is used in an optimal way be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that <u>objective those objectives.</u></p>	

		achieve that objective.			
Formula					
G	44	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION:	HAVE ADOPTED THIS REGULATION: <div>Text Origin: Commission Proposal</div>	G
CHAPTER I					
Y	45	CHAPTER I GENERAL PROVISIONS AND PRINCIPLES OF THE COMPETENCE CENTRE AND THE NETWORK	CHAPTER I GENERAL PROVISIONS AND PRINCIPLES OF THE COMPETENCE CENTRE AND THE NETWORK	CHAPTER I GENERAL PROVISIONS AND PRINCIPLES OF THE COMPETENCE CENTRE AND THE NETWORK <div>use of 'Competence'</div> <div>Text Origin: Commission Proposal</div>	Y
Article 1					
G	46	Article 1 Subject matter	Article 1 Subject matter	Article 1 Subject matter <div>Text Origin: Commission Proposal</div>	G

Article 1(1)					
Y	47	<p>1. This Regulation establishes the European Cybersecurity Industrial, Technology and Research Competence Centre (the ‘Competence Centre’), as well as the Network of National Coordination Centres, and lays down rules for the nomination of National Coordination Centres as well as for the establishment of the Cybersecurity Competence Community.</p>	<p>1. This Regulation establishes the European Cybersecurity Industrial, Technology and Research Competence Centre (the ‘Competence Centre’), as well as the Network of National Coordination Centres <u>(the “Network”)</u>, and lays down rules for the nomination of National Coordination Centres as well as for the establishment of the Cybersecurity Competence Community <u>(the “Community”). The Competence Centre and the Network shall contribute to the overall resilience and awareness in the Union towards cybersecurity threats, thoroughly taking into account societal implications.</u></p>	<p>1. This Regulation establishes the European Cybersecurity Industrial, Technology and Research Competence Centre (the ‘Competence Centre’), as well as the Network of National Coordination Centres <u>(the “Network”)</u>, and lays down rules for the nomination of National Coordination Centres, as well as for the establishment of the Cybersecurity Competence Community.</p> <p>use of 'Competence'</p> <p>Text Origin: Council Mandate</p>	Y
Article 1(2)					
	48	<p>2. The Competence Centre shall contribute to the implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] thereof and of the Horizon Europe Programme established by Regulation No XXX and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme].</p>	<p>2. The Competence Centre shall contribute to the implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] thereof and of the Horizon Europe Programme established by Regulation No XXX and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme].</p>	<p>2. The Competence Centre shall <u>have an essential role in</u> contribute to the implementation of the cybersecurity part of the Digital Europe programme established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] thereof and of the Horizon Europe programme established by Regulation No XXX and in particular Section <u>2.2.63.1.3</u> of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme].</p>	<p>2. The Competence Centre shall contribute to <u>have an essential role in</u> the implementation of the cybersecurity part of the Digital Europe programme established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] thereof and <u>and contribute to the implementation</u> of the Horizon Europe programme established by Regulation No XXX and in particular Section <u>2.2.63.1.3</u> of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme].</p>

				<p>Everyone to check</p> <p>use of 'Competence'</p> <p>Text Origin: Council Mandate</p>
Article 1(3)				
49	<p>3. The seat of the Competence Centre shall be located in [Brussels, Belgium.]</p>	<p>deleted</p> <p>No 'subject matter'. Provisions on the seat have been moved to Article 44.</p>	<p>3. The seat of the Competence Centre shall be located in [Brussels, Belgium.]</p>	<p>currently no Council mandate on seat</p>
Article 1(4)				
50	<p>4. The Competence Centre shall have legal personality. In each Member State, it shall enjoy the most extensive legal capacity accorded to legal persons under the laws of that Member State. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings.</p>	<p>deleted</p> <p>No 'subject matter'. This text has been moved without modifications to a new Article 38a</p>	<p>4. The Competence Centre shall have legal personality. In each Member State, it shall enjoy the most extensive legal capacity accorded to legal persons under the lawslaw of that Member State. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings.</p>	<p>tentatively in 4th column as new Article 38a</p> <p>Lawyer-linguists to verify most appropriate place in the text</p> <p>use of 'Competence'</p>
Article 1(5)				
Y 50a			<p><u>5. This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the state in areas of criminal law.</u></p>	<p><u>4a. This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the state in areas of criminal law.</u></p> <p>EP to check</p> <p>Text Origin: Council Mandate</p>

Article 2				
G	51	Article 2 Definitions	Article 2 Definitions	Article 2 Definitions Text Origin: Commission Proposal
Article 2, first paragraph, introductory part				
Y	52	For the purpose of this Regulation, the following definitions shall apply:	For the purpose of this Regulation, the following definitions shall apply:	For the purpose of this Regulation, the following definitions shall apply: lawyer linguists to check 'shall' Text Origin: Commission Proposal
Article 2(1), point(1)				
G	53	(1) 'cybersecurity' means the protection of network and information systems, their users, and other persons against cyber threats;	(1) 'cybersecurity' means the protection of <u>full activities necessary to protect</u> network and information systems, their users, and other <u>affected</u> persons against <u>from</u> cyber threats;	(1) 'cybersecurity' means the protection of <u>activities necessary to protect</u> network and information systems, their <u>the</u> users <u>of such systems</u> , and other persons against <u>affected by</u> cyber threats; definition copied from cybersecurity act
Article 2, first paragraph, point(1a)				
G	53a		<u>(1a) 'network and information system' means a network and information system as defined in point (1) of Article 4 of Directive (EU) 2016/1148;</u>	<u>(1a) 'network and information system' means a network and information system as defined in point (1) of Article 4 of Directive (EU) 2016/1148;</u> Text Origin: Council Mandate

Article 2, first paragraph, point(1a)				
53b		<u>(1a) 'cyber defence' and 'defence dimensions of cybersecurity' means exclusively defensive and reactive cyber defence technology which aims to protect critical infrastructures, military networks and information systems, their users, and affected persons, against cyber threats including situational awareness, threat detection and digital forensics;</u>		<p>EP will check, Council sceptical</p> <p>Defence/dual use aspect</p>
Article 2(1), point(2)				
Y 54	(2) 'cybersecurity products and solutions' means ICT products, services or process with the specific purpose of protecting network and information systems, their users and affected persons from cyber threats;	(2) ' cybersecurity products and solutions <u>processes</u> ' means <u>commercial and non-commercial</u> ICT products, services or process <u>processes</u> with the specific purpose of protecting <u>data</u> , network and information systems, their users and affected <u>other</u> persons from cyber <u>cybersecurity</u> threats;	(2) 'cybersecurity products and solutions' means ICT products, services or process <u>processes</u> with the specific purpose of protecting network and information systems, their <u>the</u> users <u>of such systems</u> and other and affected persons from <u>affected by</u> cyber threats;	<p>(2) 'cybersecurity products and solutions' means <u>[commercial and non-commercial]</u> ICT products, services or process <u>processes</u> with the specific purpose of protecting <u>ensuring the confidentiality, integrity and accesibility of data, that is processed or stored in</u> network and information systems, their <u>as well as the cybersecurity of the</u> users <u>of such systems</u> and other and affected persons from <u>affected by</u> cyber threats;</p> <p>EP to check the deletion of the part in square brackets</p>

Article 2, first paragraph, point(2a)				
G	54a		<u>(2a) 'cyber threat' means any potential circumstance, event or action that may damage, disrupt or otherwise adversely impact network and information systems, their users and affected persons;</u>	<u>(2a) '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;</u> definition copied from cybersecurity act
Article 2(1), point(3)				
Y	55	(3) 'public authority' means any government or other public administration, including public advisory bodies, at national, regional or local level or any natural or legal person performing public administrative functions under national law, including specific duties;	(3) 'public authority' means any government or other public administration, including public advisory bodies, at national, regional or local level or any natural or legal person performing public administrative functions under <u>Union and</u> national law, including specific duties;	(3) 'public authority' <u>"joint action"</u> means any government or other public administration, including public advisory bodies, at national, regional or local level or any natural or legal person performing public administrative functions under national law, including specific duties; <u>an action included in the annual work programme receiving Union financial support from the Horizon Europe programme and/or Digital Europe programme, in accordance with their Regulations, as well as financial or in-kind support by one or more Member States, which are implemented via projects involving beneficiaries established in the Member States which provide financial or in-kind support to those beneficiaries stemming from those Member States.</u> Commission to check Text Origin: Council Mandate

Article 2(1), point(4)				
Y	56	<p>(4) 'participating Member State' means a Member State which voluntarily contributes financially to the administrative and operational costs of the Competence Centre.</p>	<p>(4) 'participating contributing Member State' means a Member State which voluntarily contributes financially to the administrative and operational costs of the Competence Centre-i.</p>	<p>(4) <u><i>"in-kind contribution" means those eligible costs, incurred by National Coordination Centres and other public entities when participating Member State' means a Member State in projects funded through this Regulation,</i></u> which voluntarily contributes financially to the administrative and operational costs of the Competence Centre<u>are not financed by a Union contribution or by financial contributions by Member States.</u></p> <p>Commission to check</p> <p>Text Origin: Council Mandate</p>
Article 2, first paragraph, point(4a)				
	56a		<p><u><i>(4a) 'European Digital Innovation Hubs' means a legal entity as defined in Regulation (EU) 2019/XXX of the European Parliament and of the Council'.</i></u></p> <p><u><i>I. Regulation (EU) 2019/XXX of the European Parliament and of the Council of ... establishing the Digital Europe programme for the period 2021-2027 (OJ L ...) (2018/0227(COD)).</i></u></p>	<p>to be mentioned if Hubs are in text</p>

Article 2, first paragraph, point(4b)				
56b				<p><u>(5) ‘Agenda’ means a comprehensive and sustainable Cybersecurity Industrial, Technology and Research strategy, which shall set out strategic recommendations for the development and growth of the European cybersecurity industrial, technological and research sector and shall set out strategic priorities for the Centre’s activities (the “Agenda”)</u></p> <p>Council proposal. Commission and EP to check</p>
Article 2, first paragraph, point(4c)				
56c				<p><u>(6) ‘Technical assistance’ means assisting the National Coordination Centres or the Community (i) for the performance of theirs tasks, by providing knowledge, facilitating access to the expertise [and infrastructure], facilitating networking, raising awareness, promoting cooperation, and (ii) for the project preparation in relation to the mission and objectives set out in this Regulation, without taking over the tasks of the National Coordination Centres or the Community.</u></p> <p>Council proposal. EP and Commission to check</p>

Article 3				
G	57	Article 3 Mission of the Centre and the Network	Article 3 Mission of the Centre and the Network	Article 3 Mission of the Centre and the Network Text Origin: Commission Proposal
Article 3(1), introductory part				
Y	58	1. The Competence Centre and the Network shall help the Union to:	1. The Competence Centre and the Network shall help the Union to:	1. The Competence Centre and the Network shall help the Union to: use of 'Competence' Text Origin: Commission Proposal
Article 3(1), point(a)				
Y	59	(a) retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market;	(a) retain and develop the cybersecurity technological, <u>industrial, societal, academic and research expertise and industrial</u> capacities <u>and capabilities</u> necessary to secure its Digital Single Market <u>and further the protection of data of Union citizens, companies and public administrations</u> ;	(a) retain and develop the cybersecurity <u>strengthen its strategic autonomy in the field of cybersecurity by retaining and developing the Union's research, research,</u> technological and industrial <u>cybersecurity</u> capacities <u>and capabilities</u> necessary to <u>enhance trust and security in the</u> secure its Digital Single Market; <u>including the confidentiality, integrity and accessibility of data</u> ; Leadership added from line 60b

Article 3(1), point(aa)				
Y	59a		<u>(aa) increase the resilience and reliability of the infrastructure of network and information systems, including critical infrastructure, the internet and commonly used hardware and software in the Union;</u>	<u>(aa) support European technological capacities, capabilities and skills in relation to the resilience and reliability of the infrastructure of network and information systems, including critical infrastructure, the internet and commonly used hardware and software in the Union;</u> Term "commonly used" to be specified Council: alternative description
Article 3(1), point(b)				
Y	60	(b) increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into competitive advantage of other Union industries.	(b) increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into <u>a</u> competitive advantage of other Union industries.	(b) increase the <u>global</u> competitiveness of the Union's cybersecurity industry and turn cybersecurity into <u>a</u> competitive advantage of other Union industries. (b) increase the <u>global</u> competitiveness of the Union's cybersecurity industry, <u>to ensure the highest cybersecurity standards throughout the Union</u> and turn cybersecurity into <u>a</u> competitive advantage of other Union industries-;
Article 3(1), point(ba)				
G	60a		<u>(ba) raise the awareness for cybersecurity threats, and related societal and ethical implications and concerns and reduce the skills gap in cybersecurity in the Union;</u>	Can be deleted since New line 87za introduced about awareness of Centre's and Network's mission, objectives and tasks. [highest cybersecurity standards" added from line 60b] Skills integrated in line 59 a. Awareness raising falls in the competence of ENISA.

Article 3(1), point(bb)				
G	60b		<u>(bb) develop the Union's leadership in cybersecurity and ensure the highest cybersecurity standards throughout the Union;</u>	<div>Can be deleted since</div> <div>"Leadership" added to line 59.</div> <div>"Highest standards" added to line 60</div>
Article 3(1), point(bc)				
G	60c		<u>(bc) strengthen the Union's competitiveness and capacities while reducing its digital dependence by increasing the uptake of cybersecurity products, processes and services developed within the Union;</u>	<div>Can be deleted since</div> <div>"Uptake..." added in Council text line 87j</div> <div>The rest is covered in lines 59 and 60</div>
Article 3(1), point(bd)				
G	60d		<u>(bd) reinforce the trust of citizens, consumers and businesses in the digital world, and therefore contribute to the goals of the Digital Single Market strategy.</u>	<div>Can be deleted since</div> <div>Trust is covered above in Council text</div>
Article 3(2)				
Y	61	2. The Competence Centre shall undertake its tasks, where appropriate, in collaboration with the Network of National Coordination Centres and a Cybersecurity Competence Community.	2. The Competence Centre shall undertake its tasks, where appropriate, in collaboration with the Network of National Coordination Centres and a Cybersecurity Competence Community.	2. The <u>Centre and the Network</u> Competence Centre shall undertake its <u>their</u> tasks, where appropriate, in collaboration with the Network of National Coordination Centres and a <u>ENISA and the</u> Cybersecurity Competence Community. <div>Council text: Slight rebalancing by including the Network here.</div>

Article 3(2a)				
Y	61a		<p><u>2a. Only actions contributing to the mission set out in paragraph 1 shall be eligible for support through Union financial assistance in accordance with the legal acts establishing relevant programmes notably Horizon Europe and Digital Europe.</u></p>	<p><u>2a. [Only actions contributing to the mission set out in paragraph 1 shall be supported through Union financial assistance in accordance with the legal acts establishing relevant programmes notably Horizon Europe and Digital Europe.]</u></p> <p><u>Alternative wording suggested by Commission:</u> <u>[The Competence Centre shall utilise relevant Union financial resources in such a way so as to maximise their contribution to the mission set out in paragraph 1 in accordance with the legal acts establishing these programmes notably Horizon Europe and Digital Europe.]</u></p> <p>Commission in favour of deleting. Fallback: alternative wording suggested.</p> <p>EP and Council to check</p>
Article 4				
G	62	Article 4 Objectives and Tasks of the Centre	Article 4 Objectives and Tasks of the Centre	<p>Article 4 Objectives and Tasks of the Centre</p> <p>The Commission has suggested an alternative structure for paragraph 1. This is currently not yet copied as Council and EP want to check internally and consult lawyer-linguists.</p> <p>Text Origin: Council Mandate</p>

Article 4, first paragraph, introductory part					
Y	63	The Competence Centre shall have the following objectives and related tasks:	The Competence Centre shall have the following objectives and related tasks:	The Competence Centre shall have the following objectives and related tasks <u>enhance the coordination of research, innovation and deployment in the field of cybersecurity in order to fulfil the mission as described in Article 3 , by:</u>	The <u>Centre shall enhance research, innovation and deployment in the field of cybersecurity in order to fulfil the mission as described in Article 3; by</u> Competence Centre shall have the following objectives and related tasks:
Article 4, first paragraph, point(-a)					
Y	63a				<u>enhancing cybersecurity capacities, capabilities, knowledge and infrastructures at the service of industries, in particular SMEs, research communities, the public sector and civil society as appropriate</u>
Article 4, first paragraph, point(-b)					
Y	63b				<u>complementing the efforts of other public actors, promote cybersecurity resilience, the uptake of cybersecurity best practices, the principle of security by design, and the verifiability of the security of digital products and services.</u> EP to check wording "verifiability"

Article 4, first paragraph, point(-c)				
Y	63c			<div><div><div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div></div></div></div></div>

Article 4, first paragraph, point(-g)				
63g				<p><u>(4) where relevant and appropriate, acquiring and operating cybersecurity infrastructures and services where necessary to fulfil the tasks below and in accordance with the respective work programmes set out below</u></p> <p>Council: possible compromise, not yet accepted by MS</p>
Article 4(1), point(1)				
Y 64	<p>1. facilitate and help coordinate the work of the National Coordination Centres Network ('the Network') referred to in Article 6 and the Cybersecurity Competence Community referred to in Article 8;</p>	<p>1. facilitate and help coordinate the work of the National Coordination Centres Network (the create, manage and facilitate the Network) referred to in Article 6 and the Cybersecurity Competence Community referred to in Article 8;</p>	deleted	deleted

Article 4(1), point(2)						
Y	65	<p>2. contribute to the implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX¹ and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] and of the Horizon Europe Programme established by Regulation No XXX² and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme]. and of other Union programmes when provided for in legal acts of the Union];</p> <p>1. [add full title and OJ reference] 2. [add full title and OJ reference]</p>	<p>2. contribute to <u>coordinate</u> the implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX¹ and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] and of the Horizon Europe Programme established by Regulation No XXX² and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme]. and of other Union programmes when provided for in legal acts of the Union] <u>and contribute to the implementation of the actions funded by the European Defence Fund established by Regulation (EU) ;2019/XXX;</u></p> <p>1. [add full title and OJ reference] 2. [add full title and OJ reference]</p>	<div>deleted</div>		Y
Article 4(1), point(3), introductory part						
Y	66	<p>3. enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities, by carrying out the following tasks:</p>	<p>3. enhance cybersecurity <u>resilience, capacities,</u> capabilities, knowledge and infrastructures at the service of <u>society,</u> industries, the public sector and research communities, by carrying out the following tasks, <u>having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services:</u></p>	<div>deleted</div>	Lines 66-68 linked to line 87x	Y

Article 4(1), point(3)(a)				
Y	67	<p>(a) having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services , acquiring, upgrading, operating and making available such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community;</p>	<p>(a) having regard to the state-of-the-art cybersecurity industrial and research infrastructures <u>acquiring, upgrading, operating and making available the Competence Centre's facilities</u> and related services acquiring, upgrading, operating and making available such infrastructures and related services <u>in a fair, open and transparent way</u> to a wide range of users across the Union from industry, <u>in particular</u> including SMEs, the public sector and the research and scientific community;</p>	<div>deleted</div> <div>Lines 66-68 linked to line 87x</div>
Article 4(1), point(3)(b)				
Y	68	<p>(b) having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services, providing support to other entities, including financially, to acquiring, upgrading, operating and making available such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community;</p>	<p>(b) having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services, providing support to other entities, including financially, to acquiring, upgrading, operating and making available such infrastructures <u>such facilities</u> and related services to a wide range of users across the Union from industry, <u>in particular</u> including SMEs, the public sector and the research and scientific community;</p>	<div>deleted</div> <div>Lines 66-68 linked to line 87x</div>

Article 4(1), point(3)(ba)				
Y	68a		<u>(ba) providing financial support and technical assistance to cybersecurity start-ups, SMEs, microenterprises, associations, individual experts and to civic tech projects;</u>	Deleted
Article 4(1), point(3)(bb)				
Y	68b		<u>(bb) financing software security code audits and related improvements for Free and Open Source Software projects, commonly used for infrastructure, products and processes;</u>	Deleted
Article 4(1), point(3)(c)				
Y	69	(c) providing cybersecurity knowledge and technical assistance to industry and public authorities, in particular by supporting actions aimed at facilitating access to the expertise available in the Network and the Cybersecurity Competence Community;	(c) providing <u>facilitating the sharing</u> cybersecurity knowledge and technical assistance <u>among others to civil society,</u> the to industry and public authorities, <u>and the academic and research community,</u> in particular by supporting actions aimed at facilitating access to the expertise available in the Network and the Cybersecurity Competence Community <u>with the aim of improving cyber resilience within the Union;</u>	deleted possibly to be discussed in conjunction with technical assistance

Article 4(1), point(3)(ca)				
Y	69a		<u>(ca) promoting “security by design” as principle in the process of developing, maintaining, operating, and updating infrastructures, products and services, in particular by supporting state-of-the-art secure development methods, adequate security testing, security audits, and including the commitment of producer or provider to make available updates remedying new vulnerabilities or threats, without delay, and beyond the estimated product lifetime, or enabling a third party to create and provide such updates;</u>	EP to propose a recital
Article 4(1), point(3)(cb)				
Y	69b		<u>(cb) assisting source code contribution policies and their development, in particular for public authorities where Free and Open Source Software projects are used;</u>	Check 87p
Article 4(1), point(3)(cc)				
Y	69c		<u>(cc) bringing together stakeholders from industry, trade unions, academia, research organisations and public entities to ensure long-term cooperation on developing and implementing cybersecurity products and processes, including pooling and sharing of resources and information regarding such products and processes if appropriate;</u>	Inserted in 63c

Article 4(1), point(4), introductory part				
Y	70	4. contribute to the wide deployment of state-of-the-art cyber security products and solutions across the economy, by carrying out the following tasks:	4. contribute to the wide deployment of state-of-the-art <u>and sustainable</u> cyber security products and solutions <u>processes</u> across the <u>the Union</u> economy , by carrying out the following tasks:	4. contribute to the wide deployment of state-of-the-art cyber security products and solutions across the economy, by carrying out the following tasks: Sustainable cyber security products and processes” is for a recital. EP to propose a recital that defines sustainability.
Article 4(1), point(4)(a)				
Y	71	(a) stimulating cybersecurity research, development and the uptake of Union cybersecurity products and solutions by public authorities and user industries;	(a) stimulating cybersecurity research, development and the uptake of Union cybersecurity products and <u>holistic processes throughout the entire innovation cycle, by, inter alia,</u> solutions <u>by</u> public authorities, <u>the industry and the market</u> and user industries ;	Deleted since in 87g
Article 4(1), point(4)(b)				
Y	72	(b) assisting public authorities, demand side industries and other users in adopting and integrating the latest cyber security solutions;	(b) assisting public authorities, demand side industries and other users in <u>increasing their resilience by</u> adopting and integrating the latest cyber security solutions <u>state-of-the-art cybersecurity products and processes</u> ;	Deleted since in Art. 3

Article 4(1), point(4)(c)					
Y	73	(c) supporting in particular public authorities in organising their public procurement, or carrying out procurement of state-of-the-art cybersecurity products and solutions on behalf of public authorities;	(c) supporting in particular public authorities in organising their public procurement, or carrying out procurement of state-of-the-art cybersecurity products and solutions <u>processes</u> on behalf of public authorities, <u>including by providing support for procurement, to increase the security of and the benefits from public investment</u> ;	(c) supporting in particular public authorities in organising their public procurement, or carrying out procurement of state-of-the-art cybersecurity products and solutions on behalf of public authorities ;	To be seen in relation to line 87n and 87x
Article 4(1), point(4)(d)					
Y	74	(d) providing financial support and technical assistance to cybersecurity start-ups and SMEs to connect to potential markets and to attract investment;	(d) providing financial support and technical assistance to cybersecurity start-ups and SMEs, <u>micro-enterprises, individual experts, commonly used Free and Open Source Software projects, and civic tech projects, to enhance expertise on cybersecurity</u> , to connect to potential markets <u>and deployment opportunities</u> , and to attract investment;	(d) providing financial support and technical assistance to cybersecurity start-ups and SMEs to connect to potential markets and to attract investment ;	<p>EP wants to keep the text (not in the objectives)</p> <p>Council prefers recital. However, an inclusion of these entities in Art. 8 can be discussed.</p> <p>Possible wording (from EP): “providing support to cybersecurity start-ups and SME's to connect to potential markets and to attract investment.”</p>
Article 4(1), point(5), introductory part					
Y	75	5. improve the understanding of cybersecurity and contribute to reducing skills gaps in the Union related to cybersecurity by carrying out the following tasks:	5. improve the understanding of cybersecurity and contribute to reducing skills gaps <u>and strengthening the level of skills</u> in the Union related to cybersecurity by carrying out the following tasks:	5. improve the understanding of cybersecurity and contribute to reducing skills gaps in the Union related to cybersecurity by carrying out the following tasks ;	Deletion, (covered by 87j)

Article 4(1), point(5)(-a)					
Y	75a		<u>(-a) supporting, where appropriate, the achievement of the specific objective 4, Advanced digital skills, of the Digital Europe Programme in cooperation with European Digital Innovation Hubs;</u>	Link to Art 4a	
Article 4(1), point(5)(a)					
Y	76	(a) supporting further development of cybersecurity skills , where appropriate together with relevant EU agencies and bodies including ENISA.	(a) supporting further development, <u>pooling, and sharing</u> of cybersecurity skills <u>and competences at all relevant educational levels, supporting the objective of achieving gender balance, facilitating a common high level of cybersecurity knowledge and contributing to the resilience of users and infrastructures throughout the Union in cooperation with the Network and,</u> where appropriate together, <u>aligning</u> with relevant EU agencies and bodies including ENISA.;	(a) supporting further development of cybersecurity skills , where appropriate together with relevant EU agencies and bodies including ENISA.	Depends on wording 87j
Article 4(1), point(6), introductory part					
Y	77	6. contribute to the reinforcement of cybersecurity research and development in the Union by:	6. contribute to the reinforcement of cybersecurity research and development in the Union by:	6. contribute to the reinforcement of cybersecurity research and development in the Union by.	deleted
Article 4(1), point(6)(a)					
Y	78	(a) providing financial support to cybersecurity research efforts based on a common, continuously evaluated and improved multiannual strategic, industrial, technology and research agenda;	(a) providing financial support to cybersecurity research efforts based on a common, continuously evaluated and improved multiannual strategic, industrial, technology and research <u>plan referred to in Article 13</u> agenda;	(a) providing financial support to cybersecurity research efforts based on a common, continuously evaluated and improved multiannual strategic, industrial, technology and research agenda;	deleted

Article 4(1), point(6)(b)				
Y	79	(b) support large-scale research and demonstration projects in next generation cybersecurity technological capabilities, in collaboration with the industry and the Network;	(b) support <u>supporting</u> large-scale research and demonstration projects in next generation cybersecurity technological capabilities, in collaboration with the industry, <u>the academic and research community, public sector and authorities, including -and the Network and the Community;</u>	(b) support large-scale research and demonstration projects in next generation cybersecurity technological capabilities, in collaboration with the industry and the Network; EP will look at it in relation to 87x
Article 4(1), point(6)(ba)				
Y	79a		<u>(ba) ensuring respect for fundamental rights and ethical conduct in cybersecurity research projects supported by the Competence Centre;</u>	 Preliminary agreement on a new recital 8a, line 17a: It is important to ensure respect for fundamental rights and ethical conduct in Cybersecurity research projects supported by the Centre, in line the regulations establishing Horizon Europe, and in particular Article 15 Horizon Europe Framework Programme regulation
Article 4(1), point(6)(bb)				
Y	79b		<u>(bb) monitoring reports of vulnerabilities discovered by the Community and facilitating the disclosure of vulnerabilities, the development of patches, fixes and solutions, and the distribution of those;</u>	 Potentially to be reflected in a new recital - to be discussed For MS difficult even in recital

Article 4(1), point(6)(bc)				
Y	79c		<u>(bc) monitoring research results regarding self-learning algorithms used for malicious cyber activities in collaboration with ENISA and supporting the implementation of Directive (EU) 2016/1148;</u>	Potentially to be reflected in a new recital - to be discussed
Article 4(1), point(6)(bd)				
G	79d		<u>(bd) supporting research in the field of cybercrime;</u>	deleted
Article 4(1), point(6)(be)				
Y	79e		<u>(be) supporting the research and development of products and processes that can be freely studied, shared, and built upon, in particular in the field of verified and verifiable hardware and software, in close cooperation with the industry, the Network and the Community;</u>	Could be deleted depending on wording 87p
Article 4(1), point(6)(c)				
Y	80	(c) support research and innovation for standardisation in cybersecurity technology	(c) support research and innovation for <u>formal and non-formal</u> standardisation and <u>certification</u> in cybersecurity technology, <u>linking to the existing work and where appropriate in close cooperation with the European Standardisation Organisations, certification bodies and ENISA;</u>	(c) support research and innovation for standardisation in cybersecurity technology Deleted

Article 4, first paragraph, point(6a)					
Y	80a		<u>ca provide special support to SMEs by facilitating their access to knowledge and training through tailored access to the deliverables of research and development reinforced by the Competence Centre and the Network in order to increase competitiveness;</u>		new recital EP will work on a text proposal
Article 4(1), point(7), introductory part					
Y	81	7. enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, by carrying out the following tasks:	7. enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, by carrying out the following tasks, <u>which shall be reactive and defensive cyber defence technology, applications and services</u> :	7. enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, by carrying out the following tasks:	lines 81-87 to be discussed (Defence)
Article 4(1), point(7)(a)					
Y	82	(a) supporting Member States and industrial and research stakeholders with regard to research, development and deployment;	(a) supporting Member States and industrial and research stakeholders with regard to research, development and deployment;	(a) supporting Member States and industrial and research stakeholders with regard to research, development and deployment;	
Article 4(1), point(7)(b)					
Y	83	(b) contributing to cooperation between Member States by supporting education, training and exercises ;	(b) contributing to cooperation between Member States by supporting education, training and exercises ;	(b) contributing to cooperation between Member States by supporting education, training and exercises ;	
Article 4(1), point(7)(c)					
Y	84	(c) bringing together stakeholders, to foster synergies between civil and defence cyber security research and markets;	(c) bringing together stakeholders, to foster synergies between civil and defence cyber security research and markets;	(c) bringing together stakeholders, to foster synergies between civil and defence cyber security research and markets;	

Article 4(1), point(8), introductory part				
Y	85	8. enhance synergies between the civil and defence dimensions of cybersecurity in relation to the European Defence Fund by carrying out the following tasks:	8. enhance synergies between the civil and defence dimensions of cybersecurity in relation to the European Defence Fund by carrying out the following tasks, <u>which shall be reactive and defensive cyber defence technology, applications and services</u> :	8. enhance synergies between the civil and defence dimensions of cybersecurity in relation to the European Defence Fund by carrying out the following tasks:
Article 4(1), point(8)(a)				
Y	86	(a) providing advice, sharing expertise and facilitating collaboration among relevant stakeholders;	(a) providing advice, sharing expertise and facilitating collaboration among relevant stakeholders;	(a) providing advice, sharing expertise and facilitating collaboration among relevant stakeholders;
Article 4(1), point(8)(b)				
Y	87	(b) managing multinational cyber defence projects, when requested by Member States, and thus acting as a project manager within the meaning of Regulation XXX [Regulation establishing the European Defence Fund].	(b) managing multinational cyber defence projects, when requested by Member States, and thus acting as a project manager within the meaning of Regulation XXX [Regulation establishing the European Defence Fund].	(b) managing multinational cyber defence projects, when requested by Member States, and thus acting as a project manager within the meaning of Regulation XXX [Regulation establishing the European Defence Fund].
Article 4(1), point(8)(ba)				
Y	87a		<u>(ba) assisting and providing advice to the Commission with regard to the implementation of Regulation (EU) 2019/XXX [recast of Regulation (EC) No 428/2009 as proposed by COM(2016)0616].</u>	
Article 4, first paragraph a, introductory part				
Y	87b		<u>8a. contribute to the Union's efforts to enhance international cooperation with regard to cybersecurity by:</u>	Deleted, new text in 87p

Article 4, first paragraph b, point(a)				
Y	87c		<u>(a) facilitating the participation of the Competence Centre in international conferences and governmental organisations as well as the contribution to international standardisation organisations;</u>	Deleted, new text in 87p
Article 4, first paragraph b, point(b)				
Y	87d		<u>(b) cooperating with third countries and international organisations within relevant international cooperation frameworks.</u>	Deleted, new text in 87p
Article 4a				
G	87e		<u>Article 4a</u> <u>Tasks of the Centre</u>	<u>Article 4a</u> <u>Tasks of the Centre</u> Text Origin: Council Mandate
Article 4a(1), introductory part				
G	87f		<u>1. In order to fulfill the mission laid out in Article 3 and the objective laid out in Article 4, the Centre shall, in close cooperation with the Network, have the following tasks:</u>	<u>1. In order to fulfil the mission laid out in Article 3 and the objective laid out in Article 4, the Centre shall, in close cooperation with the Network, have the following tasks:</u> Text Origin: Council Mandate
Article 4a(1), point(a)				
Y	87g		<u>(a) strategic tasks, consisting of:</u>	<u>(a) strategic tasks, consisting of:</u> Text Origin: Council Mandate

Article 4a(1), 1				
Y	87h		<u>(1) developing and monitoring the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda, which shall set out strategic recommendations and priorities for the development and growth of the European cybersecurity industrial, technological and research sector (the “Agenda”);</u>	<u>(1) developing and monitoring the implementation of the Agenda;</u>
Article 4a(1), 2				
Y	87i		<u>(2) through the Agenda and the multiannual work programme, while avoiding any duplication of activities with ENISA and taking into account the need to create synergies between cybersecurity and other parts of Horizon Europe and Digital Europe programmes;</u>	<u>(2) through the Agenda and the multiannual work programme, while avoiding any duplication of activities with ENISA and taking into account the need to create synergies between cybersecurity and other parts of Horizon Europe and Digital Europe programmes;</u> Council: definition/clarification Agenda Text Origin: Council Mandate

Article 4a(1), 2, i				
Y	87j		<p><u>(2) i defining priorities for its work on:</u></p> <ul style="list-style-type: none"> <u>- the enhancement of cybersecurity research and innovation and its deployment,</u> <u>- the development of cybersecurity industrial, technological and research capacities capabilities, and infrastructure,</u> <u>- the reinforcement of cybersecurity industrial, technological and research skills and training and</u> <u>- the deployment of cybersecurity products and solutions, and</u> 	<p><u>(2) i defining priorities for its work on:</u></p> <ul style="list-style-type: none"> <u>- the enhancement of cybersecurity research and innovation, covering the entire innovation cycle, and its deployment,</u> <u>- the development of cybersecurity industrial, technological and research capacities, capabilities, and infrastructure,</u> <u>- the reinforcement of cybersecurity and technology skills and competences in industry, technology, research and at all relevant educational levels, supporting gender balance,</u> <u>- the deployment of cybersecurity products and solutions,</u> <u>- support the market uptake of cybersecurity products, processes and services contributing to the mission set out in Article 3,</u> <u>- the support of the adoption and integration of state-of-the-art cybersecurity products and processes by public authorities at their request, demand side industries and other users; and</u> <p>updated wording 21/10 - still to be checked by all institutions</p>
Article 4a(1), 2 ii				
Y	87k		<p><u>(2) ii supporting cybersecurity industry, with a view to strengthening Union excellence, capacities and competitiveness on cybersecurity;</u></p>	<p><u>(2) ii supporting cybersecurity industry, and in particular SMEs, with a view to strengthening the Union excellence, capacities and competitiveness on cybersecurity;</u></p>

Article 4a(1), 3				
Y	87l		<u>(3) ensuring synergies and cooperation with relevant Union institutions, agencies and bodies such as ENISA while avoiding any duplication of activities with such Union institutions, agencies and bodies;</u>	<u>(3) ensuring synergies and cooperation with relevant Union institutions, agencies and bodies such as ENISA while avoiding any duplication of activities with such Union institutions, agencies and bodies;</u> Text Origin: Council Mandate
Article 4a(1), 4				
Y	87m		<u>(4) coordinating National Coordination Centres through the Network and ensuring regular exchange of expertise;</u>	<u>(4) coordinating National Coordination Centres through the Network and ensuring regular exchange of expertise;</u> Text Origin: Council Mandate
Article 4a(1), point(h)				
Y	87n		<u>(5) providing expert cybersecurity industrial, technology and research advice upon request from a Member State to that Member State;</u>	<u>(5) providing expert cybersecurity industrial, technology and research advice, including with regard to procurements and deployment of technologies, upon request from a Member State to that Member State;</u>
Article 4a(1), point(i)				
Y	87o		<u>(6) facilitating collaboration and sharing of expertise among relevant stakeholders, in particular members of the Cybersecurity Competence Community;</u>	<u>(6) facilitating collaboration and sharing of expertise among all relevant stakeholders, in particular members of the Cybersecurity Competence Community;</u>

Article 4a(1), point(j)				
Y	87p			<u>(6a) attending national, European and international conferences, fairs and fora related to its mission, objectives and other tasks, as appropriate, with the aim of sharing views and exchanging relevant best-practices with other participants;</u>
Article 4a(1), point(j)				
Y	87q		<u>(7) facilitating the use of results from research and innovation projects in actions related to the development of cybersecurity products and solutions, seeking to avoid fragmentation and duplication of efforts and replicating good cybersecurity practices and cybersecurity products and solutions, including those developed by small and medium enterprises (SMEs) and those based on open-source software;</u>	<u>(7) facilitating the use of results from research and innovation projects in actions related to the development of cybersecurity products and solutions, seeking to avoid fragmentation and duplication of efforts and replicating good cybersecurity practices and cybersecurity products and solutions, and in particular those developed by small and medium enterprises (SMEs) and those using open source software;</u>
Article 4a(1), point(b)				
Y	87r		<u>(b) implementation tasks, consisting of:</u>	<u>(b) implementation tasks, consisting of:</u> Text Origin: Council Mandate

Article 4a(1), point(b)(1)				
Y	87s		<u>(1) coordinating and administrating the work of the Network and the Cybersecurity Competence Community in order to achieve the mission set out in Article 3, in particular supporting cybersecurity start-ups and SMEs in the Union and facilitating their access to expertise, funding, investment and to markets;</u>	<u>(1) coordinating and administrating the work of the Network and the Cybersecurity Competence Community in order to achieve the mission set out in Article 3, in particular supporting cybersecurity start-ups, SMEs, micro-entreprises, associations and civic tech projects in the Union and facilitating their access to expertise, funding, investment and to markets;</u>
Article 4a(1), point(b)(2)				
Y	87t		<u>(2) establishing and implementing the annual work programme, in accordance with the Agenda and the multiannual work programme, for the cybersecurity parts of;</u>	<u>(2) establishing and implementing the annual work programme, in accordance with the Agenda and the multiannual work programme, for the cybersecurity parts of;</u> Text Origin: Council Mandate
Article 4a(1), point(b)(2) i				
Y	87u		<u>(2) i the Digital Europe programme and in particular actions related to Article 6 of Regulation (EU) No XXX /Digital Europe Programm.</u>	<u>(2) i the Digital Europe programme and in particular actions related to Article 6 of Regulation (EU) No XXX /Digital Europe Programm.</u> Text Origin: Council Mandate

Article 4a(1), point(b)(2) ii					
Y	87v		<u>(2) ii joint actions receiving support from the cybersecurity parts of the Horizon Europe programme and in particular Section 3.1.3. of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation [ref. number of the Specific Programme], and in accordance with the multiannual work programme, and the strategic planning process of the Horizon Europe programme, and</u>	<u>(2) ii joint actions receiving support from the cybersecurity parts of the Horizon Europe programme and in particular Section 3.1.3. of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation [ref. number of the Specific Programme], and in accordance with the multiannual work programme, and the strategic planning process of the Horizon Europe programme, and</u> Text Origin: Council Mandate	Y
Article 4a(1), point(b)(2)iii					
Y	87w		<u>(2) iii other Union programmes when provided for in legal acts of the Union;</u>	<u>(2) iii other Union programmes when provided for in legal acts of the Union;</u> Text Origin: Council Mandate	Y
Article 4a(1), point(r)					
Y	87x			<u>(2a) supporting, where appropriate, the achievement of the specific objective 4, Advanced digital skills, of the Digital Europe Programme in cooperation with European Digital Innovation Hubs;</u>	Y
Article 4a(1), point(c)					
	87y				

Article 4a(1), point(b)(3)					
Y	87z		<p><u>(3) providing expert advice on cybersecurity industry, technology and research to the Commission when it prepares the draft work programmes pursuant to Article 11 of Council Decision (XXXX)¹;</u></p> <p><u>1. [1] Council Decision ..., of ..., on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation (OJ ...) [2018/0225(COD)].</u></p>	<p><u>(3) providing expert advice on cybersecurity industry, technology and research to the Commission when it prepares the draft work programmes pursuant to Article 11 of Council Decision (XXXX)¹;</u></p> <p><u>1. [1] Council Decision ..., of ..., on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation (OJ ...) [2018/0225(COD)].</u></p> <p>Text Origin: Council Mandate</p>	Y
Article 4a(1), point(b)(4)					
Y	87aa		<p><u>(4) enabling the deployment and facilitating the acquisition of cybersecurity infrastructures, at the service of industries, the public sector, research communities and operators of essential services, through inter alia contributions from Member States and Union funding for joint actions, in line with the Agenda, the multiannual work programme and the annual work programme.</u></p>	<p><u>(4) carrying out or enabling the deployment and facilitating the acquisition of cybersecurity infrastructures, at the service of society, industries, the public sector at the request of the respective Member State, research communities and operators of essential services, through inter alia contributions from Member States and Union funding for joint actions, in line with the Agenda, the multiannual work programme and the annual work programme.</u></p>	Y

Article 4a(1), point(b)(5)				
Y	87ab		<p><u>(5) without prejudice to the civilian nature of projects to be financed from the Horizon Europe programme and the Digital Europe programme and in line with the respective program regulations, enhancing synergies and exchange of knowledge and coordination between the cybersecurity civilian and defence spheres;</u></p>	<p><u>(u) without prejudice to the civilian nature of projects to be financed from the Horizon Europe programme and in line with the respective program regulations, enhancing synergies and exchange of knowledge and coordination between the cybersecurity civilian and defence spheres, including the European Defence Fund;</u></p> <p>Commission suggestion based on Council text.</p> <p>Political issue for trilogue</p> <p>Defence/dual use aspect</p>
Article 4a(1), point(w)				
Y	87ac		<p><u>(c) monitoring the fulfilment of the strategic and implementation tasks and, whenever necessary, providing proposals for the enhancement of their realisation.</u></p>	<p><u>(c) monitoring the fulfilment of the strategic and implementation tasks and, whenever necessary, providing proposals for the enhancement of their realisation.</u></p> <p>Presidency to provide updated text in relation to Art. 13(3)(l)</p> <p>Text Origin: Council Mandate</p>
Article 4a(1), point(w)				
Y	87ad			<p><u>(ca) raising awareness of the Centre's and Network's mission, objectives and tasks as laid down in articles 3, 4, and 4a</u></p>

				<u>of this regulation.</u>
Article 4a(1), 2				
Y	87ae		<u>(2) In accordance with Article 6 of the Horizon Europe Framework programme and subject to the conclusion of a contribution agreement as referred to in point (18) of Article 2 of Regulation (EU, Euratom) 2018/1046, the Centre may be entrusted with the implementation of the cybersecurity parts that are not co-funded by the Member States in the Horizon Europe Programme [established by Regulation No XXX and in particular Section 3.1.3. of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation [ref. number of the Specific Programme]</u>	<u>(2) In accordance with Article 6 of the Horizon Europe Framework programme and subject to the conclusion of a contribution agreement as referred to in point (18) of Article 2 of Regulation (EU, Euratom) 2018/1046, the Centre may be entrusted with the implementation of the cybersecurity parts that are not co-funded by the Member States in the Horizon Europe Programme [established by Regulation No XXX and in particular Section 3.1.3. of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation [ref. number of the Specific Programme]</u> Text Origin: Council Mandate
Article 5				
G	88	Article 5 Investment in and use of infrastructures, capabilities, products or solutions	Article 5 Investment in and use of infrastructures, capabilities, products or solutions <u>processes</u>	Article 5 <div>deleted</div> Tentative agreement to delete Article 5
Article 5(1), introductory part				
Y	89	1. Where the Competence Centre provides funding for infrastructures, capabilities, products or solutions pursuant to Article 4(3) and (4) in the form of a grant or a prize, the work plan of the Competence Centre may specify in particular:	1. Where the Competence Centre provides funding for infrastructures, capabilities, products or solutions <u>processes</u> pursuant to Article 4(3) and (4) in the form of a <u>procurement</u> , grant or a prize, the work plan of the Competence Centre may specify in particular:	<div>deleted</div>

Article 5(1), point(a)					
Y	90	(a) rules governing the operation of an infrastructure or capability, including where relevant entrusting the operation to a hosting entity based on criteria that the Competence Centre shall define;	(a) <u>specific</u> rules governing the operation of an infrastructure or capability, including where relevant entrusting the operation to a hosting entity based on criteria that the Competence Centre shall define;	deleted	Y
Article 5(1), point(b)					
Y	91	(b) rules governing access to and use of an infrastructure or capability.	(b) rules governing access to and use of an infrastructure or capability.	deleted	Y
Article 5(1), point(ba)					
Y	91a		<u>(ba) specific rules governing different phases of implementation;</u>		Y
Article 5(1), point(bb)					
Y	91b		<u>(bb) that as a result of Union contribution, access is as open as possible and as closed as necessary, and re-use is possible.</u>		Y
				Agreement to add this aspect as a recital	

Article 5(2)				
Y	92	2. The Competence Centre may be responsible for the overall execution of relevant joint procurement actions including pre-commercial procurements on behalf of members of the Network, members of the cybersecurity Competence Community, or other third parties representing the users of cybersecurity products and solutions. For this purpose, the Competence Centre may be assisted by one or more National Coordination Centres or members of the Cybersecurity Competence Community.	2. The Competence Centre may be responsible for the overall execution of relevant joint procurement actions including pre-commercial procurements on behalf of members of the Network, members of the cybersecurity Competence Community, or other third parties representing the users of cybersecurity products and solutions. For this purpose, the Competence Centre may be assisted by one or more National Coordination Centres or members of the Cybersecurity Competence Community <u>or relevant European Digital Innovation Hubs.</u>	deleted
Article 6				
G	93	Article 6 Nomination of National Coordination Centres	Article 6 Nomination of National Coordination Centres	Article 6 Nomination of National Coordination Centres Text Origin: Commission Proposal
Article 6(-1)				
G	93a		<u>-1. A single National Coordination Centre shall be set up in each Member State.</u>	not retained

Article 6(1)					
G	94	1. By [date], each Member State shall nominate the entity to act as the National Coordination Centre for the purposes of this Regulation and notify it to the Commission.	1. By [date], each Member State shall nominate the entity to act as the National Coordination Centre for the purposes of this Regulation and notify it to the Commission.	1. By [date], each Member State shall nominate the <u>an</u> entity to act as the National Coordination Centre for the purposes of this Regulation and notify it <u>without delay</u> to the Commission <u>Governing Board</u> . <u>Such entity may be an entity already established in that Member State.</u>	1. By [date xxx]; <u>months after the entry into force</u> each Member State shall nominate the <u>one</u> entity to act as the National Coordination Centre for the purposes of this Regulation and notify it <u>without delay</u> to the Commission <u>Governing Board</u> . <u>Such entity may be an entity already established in that Member State.</u>
Article 6(2)					
Y	95	2. On the basis of an assessment concerning the compliance of that entity with the criteria laid down in paragraph 4, the Commission shall issue a decision within 6 months from the nomination transmitted by the Member State providing for the accreditation of the entity as a National Coordination Centre or rejecting the nomination. The list of National Coordination Centres shall be published by the Commission.	2. On the basis of an assessment concerning the compliance of that entity with the criteria laid down in paragraph 4, the Commission shall issue a decision within 6 months from the nomination transmitted by the Member State providing for the accreditation of the entity as a National Coordination Centre or rejecting the nomination. The list of National Coordination Centres shall be published by the Commission.	2. On the basis of an assessment concerning the compliance of that <u>the nomination by a Member State of an</u> entity with <u>which fulfils</u> the criteria laid down in paragraph 4, the Commission <u>Governing Board</u> shall issue a decision within 6 months from the nomination transmitted by the Member State providing for the accreditation of <u>the list that</u> entity as a National Coordination Centre or rejecting <u>no later than 3 months after</u> the nomination. The list of National Coordination Centres shall be published by the Commission <u>Centre</u> .	2. On the basis of an assessment concerning the compliance of that <u>the notification by a Member State of an</u> entity with <u>which fulfils</u> the criteria laid down in paragraph 4, the Commission shall issue a decision within 6 months from the nomination transmitted by the Member State providing for the accreditation of <u>Governing Board shall list that</u> entity as a National Coordination Centre or rejecting the nomination <u>no later than 3 months after the notification</u> . The list of National Coordination Centres shall be published by the Commission <u>Centre</u> .
Article 6(3)					
G	96	3. Member States may at any time nominate a new entity as the National Coordination Centre for the purposes of this Regulation. Paragraphs 1 and 2 shall apply to nomination of any new entity.	3. Member States may at any time nominate a new entity as the National Coordination Centre for the purposes of this Regulation. Paragraphs 1 and 2 shall apply to nomination of any new entity.	3. Member States may at any time nominate a new entity as the National Coordination Centre for the purposes of this Regulation. Paragraphs 1 and 2 shall apply to <u>the</u> nomination of any new entity.	3. Member States may at any time nominate a new entity as the National Coordination Centre for the purposes of this Regulation. Paragraphs 1 and 2 shall apply to <u>the</u> nomination of any new entity.
Text Origin: Council Mandate					

Article 6(4)						
Y	97	<p>4. The nominated National Coordination Centre shall have the capability to support the Competence Centre and the Network in fulfilling their mission laid out in Article 3 of this Regulation. They shall possess or have direct access to technological expertise in cybersecurity and be in a position to effectively engage and coordinate with industry, the public sector and the research community.</p>	<p>4. The nominated National Coordination Centre shall have the capability to support the Competence Centre and the Network in fulfilling their mission laid out in Article 3 of this Regulation. They shall possess or have direct access to technological expertise in cybersecurity and be in a position to effectively engage and coordinate with industry, the public sector, <u>the academic and research community, and citizens. The Commission shall issue guidelines further detailing the assessment procedure and explaining the application of the criteria</u> and the research community.</p>	<p>4. The nominated National Coordination Centre shall have<u>be a public sector entity or an entity with a majority of public participation performing public administrative functions under national law, including by means of delegation and having</u> the capability to support the Competence Centre and the Network in fulfilling their mission laid out in Article 3 of this Regulation. They<u>It</u> shall either possess or have direct access to <u>research and</u> technological expertise in cybersecurity. <u>It shall have the capacity and be in a position</u> to effectively engage and coordinate with <u>the</u> industry, the public sector, <u>including authorities designated pursuant to the Directive (EU) 2016/1148</u>, and the research community. <u>It shall also have the administrative capacity to manage funds.</u></p>	<p>4. The nominated National Coordination Centre shall have<u>be a public sector entity or an entity with a majority of public participation performing public administrative functions under national law, including by means of delegation, and having</u> the capability to support the Competence Centre and the Network in fulfilling their mission laid out in Article 3 of this Regulation. They<u>It</u> shall either possess or have direct access to <u>research and</u> technological expertise in cybersecurity. <u>It shall have the capacity and be in a position</u> to effectively engage and coordinate with <u>the</u> industry, the public sector, <u>the academic and research community and citizens, including authorities designated pursuant to the Directive (EU) 2016/1148</u>, and the research community. <u>It shall also have the administrative capacity to manage funds.</u></p>	Y
Article 6(5)						
Y	98	<p>5. The relationship between the Competence Centre and the National Coordination Centres shall be based on a contractual agreement signed between the Competence Centre and each of the National Coordination Centres. The agreement shall provide for the rules governing the relationship and division of tasks between the Competence Centre and each National Coordination Centre.</p>	<p>5. The relationship between the Competence Centre and the National Coordination Centres shall be based on a <u>standard</u> contractual agreement signed between the Competence Centre and each of the National Coordination Centres. The agreement shall <u>consist of the same set of harmonised general conditions providing</u> provide for the rules governing the relationship and division of tasks between the Competence Centre and each <u>National Coordination Centre and special conditions tailored to the particular</u> National Coordination Centre.</p>	<p>5. The relationship between the Competence Centre and the National Coordination Centres shall be based on a contractual agreement signed between the Competence Centre and each of the National Coordination Centres. The agreement shall provide for the rules governing the relationship and division of tasks between the Competence Centre and each National Coordination Centre.</p>	Deleted	Y

Article 6(5a)				
Y	98a		<u>5a. The Commission shall adopt delegated acts in accordance with Article 45a in order to supplement this Regulation by establishing the harmonised general conditions of the contractual agreements referred to in paragraph 5 of this Article, including their format.</u>	Deleted
Article 6(6)				
Y	99	6. The National Coordination Centres Network shall be composed of all the National Coordination Centres nominated by the Member States.	6. The National Coordination Centres Network shall be composed of all the National Coordination Centres nominated by the Member States.	6. The National Coordination Centres Network shall be composed of all the National Coordination Centres nominated by the Member States. Text Origin: Council Mandate
Article 7				
G	100	Article 7 Tasks of the National Coordination Centres	Article 7 Tasks of the National Coordination Centres	Article 7 Tasks of the National Coordination Centres Text Origin: Commission Proposal
Article 7(1), introductory part				
G	101	1. The National Coordination Centres shall have the following tasks:	1. The National Coordination Centres shall have the following tasks:	1. The National Coordination Centres shall have the following tasks: Text Origin: Commission Proposal

Article 7(1), point(a)				
Y	102	(a) supporting the Competence Centre in achieving its objectives and in particular in coordinating the Cybersecurity Competence Community;	(a) supporting the Competence Centre in achieving its objectives and in particular in <u>establishing and</u> coordinating the Cybersecurity Competence Community;	(a) supporting the acting as contact points at the national level for the Cybersecurity Competence <u>Community to support the</u> Centre in achieving its objectives and objective and mission in particular in coordinating the Cybersecurity Competence Community <u>through the coordination of its national members</u> ; Text Origin: Council Mandate
Article 7(1), point(aa)				
Y	102a			(aa) <u>providing expertise and actively contributing to the strategic tasks referred to in Article 4a, taking into account relevant national and regional challenges for cybersecurity in different sectors</u> ; Text Origin: Council Mandate
Article 7(1), point(b)				
Y	103	(b) facilitating the participation of industry and other actors at the Member State level in cross-border projects;	(b) <u>promoting, encouraging and</u> facilitating the participation of <u>civil society, industry, in particular start-ups and SMEs, academic and research community</u> and other actors at the Member State level in cross-border projects;	(b) <u>promoting, encouraging and</u> facilitating the participation of <u>civil society, industry, in particular start-ups and SMEs, academic and research communities</u> and other actors at the Member State level in cross-border projects <u>and cybersecurity actions funded through all relevant Union programmes</u> ;

Article 7(1), point(ba)					
G	103a		<u>(ba) in cooperation with other entities with similar tasks, operating as a one-stop-shop for cybersecurity products and processes financed through other Union programmes like InvestEU or the Single Market Programme, in particular for SMEs;</u>	Deleted	
Article 7(1), point(c)					
Y	104	(c) contributing, together with the Competence Centre, to identifying and addressing sector-specific cyber security industrial challenges;	(c) contributing, together with the Competence Centre, to identifying and addressing sector-specific cyber security industrial challenges;	(c) contributing, together with the Competence Centre, to identifying and addressing sector-specific cyber security industrial challenges;	Deleted since is in 102a
Article 7(1), point(ca)					
Y	104a		<u>(ca) cooperating closely with National Standardisation Organisations to promote the uptake of existing standards and to involve all relevant stakeholders, particularly SMEs, in setting new standards;</u>		EP to consider deletion since covered in 106.
Article 7(1), point(d)					
Y	105	(d) acting as contact point at the national level for the Cybersecurity Competence Community and the Competence Centre;	(d) acting as contact point at the national level for the Cybersecurity Competence Community and the Competence Centre;	(d) acting as contact point at the national level for the Cybersecurity Competence Community and the Competence Centre;	Deleted

Article 7(1), point(e)					
Y	106	(e) seeking to establish synergies with relevant activities at the national and regional level;	(e) seeking to establish synergies with relevant activities at the national, <u>regional and local</u> and regional level;	(e) seeking to establish synergies with relevant activities at the national and regional level, <u>such as including national policies on research, development and innovation in the area of cybersecurity, and in particular those policies stated in the national cybersecurity strategies</u> ;	(e) seeking to establish synergies with relevant activities at the national, <u>regional and local</u> and regional level, <u>such as including national policies on research, development and innovation in the area of cybersecurity, and in particular those policies stated in the national cybersecurity strategies</u> ;
Article 7(1), point(f)					
Y	107	(f) implementing specific actions for which grants have been awarded by the Competence Centre, including through provision of financial support to third parties in line with Article 204 of Regulation XXX [new Financial Regulation] under conditions specified in the concerned grant agreements.	(f) implementing specific actions for which grants have been awarded by the Competence Centre, including through provision of financial support to third parties in line with Article 204 of Regulation XXX [new Financial Regulation] under conditions specified in the concerned grant agreements.	(f) implementing specific actions for which grants have been awarded by the Competence Centre, including through provision of financial support to third parties in <u>line accordance</u> with Article 204 of Regulation XXX [new Financial Regulation] <u>(EU, Euratom) 2018/1046</u> under conditions specified in the concerned grant agreements: <u>concerned</u> ;	(f) implementing specific actions for which grants have been awarded by the Competence Centre, including through provision of financial support to third parties in <u>line accordance</u> with Article 204 of Regulation XXX [new Financial Regulation] <u>(EU, Euratom) 2018/1046</u> under conditions specified in the concerned grant agreements: <u>concerned</u> ; use of 'Competence' Text Origin: Council Mandate

Article 7(1), point(fa)					
Y	107a		<u>(fa) promoting and disseminating a common minimal cybersecurity educational curricula in cooperation with the relevant bodies in the Member States;</u>	<p>update 21/10: A wording on "contribution to education" could be acceptable,</p> <p>recital is still difficult for the Council, especially the word "minimal"</p> <p>EP to check</p> <p>EP to provide wording without "common" Possible recital: Education in the Member States of the European Union should reflect the importance of adequate cybersecurity awareness and skills. To this end, the Centre and the Network, alongside relevant public authorities and stakeholders, should contribute to promoting and disseminating minimal cybersecurity educational curricula in cooperation with the relevant bodies in the Member States.</p>	Y
Article 7(1), point(g)					
Y	108	(g) promoting and disseminating the relevant outcomes of the work by the Network, the Cybersecurity Competence Community and the Competence Centre at national or regional level;	(g) promoting and disseminating the relevant outcomes of the work by the Network, the Cybersecurity Competence Community and the Competence Centre at national, <u>regional or local</u> or regional level;	(g) promoting and disseminating the relevant outcomes of the work by the Network, the Cybersecurity Competence Community and the Competence Centre at national or regional level;	Y

Article 7(1), point(h)				
Y	109	(h) assessing requests by entities established in the same Member State as the Coordination Centre for becoming part of the Cybersecurity Competence Community.	(h) assessing requests by entities <u>and individuals</u> established in the same Member State as the Coordination Centre for becoming part of the Cybersecurity Competence Community.	(h) assessing requests by entities established in the same Member State as the <u>National</u> Coordination Centre for becoming part of the Cybersecurity Competence Community- i double-check addition of individuals
Article 7(1), point(i)				
Y	109a		<u>(i) advocating and promoting involvement by relevant entities in the activities arising from the Centre, Network and Cybersecurity Competence Community, and monitoring, as appropriate, the level of engagement with and grant actions awarded for cybersecurity research, developments and deployments.</u>	<u>(ha) advocating and promoting involvement by relevant entities in the activities arising from the Centre, Network and Cybersecurity Competence Community, and monitoring, as appropriate, the level of engagement with and grant actions awarded for cybersecurity research, developments and deployments.</u> Text Origin: Council Mandate
Article 7(2)				
G	110	2. For the purposes of point (f), the financial support to third parties may be provided in any of the forms specified in Article 125 of Regulation XXX [new Financial Regulation] including in the form of lump sums.	2. For the purposes of point (f), the financial support to third parties may be provided in any of the forms specified in Article 125 of Regulation XXX [new Financial Regulation] including in the form of lump sums.	2. For the purposes of point (f) <u>of paragraph 1 of this Article</u> , the financial support to third parties may be provided in any of the forms specified in Article 125 of Regulation XXX [new Financial Regulation] <u>(EU, Euratom) 2018/1046</u> , including in the form of lump sums. Text Origin: Council Mandate

Article 7(3)				
Y	111	<p>3. National Coordination Centres may receive a grant from the Union in accordance with Article 195 (d) of Regulation XXX [new Financial Regulation] in relation to carrying out the tasks laid down in this Article.</p>	<p>3. National Coordination Centres may receive a grant from the Union in accordance with Article 195 (d) of Regulation XXX [new Financial Regulation] in relation to carrying out the tasks laid down in this Article.</p>	<p>3. National Coordination Centres may receive a grant from the Union in accordance with <u>point (d) of the first paragraph of</u> Article 195 (d) of Regulation XXX [new Financial Regulation] in <u>(EU, Euratom) 2018/1046</u> in relation to carrying out the tasks laid down in this Article.</p> <p><u>3a. Where a National Coordination Centre is to receive a grant from the Union in accordance with point (d) of the first paragraph of Article 195 (d) of Regulation (EU, Euratom) 2018/1046 or implement specific actions for which grants have been awarded by the Centre, including through provision of financial support to third parties in accordance with Article 204 of Regulation (EU, Euratom) 2018/1046, the Commission as member of the Governing Board may instruct the Executive Director to suspend or cancel the conclusion or execution of the respective grant agreement if it considers that the conditions outlined in Article 6(4) are not met.</u></p> <p>agreement on (3). Wording (3a) to be checked by EP, Presidency and COM. COM to check different models:</p> <p>On 3a: Another solution is to be found.</p> <p>Commission Legal Service:</p> <p>The fulfilment of the conditions set in</p>

				<p>Article 6(4) must be checked at the time of the designation of those national coordination centres and in any case before any invitation to those NCCs to submit a proposal. The Commission must have the possibility to oppose the designation if the conditions are not fulfilled. Those conditions cannot be checked by the Commission during the GAP (grant agreement preparation) or after the GA signature (to which the Commission is not even a party and has no role).</p> <p>An alternative might be that the MS notifies the designation of its NCC both to the Centre and the Commission and the Commission has the possibility to oppose within a certain deadline.</p> <p>Text Origin: Council Mandate</p>
Article 7(4)				
Y	112	<p>4. National Coordination Centres shall, where relevant, cooperate through the Network for the purpose of implementing tasks referred to in points (a), (b), (c), (e) and (g) of paragraph 1.</p>	<p>4. National Coordination Centres shall, where relevant, cooperate through the Network <u>and with the relevant European Digital Innovation Hubs</u> for the purpose of implementing tasks referred to in points (a), (b), (c), (e) and (g) of paragraph 1.</p>	<p>4. National Coordination Centres shall, where relevant, cooperate through the Network for the purpose of implementing tasks referred to in points (a), (b), (c), (e) and (g) of paragraph 1.</p> <p>Text Origin: Council Mandate</p>
Article 8				
G	113	<p>Article 8 The Cybersecurity Competence Community</p>	<p>Article 8 The Cybersecurity Competence Community</p>	<p>Article 8 The Cybersecurity Competence Community</p> <p>Text Origin: Commission</p>

				Proposal
Article 8(1)				
Y	114	1. The Cybersecurity Competence Community shall contribute to the mission of the Competence Centre as laid down in Article 3 and enhance and disseminate cybersecurity expertise across the Union.	1. The Cybersecurity Competence Community shall contribute <u>contributes</u> to the mission of the Competence Centre as laid down in Article 3 and <u>and enhances, pools, shares, enhance</u> and disseminate cybersecurity expertise across the Union <u>and provides technical expertise.</u>	1. The Cybersecurity Competence Community shall contribute to the mission of the Competence Centre <u>and the Network</u> as laid down in Article 3 and enhance and disseminate cybersecurity expertise across the Union.
Article 8(2)				
Y	115	2. The Cybersecurity Competence Community shall consist of industry, academic and non-profit research organisations, and associations as well as public entities and other entities dealing with operational and technical matters. It shall bring together the main stakeholders with regard to cybersecurity technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise..	2. The Cybersecurity Competence Community shall consist of <u>civil society, industry from the demand and supply-side, including SMEs, academic and research community, associations of users, individual experts, relevant European Standardisation non-profit research</u> Organisations, and <u>other</u> associations as well as public entities and other entities dealing with operational and technical matters <u>in the area of cybersecurity</u> . It shall bring together the main stakeholders with regard to cybersecurity technological, <u>industrial, academic and research, and societal and industrial</u> capacities <u>and capabilities</u> in the Union It and shall involve National Coordination Centres, <u>European Digital Innovation Hubs</u> as well as Union institutions and bodies with relevant expertise: <u>as referred to in Article 10 of this Regulation</u> .	2. The Cybersecurity Competence Community shall, <u>on the one hand</u> , consist of industry, academic and non-profit research organisations, and other relevant civil society associations as well as public entities and other entities dealing with <u>cybersecurity</u> operational and technical matters <u>and, on the other hand, where relevant, actors of sectors having an interest in cybersecurity and facing cybersecurity challenges</u> . It shall bring together the main stakeholders with regard to cybersecurity <u>research</u> , technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise, <u>such as ENISA</u> .
				Individual experts in square brackets. reference to European Standardiation

				Organisations in square brackets
--	--	--	--	----------------------------------

Article 8(3), introductory part					
Y	116	3. Only entities which are established within the Union may be accredited as members of the Cybersecurity Competence Community. They shall demonstrate that they have cybersecurity expertise with regard to at least one of the following domains:	3. Only entities which are established <u>and individuals resident</u> within the Union, <u>the European Economic Area (EEA) or the European Free Trade Association (EFTA)</u> may be accredited as members of the Cybersecurity Competence Community. They <u>Applicants</u> shall demonstrate that they <u>can provide</u> have cybersecurity expertise with regard to at least one of the following domains:	3. Only entities which are established within the Union may be accredited <u>registered</u> as members of the Cybersecurity Competence Community. They shall demonstrate that they have <u>can contribute to the mission as set out in Article 3 and shall have</u> cybersecurity expertise with regard to at least one of the following domains:	3. Only entities which are established <u>and individual resident</u> within the Union, <u>the European Economic Area (EEA) or the European Free Trade Association (EFTA)</u> may be accredited <u>registered</u> as members of the Cybersecurity Competence Community. They shall demonstrate that they <u>can contribute to the mission as set out in Article 3 and shall</u> have cybersecurity expertise with regard to at least one of the following domains: Issue of "individuals", "EEA", "EFTA" Needs to be checked who will evaluate whether non EU entities can be registered (COM or Centre).
Article 8(3), point(a)					
G	117	(a) research;	(a) <u>academia or</u> research;	(a) research <u>and innovation</u> ;	(a) <u>academia</u> , research <u>and innovation</u> ;
Article 8(3), point(b)					
G	118	(b) industrial development;	(b) industrial development;	(b) industrial <u>or product</u> development;	(b) industrial <u>or product</u> development; Text Origin: Council Mandate
Article 8(3), point(c)					
G	119	(c) training and education.	(c) training and education.	(c) training and education.	(c) training and education. Text Origin: Commission Proposal

Article 8(3), point(d)					
Y	119a		<u>(d) information security and/or incident response operations;</u>	<u>(d) information security and/or incident response operations;</u> <div>Text Origin: Council Mandate</div>	Y
Article 8(3), point(ca)					
Y	119b		<u>(ca) ethics;</u>	<u>(da) ethics;</u> <div>Text Origin: EP Mandate</div>	Y
Article 8(3), point(e)					
Y	119c		<u>(e) scientific or technical partnerships or cooperation with academic and/or public authorities.</u>	Presidency to confirm whether it can be deleted	Y
Article 8(3), point(cb)					
Y	119d		<u>(cb) formal and technical standardisation and specifications.</u>	<u>(cd) formal and technical standardisation and specifications.</u> <div>addition agreed but Council to check with MS</div> <div>Text Origin: EP Mandate</div>	Y

Article 8(4)						
Y	120	<p>4. The Competence Centre shall accredit entities established under national law as members of the Cybersecurity Competence Community after an assessment made by the National Coordination Centre of the Member State where the entity is established, on whether that entity meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it or the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation].</p>	<p>4. The Competence Centre shall accredit entities established under national law, <u>or individuals</u>, as members of the Cybersecurity Competence Community after <u>a harmonised</u> an assessment made by the <u>Competence Centre, the</u> National Coordination Centre of the Member State where the entity is established, <u>or the individual is a resident</u>, on whether that entity meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it or the relevant National Coordination Centre considers that the entity <u>or individual</u> does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation]. <u>The National Coordination Centres of the Member States shall aim to achieve a balanced representation of stakeholders in the Community, actively stimulating participation from under-represented categories, especially SMEs, and groups of individuals.</u></p>	<p>4. The Competence Centre shall accredit <u>register</u> entities established under national law as members of the Cybersecurity Competence Community after an assessment made by the National Coordination Centre of the Member State where the entity is established, on <u>of</u> whether that entity meets the criteria provided for in paragraph 3 <u>of this Article. That assessment shall also take into account, where relevant, any national assessment on security grounds made by the national competent authorities. A registration.</u> An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it or the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 <u>of this Article</u> or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation] <u>(EU, Euratom) 2018/1046, or for justified security reasons.</u></p>	<p>4. The Competence Centre shall accredit <u>register</u> entities established under national law as members of the Cybersecurity Competence Community after an assessment made by the National Coordination Centre of the Member State where the entity is established, on <u>of</u> whether that entity meets the criteria provided for in paragraph 3 <u>of this Article. That assessment shall also take into account, where relevant, any national assessment on security grounds made by the national competent authorities. A registration.</u> An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it or the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 <u>of this Article</u> or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation] <u>(EU, Euratom) 2018/1046, or for justified security reasons.</u> <u>Where Community membership is revoked on security grounds, such a decision shall be proportional and justified.</u> <u>The National Coordination Centres of the Member States shall aim to achieve a balanced representation of stakeholders in the Community actively stimulating participation from SMEs in particular.</u></p> <p>COM to check regarding EFTA countries.</p>	Y

Article 8(4a)				
Y	120a		<p><u>4a. The Commission shall adopt delegated acts in accordance with Article 45a in order to supplement this Regulation by detailing the criteria provided for in paragraph 3 of this Article according to which applicants are selected, and the procedures for assessing and accrediting entities that meet the criteria referred to in paragraph 4 of this Article.</u></p>	<p><u>4a. The Centre shall register relevant Union bodies, agencies and offices as members of the Cybersecurity Competence Community after carrying out an assessment whether that Union body, agency or office meets the criteria provided for in paragraph 3 of this Article. A registration shall not be limited in time but may be revoked by the Competence Centre at any time if it considers that the Union body, agency or office does not fulfil the criteria set out in paragraph 3 of this Article or falls under the relevant provisions set out in Article 136 of (EU, Euratom) 2018/1046, or for justified security reasons following an assessment by the Commission.</u></p> <p>Council proposes to move to recital</p> <p>Possible item for Political Trilogue (harmonisation of criteria for NCC)</p>
Article 8(5)				
Y	121	<p>5. The Competence Centre shall accredit relevant bodies, agencies and offices of the Union as members of the Cybersecurity Competence Community after carrying out an assessment whether that entity meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it considers that the entity does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation].</p>	<p>5. The Competence Centre shall accredit relevant bodies, agencies and offices of the Union as members of the Cybersecurity Competence Community after carrying out an assessment whether that entity meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it considers that the entity does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation].</p>	<p>5. The Competence Centre shall accredit relevant bodies <u>representatives of the Union institutions</u>, agencies and offices of the Union as members <u>bodies may participate in the work</u> of the Cybersecurity Competence Community after carrying out an assessment whether that entity meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it considers that the entity does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation].</p> <p>5. The Competence Centre shall <u>register relevant Union-accredited relevant</u> bodies, agencies and offices of the Union as members of the Cybersecurity Competence Community after carrying out an assessment whether that entity <u>Union body, agency or office</u> meets the criteria provided for in paragraph 3 <u>of this Article</u>. A registration. An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it considers that the entity <u>Union body, agency or office</u> does not fulfil the criteria set out in paragraph <u>3 of this Article or 3</u> or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new</p>

				<p>financial regulation <u>(EU, Euratom) 2018/1046 I, or for justified security reasons following an assessment by the Commission]</u>.</p> <p>Commission suggests to delete part in square brackets</p>
Article 8(6)				
Y	122	<p>6. The representatives of the Commission may participate in the work of the Community.</p>	<p>6. The representatives of the Commission may participate in the work of the Community.</p>	<p>6. The <u>Cybersecurity Competence Community shall designate its own representatives to ensure an efficient and regular dialogue and cooperation with the Centre at Union level.</u> Representatives of the Commission may participate in the work of the Community <u>Cybersecurity Competence Community shall have expertise with regard to cybersecurity research, technology and industry. The representation of the Cybersecurity Competence Community shall be balanced between scientific, industrial and civil society entities, demand and supply side industries, large and small and medium enterprises, as well as in terms of geographical provenance and gender as well as intra-sectorial balance. The requirements and number of representatives shall be further specified by the Governing Board.</u></p> <p><u>Representatives of the Cybersecurity Competence Community shall have expertise with regard to cybersecurity research, technology and industry. The representation of the Cybersecurity Competence Community shall be balanced between scientific, industrial and civil society entities, demand and supply side industries, large and small and medium enterprises, as well as in terms of geographical provenance and gender as well as intra-sectorial balance. The requirements and number of representatives shall be further specified by the Governing Board.</u></p> <p>Commission to provide updated text; merge with 115? EP comment: pending agreement on advisory board/community representation (same for 122a)</p>

Article 8(7)				
Y	122a		<u>7. The Cybersecurity Competence Community shall through its representatives provide to the Executive Director and the Governing Board strategic advice on the Agenda, annual and multiannual work programme in accordance with the rules of procedure set by the Governing Board. The Cybersecurity Competence Community shall also promote and collect feedback on the annual work programme and the multiannual work programme.</u>	<u>6a. [The Cybersecurity Competence Community shall through its representatives provide to the Executive Director and the Governing Board strategic advice on the Agenda, annual and multiannual work programme in accordance with the rules of procedure set by the Governing Board. The Cybersecurity Competence Community shall also promote and collect feedback on the annual work programme and the multiannual work programme.]</u> Text Origin: Council Mandate
Article 9				
G	123	Article 9 Tasks of the members of the Cybersecurity Competence Community	Article 9 Tasks of the members of the Cybersecurity Competence Community	Article 9 Tasks of the members of the Cybersecurity Competence Community Text Origin: Commission Proposal
Article 9, first paragraph, introductory part				
G	124	The members of the Cybersecurity Competence Community shall:	The members of the Cybersecurity Competence Community shall:	The members of the Cybersecurity Competence Community shall: Text Origin: Commission Proposal

Article 9(1), point(1)				
Y	125	(1) support the Competence Centre in achieving the mission and the objectives laid down in Articles 3 and 4 and, for this purpose, work closely with the Competence Centre and the relevant National Coordinating Centres;	(1) support the Competence Centre in achieving the mission and the objectives laid down in Articles 3 and 4 and, for this purpose, work closely with the Competence Centre and the relevant National Coordinating Centres;	(1) support the Competence Centre in achieving the mission and the objectives laid down in Articles 3 and 4 and, for this purpose, work closely with the Competence Centre and the relevant National Coordinating <u>Coordination</u> Centres; use of 'Competence' Text Origin: Council Mandate
Article 9(1), point(2)				
Y	126	(2) participate in activities promoted by the Competence Centre and National Coordination Centres;	(2) participate in activities promoted by the Competence Centre and National Coordination Centres;	(2) participate in activities promoted by the Competence Centre and National Coordination Centres; Deleted
Article 9(1), point(3)				
G	127	(3) where relevant, participate in working groups established by the Governing Board of the Competence Centre to carry out specific activities as provided by the Competence Centre's work plan;	(3) where relevant, participate in working groups established by the Governing Board of the Competence Centre to carry out specific activities as provided by the Competence Centre's work plan;	(3) where relevant, participate in <u>formal or informal activities and in the</u> working groups <u>referred to in point (i) of Article 13(3)-established by the Governing Board of the Competence Centre</u> to carry out specific activities as provided by the Competence Centre's work plan <u>annual work programme;</u> ; Text Origin: Council Mandate

Article 9(1), point(4)				
Y	128	(4) where relevant, support the Competence Centre and the National Coordination Centres in promoting specific projects;	(4) where relevant, support the Competence Centre and the National Coordination Centres in promoting specific projects;	(4) where relevant, support the Competence Centre and the National Coordination Centres in promoting specific projects; use of 'Competence' Text Origin: Commission Proposal
Article 9(1), point(5)				
G	129	(5) promote and disseminate the relevant outcomes of the activities and projects carried out within the community.	(5) promote and disseminate the relevant outcomes of the activities and projects carried out within the community.	(5) promote and disseminate the relevant outcomes of the activities and projects carried out within the <u>Cybersecurity Competence</u> Community. Text Origin: Council Mandate
Article 9, first paragraph, point(5a)				
Y	129a		<u>(5a) support the Competence Centre by reporting and disclosing vulnerabilities, helping to mitigate them and providing advice on how to reduce such vulnerabilities including through certification under the schemes adopted in conformity with Regulation (EU) 2019/XXX [the Cybersecurity Act].</u>	Agree to move to recital. COM to provide wording. addendum: difficult for MS even in recitals: Exact wording proposal will need to be assessed; no active direct role of Centre in this matter.

Article 10						
Y	130	Article 10 Cooperation of the Competence Centre with Union institutions, bodies, offices and agencies	Article 10 Cooperation of the Competence Centre with Union institutions, bodies, offices and agencies	Article 10 Cooperation of the Competence Centre with Union institutions, bodies, offices and agencies <u>and international organisations</u> use of 'Competence' Text Origin: Council Mandate	Y	
Article 10(1)						
Y	131	1. The Competence Centre shall cooperate with relevant Union institutions, bodies, offices and agencies including the European Union Agency for Network and Information Security, the Computer Emergency Response Team (CERT-EU), the European External Action Service, the Joint Research Centre of the Commission, the Research Executive Agency, Innovation and Networks Executive Agency, European Cybercrime Centre at Europol as well as the European Defence Agency.	1. <u>To ensure coherence and complementarity,</u> the Competence Centre shall cooperate with relevant Union institutions, bodies, offices and agencies including the European Union Agency for Network and Information Security <u>ENISA</u> , the Computer Emergency Response Team (CERT-EU), the European External Action Service, the Joint Research Centre of the Commission, the Research Executive Agency, Innovation and Networks Executive Agency, <u>relevant European Digital Innovation Hubs</u> , European Cybercrime Centre at Europol as well as the European Defence Agency <u>as regards dual-use projects, services and competences</u> .	1. The Competence <u>To ensure coherence and complementarity, avoiding any duplication of efforts the</u> Centre shall cooperate with relevant Union institutions, bodies, offices and agencies including the European Union Agency for Network and Information Security <u>ENISA</u> , the Computer Emergency Response Team (CERT-EU), the European External Action Service, the Joint Research Centre of the Commission, the Research Executive Agency <u>established by Commission Implementing Decision 2013/778/EU¹, the</u> Innovation and Networks Executive Agency <u>established by Commission Implementing Decision 2013/801/EU², the</u> European Cybercrime Centre at <u>the European Union Agency for Law Enforcement Cooperation (Europol) established by Regulation (EU) 2016/794 of the European Parliament and of the Council³, as well as</u> the European Defence Agency <u>and other relevant Union entities. The Centre may also cooperate with international organisations, where</u>	1. The Competence <u>To ensure coherence and complementarity, avoiding any duplication of efforts the</u> Centre shall cooperate with relevant Union institutions, bodies, offices and agencies including the European Union Agency for Network and Information Security <u>ENISA</u> , the Computer Emergency Response Team (CERT-EU), the European External Action Service, the Joint Research Centre of the Commission, the Research Executive Agency <u>established by Commission Implementing Decision 2013/778/EU¹, the</u> Innovation and Networks Executive Agency <u>established by Commission Implementing Decision 2013/801/EU², relevant European Digital Innovation Hubs, the</u> European Cybercrime Centre at <u>the European Union Agency for Law Enforcement Cooperation (Europol) established by Regulation (EU) 2016/794 of the European Parliament and of the Council³, as well as</u> the European Defence Agency <u>as regards dual-use projects,</u>	Y

			<p><u>relevant.</u></p> <p><u>1. [1] Commission Implementing Decision 2013/778/EU of 13 December 2013 establishing the Research Executive Agency and repealing Decision 2008/46/EC (OJ 346, 20.12.2013, p. 54).</u></p> <p><u>2. [2] Commission Implementing Decision 2013/801/EU of 23 December 2013 establishing the Innovation and Networks Executive Agency and repealing Decision 2007/60/EC as amended by Decision 2008/593/EC (OJ 352, 24.12.2013, p. 65).</u></p> <p><u>3. [3] 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).</u></p>	<p><u>services and competences, and other relevant Union entities. The Centre may also cooperate with international organisations, where relevant.</u></p> <p><u>1. [1] Commission Implementing Decision 2013/778/EU of 13 December 2013 establishing the Research Executive Agency and repealing Decision 2008/46/EC (OJ 346, 20.12.2013, p. 54).</u></p> <p><u>2. [2] Commission Implementing Decision 2013/801/EU of 23 December 2013 establishing the Innovation and Networks Executive Agency and repealing Decision 2007/60/EC as amended by Decision 2008/593/EC (OJ 352, 24.12.2013, p. 65).</u></p> <p><u>3. [3] 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).</u></p> <p>Presidency to check with MS EP addition of dual use</p> <p>Text Origin: Council Mandate</p>
--	--	--	---	---

Article 10(2)				
Y	132	2. Such cooperation shall take place within the framework of working arrangements. Those arrangements shall be submitted to the prior approval of the Commission.	2. Such cooperation shall take place within the framework of working arrangements. Those arrangements shall be submitted to the <u>adopted by the Governing Board after</u> prior approval of the Commission.	2. Such cooperation shall take place within the framework of working arrangements. Those arrangements shall be submitted to the prior approval of the <u>Governing Board-Commission</u> . prior Commission approval yes/no? EP and Presidency does not see the need for a prior approval by COM because COM is part of the governing board, redundant. Depends on discussion regarding voting rights Text Origin: Council Mandate
CHAPTER II				
Y	133	CHAPTER II ORGANISATION OF THE COMPETENCE CENTRE	CHAPTER II ORGANISATION OF THE COMPETENCE CENTRE	CHAPTER II ORGANISATION OF THE COMPETENCE CENTRE use of 'Competence' Text Origin: Commission Proposal
Article 11				
G	134	Article 11 Membership and structure	Article 11 Membership and structure	Article 11 Membership and structure Text Origin: Commission Proposal

Article 11(1)				
Y	135	1. The members of the Competence Centre shall be the Union, represented by the Commission, and the Member States.	1. The members of the Competence Centre shall be the Union, represented by the Commission, and the Member States.	1. The members of the Competence Centre shall be the Union, represented by the Commission, and the Member States. use of 'Competence' Text Origin: Commission Proposal
Article 11(2), introductory part				
Y	136	2. The structure of the Competence Centre shall comprise:	2. The structure of the Competence Centre shall comprise:	2. The structure of the Competence Centre shall [be conducive to/ensure] the achievement of the objectives set out in Article 4 and tasks set out in Article 4a, and comprise: To be re-discussed, linked to other issues as the Agenda, voting rights and Advisory Board Council preference for “shall ensure the achievement”. Commission sceptical use of 'Competence' Text Origin: Council Mandate
Article 11(2), point(a)				
G	137	(a) a Governing Board which shall exercise the tasks set out in Article 13;	(a) a Governing Board which shall exercise the tasks set out in Article 13;	(a) a Governing Board which shall exercise the tasks set out in Article 13; Text Origin: Commission Proposal

Article 11(2), point(b)				
Y	138	(b) an Executive Director who shall exercise the tasks set out in Article 16;	(b) an Executive Director who shall exercise the tasks set out in Article 16;	(b) an Executive Director who shall exercise the tasks set out in Article 16 ¹⁷ ; COM to come with text proposal regarding the staff. Text Origin: Council Mandate
Article 11(2), point(c)				
R	139	(c) an Industrial and Scientific Advisory Board which shall exercise the functions set out in Article 20.	(c) an Industrial and Scientific Advisory Board which shall exercise the functions set out in Article 20.	<div>deleted</div> Advisory board
CHAPTER II, SECTION I				
G	140	SECTION I GOVERNING BOARD	SECTION I GOVERNING BOARD	SECTION I GOVERNING BOARD Text Origin: Commission Proposal
Article 12				
G	141	Article 12 Composition of the Governing Board	Article 12 Composition of the Governing Board	Article 12 Composition of the Governing Board Text Origin: Commission Proposal

Article 12(1)				
Y	142	1. The Governing Board shall be composed of one representative of each Member State, and five representatives of the Commission, on behalf of the Union.	1. The Governing Board shall be composed of one representative of each Member State, <u>one representative nominated by the European Parliament as an observer, and four-and-five</u> representatives of the Commission, on behalf of the Union, <u>aiming to achieve gender balance among board members and their alternates</u> .	1. The Governing Board shall be composed of one representative of each Member State, and five <u>two</u> representatives of the Commission, on behalf of the Union. gender balance aim mentioned in 144 Brackets pending clarification on what the representative might do. EP to come back
Article 12(2)				
G	143	2. Each member of the Governing Board shall have an alternate to represent them in their absence.	2. Each member of the Governing Board shall have an alternate to represent them in their absence.	2. Each member of the Governing Board shall have an alternate to represent them in their absence. Text Origin: Commission Proposal
Article 12(2a)				
Y	143a		<u>2a. Members of the Governing Board and their alternates shall possess adequate knowledge in the field of cybersecurity.</u>	Suggestion to insert in 144

Article 12(3)						
Y	144	<p>3. Members of the Governing Board and their alternates shall be appointed in light of their knowledge in the field of technology as well as of relevant managerial, administrative and budgetary skills. The Commission and the Member States shall make efforts to limit the turnover of their representatives in the Governing Board, in order to ensure continuity of the Board’s work. The Commission and the Member States shall aim to achieve a balanced representation between men and women on the Governing Board.</p>	<p>3. Members of the Governing Board and their alternates shall be appointed in light of their knowledge in the field of technology <u>cybersecurity</u> as well as of relevant managerial, administrative and budgetary skills. The Commission and the Member States shall make efforts to limit the turnover of their representatives in the Governing Board, in order to ensure continuity of the Board’s work. The Commission and the Member States shall aim to achieve a balanced representation between men and women on the Governing Board.</p>	<p>3. Members of the Governing Board and their alternates <u>appointed by Member States</u> shall be appointed in<u>employees of their respective Member State’s public sector appointed in</u> light of their knowledge in the field of technology, <u>their interlink with their respective National Coordination Centre or their relevant managerial, administrative and budgetary skills. Members of the Governing Board and their alternates appointed by the Commission shall be appointed in light of their knowledge in the field of technology, or their</u> as well as of relevant managerial, administrative and budgetary skills <u>and of their capacity to ensure coordination, synergies and, as far as possible, joint initiatives between different Union policies (sectoral and horizontal), involving cybersecurity</u>. The Commission and the Member States shall make efforts to limit the turnover of their representatives in the Governing Board, in order to ensure continuity of the Board’s work. The Commission and the Member States shall aim to achieve a balanced representation between men and women on the Governing Board.</p>	<p>3. Members of the Governing Board and their alternates <u>appointed by Member States</u> shall be <u>employees of their respective Member State’s public sector,</u> appointed in light of their knowledge in the field of <u>cybersecurity,</u> technology, <u>their interlink with their respective National Coordination Centre or their relevant managerial, administrative and budgetary skills. Members of the Governing Board and their alternates appointed by the Commission shall be appointed in light of their knowledge in the field of cybersecurity, technology, or their</u> as well as of relevant managerial, administrative and budgetary skills <u>and of their capacity to ensure coordination, synergies and, as far as possible, joint initiatives between different Union policies (sectoral and horizontal), involving cybersecurity</u>. The Commission and the Member States shall make efforts to limit the turnover of their representatives in the Governing Board, in order to ensure continuity of the Board’s work. The Commission and the Member States shall aim to achieve a balanced representation between men and women on the Governing Board.</p>	Y

Article 12(4)				
G	145	4. The term of office of members of the Governing Board and of their alternates shall be four years. That term shall be renewable.	4. The term of office of members of the Governing Board and of their alternates shall be four years. That term shall be renewable.	4. The term of office of members of the Governing Board and of their alternates shall be four years. That term shall be renewable. Text Origin: Commission Proposal
Article 12(5)				
G	146	5. The Governing Board members shall act in the interest of the Competence Centre, safeguarding its goals and mission, identity, autonomy and coherence, in an independent and transparent way.	5. The Governing Board members shall act in the interest of the Competence Centre, safeguarding its goals and mission, identity, autonomy and coherence, in an independent and transparent way.	5. The Governing Board members <u>members of the Governing Board</u> shall act in the interest of the Competence to <u>safeguard the</u> Centre, safeguarding its <u>'s</u> goals and mission, identity, autonomy and coherence, in an independent and transparent way. Text Origin: Council Mandate
Article 12(6)				
G	147	6. The Commission may invite observers, including representatives of relevant Union bodies, offices and agencies, to take part in the meetings of the Governing Board as appropriate.	6. The Governing Board-Commission may invite observers, including representatives of relevant Union bodies, offices and agencies, <u>and the members of the Community</u> , to take part in the meetings of the Governing Board as appropriate.	6. The Commission <u>Governing Board</u> may invite observers, including representatives of relevant Union bodies, offices and agencies, to take part in the meetings of the Governing Board as appropriate. Text Origin: EP Mandate

Article 12(7)				
Y	148	7. The European Agency for Network and Information Security (ENISA) shall be a permanent observer in the Governing Board.	7. The European Agency for Network and Information Security (ENISA) <u>ENISA, and the Industrial and Scientific Advisory Board</u> , shall be <u>permanent observers in the Governing Board, in an advisory role without voting rights.</u> a permanent observer in The Governing Board <u>shall have the utmost regard to the views expressed by the permanent observers.</u>	7. The European Agency for Network and Information Security (ENISA) shall be a permanent observer in the Governing Board. 7. <u>A representative from ENISA shall be a permanent observer in the Governing Board. [The Governing Board may invite a representative from the Industrial and Scientific Advisory Board].</u> <u>7a. The Executive Director shall take part</u> The European Agency for Network and Information Security (ENISA) shall be a permanent observer in the <u>meetings of the</u> Governing Board <u>but shall have no right to vote.</u> Council check with MS
Article 13				
G	149	Article 13 Tasks of the Governing Board	Article 13 Tasks of the Governing Board	Article 13 Tasks of the Governing Board Text Origin: Commission Proposal

Article 13(1)				
Y	150	1. The Governing Board shall have the overall responsibility for the strategic orientation and the operations of the Competence Centre and shall supervise the implementation of its activities.	1. The Governing Board shall have the overall responsibility for the strategic orientation and the operations of the Competence Centre and shall supervise the implementation of its activities.	1. The Governing Board shall have the overall responsibility for the strategic orientation and the operations of the Competence Centre and shall supervise the implementation of its activities <u>and shall be responsible for any task that is not specifically allocated to the Executive Director.</u> COM to check wording in ENISA Regulation. Text Origin: Council Mandate
Article 13(2)				
G	151	2. The Governing Board shall adopt its rules of procedure. These rules shall include specific procedures for identifying and avoiding conflicts of interest and ensure the confidentiality of any sensitive information.	2. The Governing Board shall adopt its rules of procedure. These rules shall include specific procedures for identifying and avoiding conflicts of interest and ensure the confidentiality of any sensitive information.	2. The Governing Board shall adopt its rules of procedure. These rules shall include specific procedures for identifying and avoiding conflicts of interest and ensure the confidentiality of any sensitive information. Text Origin: Commission Proposal
Article 13(3), introductory part				
G	152	3. The Governing Board shall take the necessary strategic decisions, in particular:	3. The Governing Board shall take the necessary strategic decisions, in particular:	3. The Governing Board shall take the necessary strategic decisions, in particular: Text Origin: Commission Proposal

Article 13(3), point(a)					
Y	153	(a) adopt a multi-annual strategic plan, containing a statement of the major priorities and planned initiatives of the Competence Centre, including an estimate of financing needs and sources;	(a) adopt a multi-annual strategic plan, containing a statement of the major priorities and planned initiatives of the Competence Centre, including an estimate of financing needs and sources, <u>taking into account advice provided by ENISA</u> ;	(a) adopt a multi-annual strategic plan, containing a statement of the major priorities and planned initiatives <u>develop and adopt the Agenda encompassing strategic goals and priorities for a sustainable development</u> of the Competence Centre, including an estimate of financing needs and sources <u>European cybersecurity research, technological and industrial sector and monitor its implementation</u> ; Text Origin: Council Mandate	Y
Article 13(3), point(aa)					
Y	153a		<u>(aa) based on the Agenda, adopt the multiannual work programme containing the development of common, industrial, technology and research strategic priorities , which are based on the needs identified by Member States in cooperation with the Cybersecurity Competence Community and which require the focus of Union's financial support. Such priorities shall include key technologies and domains for developing the Union's own capabilities in cybersecurity</u> ;	<u>(aa) based on the Agenda, adopt the multiannual work programme which are based on the needs identified by Member States in cooperation with the Cybersecurity Competence Community and which require the focus of Union's financial support. Such priorities shall include key technologies and domains for developing the Union's own capabilities in cybersecurity</u> ; PR and COM to redraft (streamline definition of Agenda). Add role for ENISA Text Origin: Council Mandate	Y

Article 13(3), point(aaa)					
Y	153b		<p><u>(aaa) adopt the annual work programme for implementing the relevant Union funds, notably the cybersecurity parts of the Horizon Europe programme and the Digital Europe programme, in accordance with the Centre's multiannual work programme and the strategic planning process of the Horizon Europe programme; Where appropriate, proposals and in particular the annual work programme shall assess the need to apply security rules as set out in Article 34 of this Regulation, including in particular the security self-assessment procedure in accordance with Article 16 of the [XXXX Horizon Europe Regulation];</u></p>	<p><u>(ab) adopt the annual work programme for implementing the relevant Union funds, notably the cybersecurity parts of the Horizon Europe programme and the Digital Europe programme, in accordance with the Centre's multiannual work programme and the strategic planning process of the Horizon Europe programme; Where appropriate, proposals and in particular the annual work programme shall assess the need to apply security rules as set out in Article 34 of this Regulation, including in particular the security self-assessment procedure in accordance with Article 16 of the [XXXX Horizon Europe Regulation];</u></p> <p>COM to check compliance with Horizon Europe</p> <p>Text Origin: Council Mandate</p>	Y
Article 13(3), point(b)					
Y	154	<p>(b) adopt the Competence Centre's work plan, annual accounts and balance sheet and annual activity report, on the basis of a proposal from the Executive Director;</p>	<p>(b) adopt the Competence Centre's work plan, annual accounts and balance sheet and annual activity report, on the basis of a proposal from the Executive Director, <u>taking into account advice provided by ENISA;</u></p>	<p>(b) adopt the Competence Centre's work plan;s annual accounts and balance sheet and annual activity report, on the basis of a proposal from the Executive Director;</p> <p>To be moved to 153a</p>	Y

Article 13(3), point(c)				
Y	155	(c) adopt the specific financial rules of the Competence Centre in accordance with [Article 70 of the FR];	(c) adopt the specific financial rules of the Competence Centre in accordance with [Article 70 of the FR];	(c) adopt the specific financial rules of the Competence Centre in accordance with [Article 70 of the FR <u>Regulation (EU, Euratom) 2018/1046</u>]; <u>as part of the annual work programme adopt decisions to allocate funds from the Union budget to joint actions between the Union and Member States;</u> Text Origin: Council Mandate
Article 13(3), point(ca)				
Y	155a			<u>(ca) as part of the annual work programme adopt decisions to allocate funds from the Union budget to joint actions between the Union and Member States;</u> Text Origin: Council Mandate
Article 13(3), point(cb)				
Y	155b			<u>(cb) as part of the annual work programme and in accordance with the decisions referred to in point (ca), and in compliance with the regulations establishing Horizon Europe and the Digital Europe Programme, adopt decisions relating to the description of the joint actions referred to in point (ca) and lay down conditions for their implementation.</u> EP to check possible changes Text Origin: Council Mandate

Article 13(3), point(d)				
G	156	(d) adopt a procedure for appointing the Executive Director;	(d) adopt a procedure for appointing the Executive Director;	(d) adopt a procedure for appointing the Executive Director; Text Origin: Commission Proposal
Article 13(3), point(e)				
	157	(e) adopt the criteria and procedures for assessing and accrediting the entities as members of the Cybersecurity Competence Community;	(e) adopt the criteria and procedures for assessing and accrediting the entities as members of the Cybersecurity Competence Community ;	(e) adopt the criteria and procedures for assessing and accrediting the entities as members of the Cybersecurity Competence Community ; COM to check whether in line with procedure for assessing entities of the Community
Article 13(3), point(ea)				
Y	157a		<u>(ea) adopt the working arrangements referred to in Article 10(2);</u>	<u>(ea) adopt the working arrangements referred to in Article 10(2);</u> Text Origin: EP Mandate
Article 13(3), point(f)				
G	158	(f) appoint, dismiss, extend the term of office of, provide guidance to and monitor the performance of the Executive Director, and appoint the Accounting Officer;	(f) appoint, dismiss, extend the term of office of, provide guidance to and monitor the performance of the Executive Director, and appoint the Accounting Officer;	(f) appoint, dismiss, extend the term of office of, provide guidance to and monitor the performance of the Executive Director, and appoint the Accounting Officer; Text Origin: Commission Proposal

Article 13(3), point(g)				
Y	159	(g) adopt the annual budget of the Competence Centre, including the corresponding staff establishment plan indicating the number of temporary posts by function group and by grade, the number of contract staff and seconded national experts expressed in full-time equivalents	(g) adopt the annual budget of the Competence Centre, including the corresponding staff establishment plan indicating the number of temporary posts by function group and by grade, the number of contract staff and seconded national experts expressed in full-time equivalents	(g) adopt the annual budget of the Competence Centre, including the corresponding staff establishment plan indicating the number of temporary posts by function group and by grade, and the number of contract staff and seconded national experts expressed in full-time equivalents; use of 'Competence' Text Origin: Council Mandate
Article 13(3), point(ga)				
Y	159a		<u>(ga) adopt transparency rules for the Competence Centre;</u>	Tentative agreement to move to 160
Article 13(3), point(h)				
Y	160	(h) adopt rules regarding conflicts of interest;	(h) adopt rules regarding conflicts of interest	(h) adopt <u>transparency</u> rules regarding for the prevention and management of conflicts of interest <u>in respect of its members</u> ; Commission to check part in brackets

Article 13(3), point(i)				
161	(i) establish working groups with members of the Cybersecurity Competence Community;	(i) establish working groups with members of the <u>Community, taking into account advice provided by the permanent observers</u> Cybersecurity Competence Community ;	(i) establish working groups with members of <u>when appropriate, provide advice to the Cybersecurity Competence Community with regard to the establishment of working groups by</u> the Cybersecurity Competence Community <u>and assist in the coordination of such groups</u> ;	Commission/EP to propose text; addition of advice from ENISA agreed
Article 13(3), point(j)				
162	(j) appoint members of the Industrial and Scientific Advisory Board;	(j) appoint members of the Industrial and Scientific Advisory Board;	(j) appoint members of the Industrial and Scientific Advisory Board ;	Advisory board
Article 13(3), point(k)				
G 163	(k) set up an Internal Auditing Function in accordance with Commission Delegated Regulation (EU) No 1271/2013 ¹ ; 1. Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council (OJ L 328, 7.12.2013, p. 42).	(k) set up an Internal Auditing Function in accordance with Commission Delegated Regulation (EU) No 1271/2013 ¹ ; 1. Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council (OJ L 328, 7.12.2013, p. 42).	(k) set up an Internal Auditing Function in accordance with Commission Delegated Regulation (EU) No 1271/2013 ¹ ; 1. <u>III</u> Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council (OJ L 328, 7.12.2013, p. 42).	(k) set up an Internal Auditing Function in accordance with Commission Delegated Regulation (EU) No 1271/2013 ¹ ; 1. Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council (OJ L 328, 7.12.2013, p. 42). Text Origin: Commission Proposal

Article 13(3), point(l)				
164	(l) promote the Competence Centre globally, so as to raise its attractiveness and make it a world-class body for excellence in cybersecurity;	(l) promote the Competence Centre globally, so as to raise its attractiveness and make it a world-class body for excellence in cybersecurity <u>cooperation of the Competence Centre with global actors</u> ;	(l) promote the Competence <u>set up a monitoring mechanism to ensure that the implementation of the respective funds managed by the</u> Centre globally, so as to raise its attractiveness and make it a world-class body for excellence in cybersecurity <u>is done in accordance with the Agenda, the mission and the multiannual work programme and with the rules of programmes where funding originates from</u> ;	Presidency to suggest wording on agenda, Commission to check Possible wording discussed: 'monitor that the implementation of funds is managed by the Centre in accordance with the Agenda....'
Article 13(3), point(la)				
Y 164a			<u>(la) ensure a regular dialogue and establish an effective cooperation mechanism with the Cybersecurity Competence Community</u> ;	<u>(la) ensure a regular dialogue and establish an effective cooperation mechanism with the Cybersecurity Competence Community</u> ; Advisory board Text Origin: Council Mandate
Article 13(3), point(m)				
Y 165	(m) establish the Competence Centre's communications policy upon recommendation by the Executive Director;	(m) establish the Competence Centre's communications policy upon recommendation by the Executive Director;	(m) establish the Competence Centre's communications policy upon recommendation by the Executive Director;	(m) establish the Competence Centre's communications policy upon recommendation by the Executive Director; use of 'Competence' Text Origin: Commission Proposal

Article 13(3), point(n)				
G	166	(n) be responsible to monitor the adequate follow-up of the conclusions of retrospective evaluations.	(n) be responsible to monitor the adequate follow-up of the conclusions of retrospective evaluations.	(n) be responsible to monitor the adequate follow-up of the conclusions of retrospective evaluations. Text Origin: Commission Proposal
Article 13(3), point(o)				
G	167	(o) where appropriate, establish implementing rules to the Staff Regulations and the Conditions of Employment in accordance with Article 31(3);	(o) where appropriate, establish implementing rules to the Staff Regulations and the Conditions of Employment in accordance with Article 31(3);	(o) where appropriate, establish implementing rules to the Staff Regulations and the Conditions of Employment in accordance with Article 31(3); Text Origin: Commission Proposal
Article 13(3), point(p)				
Y	168	(p) where appropriate, lay down rules on the secondment of national experts to the Competence Centre and on the use of trainees in accordance with Article 32(2);	(p) where appropriate, lay down rules on the secondment of national experts to the Competence Centre and on the use of trainees in accordance with Article 32(2);	(p) where appropriate, lay down rules on the secondment of national experts to the Competence Centre and on the use of trainees in accordance with Article 32(2); use of 'Competence' Text Origin: Commission Proposal

Article 13(3), point(q)					
Y	169	(q) adopt security rules for the Competence Centre;	(q) adopt security rules for the Competence Centre;	(q) adopt security rules for the Competence Centre; use of 'Competence' Text Origin: Commission Proposal	Y
Article 13(3), point(r)					
G	170	(r) adopt an anti-fraud strategy that is proportionate to the fraud risks having regard to a cost-benefit analysis of the measures to be implemented;	(r) adopt an anti-fraud <u>and anti-corruption</u> strategy that is proportionate to the fraud <u>and corruption</u> risks having regard to a cost-benefit analysis of the measures to be implemented, <u>as well as adopt comprehensive protection measures for persons reporting on breaches of Union law in accordance with applicable Union legislation</u> ;	(r) adopt an anti-fraud <u>and anti-corruption</u> strategy that is proportionate to the fraud <u>and corruption</u> risks <u>as well as adopt comprehensive protection measures for persons reporting on breaches of Union law in accordance with applicable Union legislation</u> , having regard to a cost-benefit analysis of the measures to be implemented; Text Origin: EP Mandate	G

Article 13(3), point(s)				
171	(s) adopt the methodology to calculate the financial contribution from Member States;	(s) adopt <u>an extensive definition of financial contributions from Member States and a the methodology to calculate the amount of Member States' voluntary contributions that can be accounted for as financial contribution from Member States contributions in accordance with that definition, such a calculation being executed at the end of every financial year;</u>	(s) adopt the methodology to calculate the <u>voluntary</u> financial <u>and in-kind</u> contribution from <u>contributing</u> Member States <u>in accordance with Horizon Europe and Digital Europe Regulations</u> ;	(s) <u>/adopt the methodology to calculate the voluntary financial and in-kind contribution from contributing Member States in accordance with Horizon Europe and Digital Europe Regulations. The calculation is being executed at the end of every financial year;]</u> Presidency proposed merged text Commission comment: no rules in DEP, finreg applies text in brackets, COM and EP to check. Commission reservation on voluntary contributions; for EP ok.
Article 13(3), point(sa)				
G 171a			<u>(sa) register entities nominated by Member States as their National Coordination Centres;</u>	<u>(sa) register entities notified by Member States as their National Coordination Centres;</u> Text Origin: Council Mandate

Article 13(3), point(sb)				
Y	171b		<u>(sb) in deciding on the annual work programme and the multiannual work programme, ensure coherence and synergies with those parts of the Digital Europe programme and the Horizon Europe programme which are not managed by the Centre, as well as with other Union programmes;</u>	<u>(sb) in deciding on the annual work programme and the multiannual work programme, ensure coherence and synergies with those parts of the Digital Europe programme and the Horizon Europe programme which are not managed by the Centre, as well as with other Union programmes;</u> Text Origin: Council Mandate
Article 13(3), point(t)				
G	172	(t) be responsible for any task that is not specifically allocated to a particular body of the Competence Centre; it may assign such tasks to anybody of the Competence Centre;	(t) be responsible for any task that is not specifically allocated to a particular body of the Competence Centre; it may assign such tasks to anybody of the Competence Centre;	(t) be responsible for any task that is not specifically allocated to a particular body of the Competence Centre; it may assign such tasks to anybody of the Competence Centre; in line 150 Text Origin: Council Mandate
Article 13(3), point(u)				
G	172a		<u>(u) discuss and adopt the annual report on the implementation of the Centre's strategic goals and priorities with a recommendation, if necessary, for their better realisation</u>	<u>(ta) discuss and adopt the annual report on the implementation of the Centre's strategic goals and priorities with a recommendation, if necessary, for their better realisation</u> Laywer-linguists to check the meaning Text Origin: Council Mandate

Article 13(4)				
G	172b			<p><u>4. Regarding the tasks laid down in points (a), (aa) and (aaa) of paragraph 3, the Executive Director and the Governing Board shall take into account any relevant strategic advice and input provided by ENISA, according to the rules of procedure set by the Governing Board.</u></p> <p>(tb) <u>Regarding the tasks laid down in points (a), (aa) and (aaa) of paragraph 3, the Executive Director and the Governing Board shall take into account any relevant strategic advice and input provided by ENISA, according to the rules of procedure set by the Governing Board.</u></p> <p>Text Origin: Council Mandate</p>
Article 14				
G	173	Article 14 Chairperson and Meetings of the Governing Board	Article 14 Chairperson and Meetings of the Governing Board	<p>Article 14 Chairperson and Meetings of the Governing Board</p> <p>Text Origin: Commission Proposal</p>

Article 14(1)				
Y	174	<p>1. The Governing Board shall elect a Chairperson and a Deputy Chairperson from among the members with voting rights, for a period of two years. The mandate of the Chairperson and the Deputy Chairperson may be extended once, following a decision by the Governing Board. If, however, their membership of the Governing Board ends at any time during their term of office, their term of office shall automatically expire on that date. The Deputy Chairperson shall ex officio replace the Chairperson if the latter is unable to attend to his or her duties. The Chairperson shall take part in the voting.</p>	<p>1. The Governing Board shall elect a Chairperson and a Deputy Chairperson from among the members with voting rights, for a period of two years, <u>aiming to achieve gender balance</u>. The mandate of the Chairperson and the Deputy Chairperson may be extended once, following a decision by the Governing Board. If, however, their membership of the Governing Board ends at any time during their term of office, their term of office shall automatically expire on that date. The Deputy Chairperson shall ex officio replace the Chairperson if the latter is unable to attend to his or her duties. The Chairperson shall take part in the voting.</p>	<p>1. The Governing Board shall elect a Chairperson and a Deputy Chairperson from among the <u>its</u> members with voting rights, for a period of two <u>three</u> years. The mandate of the Chairperson and the Deputy Chairperson may be extended once, following a decision by the Governing Board. If, however, their membership of the Governing Board ends at any time during their term of office, their term of office shall automatically expire on that date. The Deputy Chairperson shall ex officio replace the Chairperson if the latter is unable to attend to his or her duties. The Chairperson shall take part in the voting.</p> <p>Duration to be checked</p> <p>EP to propose separate article on gender balance</p> <p>Text Origin: Council Mandate</p>
Article 14(2)				
G	175	<p>2. The Governing Board shall hold its ordinary meetings at least three times a year. It may hold extraordinary meetings at the request of the Commission, at the request of one third of all its members, at the request of the chair, or at the request of the Executive Director in the fulfilment of his/her tasks.</p>	<p>2. The Governing Board shall hold its ordinary meetings at least three times a year. It may hold extraordinary meetings at the request of the Commission, at the request of one third of all its members, at the request of the chair, or at the request of the Executive Director in the fulfilment of his/her tasks.</p>	<p>2. The Governing Board shall hold its ordinary meetings at least three times a year. It may hold extraordinary meetings at the request of the Commission, at the request of one third of all its members, at the request of the chair <u>Chairperson</u>, or at the request of the Executive Director in the fulfilment of his/her tasks.</p> <p>Text Origin: Council Mandate</p>

Article 14(3)				
G	176	3. The Executive Director shall take part in the deliberations, unless decided otherwise by the Governing Board, but shall have no voting rights. The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers.	3. The Executive Director shall take part in the deliberations, unless decided otherwise by the Governing Board, but shall have no voting rights. The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers.	3. The Executive Director shall take part in the deliberations, unless decided otherwise by the Governing Board, but shall have no voting rights. The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers. Text Origin: EP Mandate
Article 14(3a)				
G	176a		<u>3a. The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers, including additional representatives of the Commission, for ensuring coordination and synergies between different Union activities involving cybersecurity.</u>	<u>3a. The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers.</u> Text Origin: Council Mandate
Article 14(4)				
G	177	4. Members of the Industrial and Scientific Advisory Board may take part, upon invitation from the Chairperson, in the meetings of the Governing Board, without voting rights.	4. Members of the Industrial and Scientific Advisory Board may take part, upon invitation from the Chairperson, in the meetings of the Governing Board, without voting rights.	4. Members <u>Representatives</u> of the Industrial and Scientific Advisory Board <u>Cybersecurity Competence Community</u> may take part, upon invitation from the Chairperson, in the meetings of the Governing Board, without voting rights. Text Origin: Council Mandate

Article 14(5)				
G	178	5. The members of the Governing Board and their alternates may, subject to its rules of procedure, be assisted at the meetings by advisers or experts.	5. The members of the Governing Board and their alternates may, subject to its rules of procedure, be assisted at the meetings by advisers or experts.	5. The members of the Governing Board and their alternates may, subject to its rules of procedure, be assisted at the meetings by advisers or experts. Text Origin: Commission Proposal
Article 14(6)				
Y	179	6. The Competence Centre shall provide the secretariat for the Governing Board.	6. The Competence Centre shall provide the secretariat for the Governing Board.	6. The Competence Centre shall provide the secretariat for the Governing Board. use of 'Competence' Text Origin: Commission Proposal
Article 15				
	180	Article 15 Voting rules of the Governing Board	Article 15 Voting rules of the Governing Board	Article 15 Voting rules of the Governing Board Commission will look into possible compromise on voting rules
Article 15(-1)				
	180a			1. A vote shall be held if the members of the Governing Board failed to achieve consensus.

Article 15(-2)				
180b			<p><u>-2. The Governing Board shall take its decisions by a majority of at least 75% of all its members, the representatives of the Commission constituting a single member for this purpose. An absent member of the Governing Board may delegate his or her vote to his or her alternate or, in the absence of his or her alternate, to another member. Any member of the Governing Board may represent not more than one other member.</u></p>	EP to check
Article 15(-2a)				
180c			<p><u>-2a. Decisions of the Governing Board on the joint actions and their management laid down in points (ca) and (cb) of Article 13(3) shall be taken as follows: (a) decisions to allocate funds from the Union budget to joint actions as referred to in point (ca) of Article 13(3) and the inclusion of such joint action in the annual work programme shall be taken in accordance with the rules set up in paragraph -2 of this Article; (b) decisions relating to the description of the joint actions and laying down conditions for their implementation referred in point (cb) of Article 13(3) shall be taken by participating Members States and the Commission and the voting rights shall be proportional to their relevant contribution to that joint action in accordance with the methodology adopted pursuant to point (s) of Article 13(3).</u></p>	EP to check

Article 15(-1c)				
180d			<u>-3. For decisions which are taken under Article 13(3), except those taken under point (cb), and only insofar as they concern the implementation of Union funds, the Commission shall have a right of veto with the sole aim of ensuring the legality of those decisions, including their compatibility with the Commission's responsibility for implementing the Union's budget. Where the Commission intends to use this right, it shall justify in writing why the legality of the respective draft decision would not be ensured.</u>	Problem for Commission
Article 15(1)				
181	1. The Union shall hold 50 % of the voting rights. The voting rights of the Union shall be indivisible.	deleted	1. The Union shall hold 50 % of the voting rights. The voting rights <u>For decisions other than those referred to in paragraph -2a (b), each Member State and the Union shall have one vote. The vote</u> of the Union shall be indivisible <u>cast jointly by the two representatives of the Commission.</u>	Problem for Commission
Article 15(2)				
G 182	2. Every participating Member State shall hold one vote.	deleted	2. Every participating Member State shall hold one vote <u>The Chairperson shall take part in the voting.</u>	2. Every participating <u>If the Chairperson has been elected from among the representatives of the</u> Member State <u>States,</u> <u>the Chairperson</u> shall hold one vote <u>take part in the voting as a representative of his or her Member State.</u> From EP mandate

Article 15(3)				
183	3. The Governing Board shall take its decisions by a majority of at least 75% of all votes, including the votes of the members who are absent, representing at least 75% of the total financial contributions to the Competence Centre. The financial contribution will be calculated based on the estimated expenditures proposed by the Member States referred to in point c of Article 17(2) and based on the report on the value of the contributions of the participating Member States referred to in Article 22(5).	deleted	deleted	
Article 15(4)				
184	4. Only the representatives of the Commission and the representatives of the participating Member States shall hold voting rights.	deleted	deleted	
Article 15(5)				
G 185	5. The Chairperson shall take part in the voting.	deleted	5. The Chairperson shall take part in the voting.	5. The Chairperson shall take part in the voting. <u>deleted</u>
Article 15a				
185a		<u>Article 15a</u> <u>Voting rules of the Governing Board</u>		to be aligned

Article 15a(1), introductory part				
185b		<u>1. Decisions subject to vote may concern:</u>		
Article 15a(1), point(a)				
185c		<u>(a) governance and organisation of the Competence Centre and the Network;</u>		
Article 15a(1), point(b)				
185d		<u>(b) allocation of budget for the Competence Centre and the Network;</u>		
Article 15a(1), point(c)				
185e		<u>(c) joint actions by several Member States, possibly complemented by Union budget further to decision allocated in accordance with point (b).</u>		
Article 15a(2)				
185f		<u>2. The Governing Board shall adopt its decisions on the basis of at least 75 % of the votes of all members. The voting rights of the Union shall be represented by the Commission and shall be indivisible.</u>		

Article 15a(3)				
185g		<u>3. For decisions under point (a) of paragraph 1, each Member States shall be represented and have the same equal rights of vote. For the remaining votes available up to 100 %, the Union should have at least 50 % of the voting rights corresponding to its financial contribution.</u>		
Article 15a(4)				
185h		<u>4. For decisions falling under point (b) or (c) of paragraph 1, or any other decision not falling under any other category of paragraph 1, the Union shall hold at least 50 % of the voting rights corresponding to its financial contribution. Only contributing Member States shall have voting rights and they will correspond to its financial contribution.</u>		
Article 15a(5)				
185i		<u>5. If the Chairperson has been elected from among the representatives of the Member States, the Chairperson shall take part in the voting as a representative of his or her Member State.</u>		

CHAPTER II, SECTION II				
G	186	SECTION II EXECUTIVE DIRECTOR	SECTION II EXECUTIVE DIRECTOR	SECTION II EXECUTIVE DIRECTOR Text Origin: Commission Proposal
Article 16				
G	187	Article 16 Appointment, dismissal or extension of the term of office of the Executive Director	Article 16 Appointment, dismissal or extension of the term of office of the Executive Director	Article 16 Appointment, dismissal or and extension of the term of office of the Executive Director legal linguistic check Text Origin: Council Mandate
Article 16(1)				
Y	188	1. The Executive Director shall be a person with expertise and high reputation in the areas where the Competence Centre operates.	1. The Executive Director shall be a person with expertise and high reputation in the areas where the Competence Centre operates.	1. The Executive Director shall be a person with expertise and high reputation in the areas where the Competence Centre operates. use of 'Competence' Text Origin: Commission Proposal

Article 16(2)				
Y	189	2. The Executive Director shall be engaged as a temporary agent of the Competence Centre under Article 2(a) of the Conditions of Employment of Other Servants.	2. The Executive Director shall be engaged as a temporary agent of the Competence Centre under Article 2(a) of the Conditions of Employment of Other Servants.	2. The Executive Director shall be engaged as a temporary agent of the Competence Centre under Article 2(a) of the Conditions of Employment of Other Servants. use of 'Competence' Text Origin: Commission Proposal
Article 16(3)				
G	190	3. The Executive Director shall be appointed by the Governing Board from a list of candidates proposed by the Commission, following an open and transparent selection procedure.	3. The Executive Director shall be appointed by the Governing Board from a list of candidates proposed by the Commission, <u>including nominations aiming to achieve gender balance from the Member States</u> , following an open, <u>transparent and non-discriminatory</u> and transparent selection procedure.	3. The Executive Director shall be appointed by the Governing Board from a list of candidates proposed by the Commission, following an open, <u>transparent and non-discriminatory</u> and transparent selection procedure. Text Origin: EP Mandate
Article 16(4)				
Y	191	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.	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.	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. use of 'Competence' Text Origin: Commission Proposal

Article 16(5)				
Y	192	5. The term of office of the Executive Director shall be four years. By the end of that period, the Commission shall carry out an assessment which takes into account the evaluation of the performance of the Executive Director and the Competence Centre's future tasks and challenges.	5. The term of office of the Executive Director shall be four <u>five</u> years. By the end of that period, the Commission shall carry out an assessment which takes into account the evaluation of the performance of the Executive Director and the Competence Centre's future tasks and challenges.	5. The term of office of the Executive Director shall be four years. By the end of that period, the Commission shall carry out an assessment which takes into account the evaluation of the performance of the Executive Director and the Competence Centre's future tasks and challenges. duration still open use of 'Competence' use of 'Competence' Text Origin: Commission Proposal
Article 16(6)				
Y	193	6. The Governing Board may, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 5, extend once the term of office of the Executive Director for no more than four years.	6. The Governing Board may, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 5, extend once the term of office of the Executive Director for no more than four <u>five</u> years.	6. The Governing Board may, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 5, extend once the term of office of the Executive Director for no more than (four) <u>four</u> years. Text Origin: Commission Proposal

Article 16(7)				
G	194	7. An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post.	7. An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post.	7. An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post. Text Origin: Commission Proposal
Article 16(8)				
G	195	8. The Executive Director shall be removed from office only by decision of the Governing Board, acting on a proposal from the Commission.	8. The Executive Director shall be removed from office only by decision of the Governing Board, acting on <u>proposal from its members or on</u> a proposal from the Commission.	8. The Executive Director shall be removed from office only by decision of the Governing Board, acting on a proposal from the Commission <u>or at least 50% of the Member States</u> . Text Origin: Council Mandate
Article 17				
G	196	Article 17 Tasks of the Executive Director	Article 17 Tasks of the Executive Director	Article 17 Tasks of the Executive Director Text Origin: Commission Proposal

Article 17(1)				
Y	197	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.	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.	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. use of 'Competence' Text Origin: Commission Proposal
Article 17(2), introductory part				
G	198	2. The Executive Director shall in particular carry out the following tasks in an independent manner:	2. The Executive Director shall in particular carry out the following tasks in an independent manner:	2. The Executive Director shall in particular carry out the following tasks in an independent manner: Text Origin: Commission Proposal
Article 17(2), point(a)				
G	199	(a) implement the decisions adopted by the Governing Board;	(a) implement the decisions adopted by the Governing Board;	(a) implement the decisions adopted by the Governing Board; Text Origin: Commission Proposal

Article 17(2), point(b)				
G	200	(b) support the Governing Board its work, provide the secretariat for their meetings and supply all information necessary for the performance of their duties;	(b) support the Governing Board its work, provide the secretariat for their meetings and supply all information necessary for the performance of their duties;	(b) support the Governing Board <u>in</u> its work, provide the secretariat for their <u>its</u> meetings and supply all information necessary for the performance of their <u>its</u> duties; Text Origin: Council Mandate
Article 17(2), point(c)				
Y	201	(c) after consultation with the Governing Board and the Commission, prepare and submit for adoption to the Governing Board the draft multiannual strategic plan and the draft annual work plan of the Competence Centre including the scope of the calls for proposals, calls for expressions of interest and calls for tenders needed to implement the work plan and the corresponding expenditure estimates as proposed by the Member States and the Commission;	(c) after consultation with the Governing Board, <u>the Industrial and Scientific Advisory Board, ENISA,</u> and the Commission, prepare and submit for adoption to the Governing Board the draft multiannual strategic plan and the draft annual work plan of the Competence Centre including the scope of the calls for proposals, calls for expressions of interest and calls for tenders needed to implement the work plan and the corresponding expenditure estimates as proposed by the Member States and the Commission;	(c) after consultation with the Governing Board and the Commission, <u>and taking into account the input of the Network and the Cybersecurity Competence Community, and in accordance with the Agenda,</u> prepare and submit for adoption to the Governing Board the draft multiannual strategie plan <u>work programme</u> and the draft annual work plan <u>programme</u> 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 <u>annual work programme</u> work plan and the corresponding expenditure estimates as proposed by the Member States and the Commission; 'agenda' still to be agreed upon use of 'Competence'

Article 17(2), point(d)				
G	202	(d) prepare and submit for adoption to the Governing Board the draft annual budget, including the corresponding staff establishment plan indicating the number of temporary posts in each grade and function group and the number of contract staff and seconded national experts expressed in full-time equivalents;	(d) prepare and submit for adoption to the Governing Board the draft annual budget, including the corresponding staff establishment plan indicating the number of temporary posts in each grade and function group and the number of contract staff and seconded national experts expressed in full-time equivalents;	(d) prepare and submit for adoption to the Governing Board the draft annual budget, including the corresponding <u>establishment plan referred to in point (g) of Article 13(3), staff establishment plan</u> 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; Text Origin: Council Mandate
Article 17(2), point(e)				
G	203	(e) implement the work plan and report to the Governing Board thereon;	(e) implement the work plan and report to the Governing Board thereon;	(e) implement the <u>annual work programme and the multiannual work programme</u> work plan and report to the Governing Board thereon; Text Origin: Council Mandate

Article 17(2), point(f)				
204	(f) prepare the draft annual activity report on the Competence Centre, including the information on corresponding expenditure;	(f) prepare the draft annual activity report on the Competence Centre, including the information on corresponding expenditure;	(f) prepare the draft annual activity report on the Competence Centre, including the information on corresponding expenditure <u>and the realisation of the strategic goals and priorities set out in the Agenda and the multiannual work programme of the Centre; if necessary, that report shall be accompanied by proposals for the further improvement of the realisation and/or the reformulation of the strategic goals and priorities;</u>	(f) <u>prepare the draft annual activity report on the Competence Centre, including the information on corresponding expenditure and the realisation of the Agenda and the multiannual work programme of the Centre; if necessary, that report shall be accompanied by proposals for the further improvement of the realisation and/or the reformulation of the strategic goals and priorities;</u> EP to check Alignment with Art 13 by Commission use of 'Competence' Text Origin: Council Mandate
Article 17(2), point(g)				
Y 205	(g) ensure the implementation of effective monitoring and evaluation procedures relating to the performance of the Competence Centre;	(g) ensure the implementation of effective monitoring and evaluation procedures relating to the performance of the Competence Centre;	(g) ensure the implementation of effective monitoring and evaluation procedures relating to the performance of the Competence Centre;	(g) ensure the implementation of effective monitoring and evaluation procedures relating to the performance of the Competence Centre; use of 'Competence' Text Origin: Commission Proposal

Article 17(2), point(h)				
G	206	(h) prepare an action plan following-up on the conclusions of the retrospective evaluations and reporting on progress every two years to the Commission	(h) prepare an action plan following-up on the conclusions of the retrospective evaluations and reporting on progress every two years to the Commission <u>and the European Parliament;</u>	(h) prepare an action plan following-up <u>that follows up</u> on the conclusions of the retrospective evaluations and reporting reports on progress every two years to the Commission <u>and the European Parliament;</u>
Article 17(2), point(i)				
G	207	(i) prepare, negotiate and conclude the agreements with the National Coordination Centres;	(i) prepare, negotiate and conclude the agreements with the National Coordination Centres;	(i) prepare, negotiate and conclude the agreements with the National Coordination Centres; Text Origin: Council Mandate
Article 17(2), point(j)				
Y	208	(j) be responsible for administrative, financial and staff matters, including the implementation of the Competence Centre budget, taking due account of advice received from the Internal Auditing Function, within the limits of the delegation by the Governing Board;	(j) be responsible for administrative, financial and staff matters, including the implementation of the Competence Centre budget, taking due account of advice received from the Internal Auditing Function, within the limits of the delegation by the Governing Board;	(j) be responsible for administrative, financial and staff matters, including the implementation of the Competence Centre budget, taking due account of advice received from the Internal Auditing Function, within the limits of the delegation by the Governing Board <u>decisions referred to in points (c), (g), (o), (p), (q) and (r) of Article 13(3);</u> use of 'Competence' Text Origin: Council Mandate

Article 17(2), point(k)				
G	209	(k) approve and manage the launch of calls for proposals, in accordance with the work plan and administer the grant agreements and decisions;	(k) approve and manage the launch of calls for proposals, in accordance with the work plan and administer the grant agreements and decisions;	(k) approve and manage the launch of calls for proposals, in accordance with the <u>annual work programme, work plan</u> and administer the grant agreements and decisions; Text Origin: Council Mandate
Article 17(2), point(l)				
G	210	(l) approve the list of actions selected for funding on the basis of the ranking list established by a panel of independent experts;	(l) <u>after consulting the Industrial and Scientific Advisory Board and ENISA,</u> approve the list of actions selected for funding on the basis of the ranking list established by a panel of independent experts;	(l) approve the list of actions selected for funding on the basis of the a ranking list established by a panel of independent experts; Text Origin: Council Mandate
Article 17(2), point(m)				
G	211	(m) approve and manage the launch of calls for tenders, in accordance with the work plan and administer the contracts;	(m) approve and manage the launch of calls for tenders, in accordance with the work plan and administer the contracts;	(m) approve and manage the launch of calls for tenders , in accordance with the <u>annual work programme, work plan</u> and administer the contracts; Text Origin: Council Mandate
Article 17(2), point(n)				
G	212	(n) approve the tenders selected for funding;	(n) approve the tenders selected for funding;	(n) approve the tenders selected for funding; Text Origin: Commission Proposal

Article 17(2), point(o)				
G	213	(o) submit the draft annual accounts and balance sheet to the Internal Auditing Function, and subsequently to the Governing Board,	(o) submit the draft annual accounts and balance sheet to the Internal Auditing Function, and subsequently to the Governing Board,	(o) submit the draft annual accounts and balance sheet to the Internal Auditing Function, and subsequently to the Governing Board, Text Origin: Commission Proposal
Article 17(2), point(p)				
G	214	(p) ensure that risk assessment and risk management are performed;	(p) ensure that risk assessment and risk management are performed;	(p) ensure that risk assessment and risk management are performed; Text Origin: Commission Proposal
Article 17(2), point(q)				
G	215	(q) sign individual grant agreements, decisions and contracts;	(q) sign individual grant agreements, decisions and contracts;	(q) sign individual grant agreements, decisions and contracts; Text Origin: Commission Proposal
Article 17(2), point(r)				
G	216	(r) sign procurement contracts;	(r) sign procurement contracts;	(r) sign procurement contracts; Text Origin: Commission Proposal

Article 17(2), point(s)				
Y	217	(s) prepare an action plan following-up conclusions of internal or external audit reports, as well as investigations by the European Anti-Fraud Office (OLAF) and reporting on progress twice a year to the Commission and regularly to the Governing Board;	(s) prepare an action plan following-up conclusions of internal or external audit reports, as well as investigations by the European Anti-Fraud Office (OLAF) and reporting on progress twice a year to the Commission and <u>the European Parliament and</u> regularly to the Governing Board;	<p>(s) prepare an action plan following-up that <u>follows up on the</u> conclusions of internal or external audit reports, as well as investigations by the European Anti-Fraud Office (OLAF) <u>established with Commission Decision 1999/352/EC, ECSC, Euratom¹ ("OLAF") and</u> report<u>and reporting</u> on progress twice a year to the Commission and regularly to the Governing Board;</p> <p><u>1. [1] 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).</u></p> <p>EP to check its addition</p> <p>Text Origin: Council Mandate</p>
Article 17(2), point(t)				
Y	218	(t) prepare draft financial rules applicable to the Competence Centre;	(t) prepare draft financial rules applicable to the Competence Centre;	<p>(t) prepare draft financial rules applicable to the Competence Centre;</p> <p>use of 'Competence'</p> <p>Text Origin: Commission Proposal</p>

Article 17(2), point(u)				
G	219	(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;	(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;	(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; Text Origin: Commission Proposal
Article 17(2), point(v)				
Y	220	(v) ensure effective communication with the Union's institutions;	(v) ensure effective communication with the Union's institutions <u>and report, upon request, to the European Parliament and to the Council</u> ;	(v) ensure effective communication with the Union's institutions <u>(and report, upon request, to the European Parliament and to the Council)</u> ; Text Origin: EP Mandate
Article 17(2), point(w)				
Y	221	(w) take any other measures needed to assess the progress of the Competence Centre towards its mission and objectives as set out in Articles 3 and 4 of this Regulation;	(w) take any other measures needed to assess the progress of the Competence Centre towards its mission and objectives as set out in Articles 3 and 4 of this Regulation;	(w) take any other measures needed to assess the progress of the Competence Centre towards its mission and objectives as set out in Articles 3 and 4 of this Regulation; use of 'Competence' Text Origin: Commission Proposal

Article 17(2), point(x)					
G	222	(x) perform any other tasks entrusted or delegated to him or her by the Governing Board.	(x) perform any other tasks entrusted or delegated to him or her by the Governing Board.	(x) perform any other tasks entrusted or delegated to him or her by the Governing Board. Text Origin: Commission Proposal	G
CHAPTER II, SECTION III					
	223	SECTION III INDUSTRIAL AND SCIENTIFIC ADVISORY BOARD	SECTION III INDUSTRIAL AND SCIENTIFIC ADVISORY BOARD	<div>deleted</div> <div>Commission to provide input</div> <div>Advisory board</div>	
Article 18					
	224	Article 18 Composition of the Industrial and Scientific Advisory Board	Article 18 Composition of the Industrial and Scientific Advisory Board	<div>deleted</div>	

Article 18(1)				
225	1. The Industrial and Scientific Advisory Board shall consist of no more than 16 members. The members shall be appointed by the Governing Board from among the representatives of the entities of the Cybersecurity Competence Community.	1. The Industrial and Scientific Advisory Board shall consist of no more than 16 <u>25</u> members. The members shall be appointed by the Governing Board from among the representatives of the entities of the <u>Community, or its individual members. Only representatives of entities which are not controlled by a third country or a third-country entity except from EEA and EFTA countries shall be eligible. The appointment shall be made in accordance with an open, transparent and non-discriminatory procedure. The Board composition shall aim to achieve gender balance, and include a balanced representation of the stakeholder groups from industry, academic</u> Cybersecurity Competence community <u>and civil society.</u>	deleted	
Article 18(2)				
226	2. Members of the Industrial and Scientific Advisory Board shall have expertise either with regard to cybersecurity research, industrial development, professional services or the deployment thereof. The requirements for such expertise shall be further specified by the Governing Board.	2. Members of the Industrial and Scientific Advisory Board shall have expertise either with regard to cybersecurity research, industrial development, professional services or the deployment thereof <u>offering, implementing, or deploying professional services or products.</u> The requirements for such expertise shall be further specified by the Governing Board.	deleted	

Article 18(3)				
227	3. Procedures concerning the appointment of its members by the Governing Board and the operation of the Advisory Board, shall be specified in the Competence Centre's rules of procedure and shall be made public.	3. Procedures concerning the appointment of its members by the Governing Board and the operation of the Advisory Board, shall be specified in the Competence Centre's rules of procedure and shall be made public.	deleted	
Article 18(4)				
228	4. The term of office of members of the Industrial and Scientific Advisory Board shall be three years. That term shall be renewable.	4. The term of office of members of the Industrial and Scientific Advisory Board shall be three years. That term shall be renewable.	deleted	
Article 18(5)				
229	5. Representatives of the Commission and of the European Network and Information Security Agency may participate in and support the works of the Industrial and Scientific Advisory Board.	5. Representatives of the Commission and of the European Network and Information Security Agency may <u>ENISA shall be invited to</u> participate in and support the works of the Industrial and Scientific Advisory Board. <u>The Board may invite additional representatives from the Community in an observer, adviser, or expert capacity as appropriate, on a case-by-case basis.</u>	deleted	
Article 19				
230	Article 19 Functioning of the Industrial and Scientific Advisory Board	Article 19 Functioning of the Industrial and Scientific Advisory Board	deleted	

Article 19(1)				
231	1. The Industrial and Scientific Advisory Board shall meet at least twice a year.	1. The Industrial and Scientific Advisory Board shall meet at least <u>three times</u> twice a year.	deleted	
Article 19(2)				
232	2. The Industrial and Scientific Advisory Board may advise the Governing Board on the establishment of working groups on specific issues relevant to the work of the Competence Centre where necessary under the overall coordination of one or more members of the Industrial and Scientific Advisory Board.	2. The Industrial and Scientific Advisory Board <u>shall provide suggestions to</u> may advise the Governing Board on the establishment of working groups on specific issues relevant to the work of the Competence Centre, <u>whenever those issues fall within the tasks and areas of competence outlined in Article 20 and</u> where necessary under the overall coordination of one or more members of the Industrial and Scientific Advisory Board.	deleted	
Article 19(3)				
233	3. The Industrial and Scientific Advisory Board shall elect its chair.	3. The Industrial and Scientific Advisory Board shall elect its chair.	deleted	
Article 19(4)				
234	4. The Industrial and Scientific Advisory Board shall adopt its rules of procedure, including the nomination of the representatives that shall represent the Advisory Board where relevant and the duration of their nomination.	4. The Industrial and Scientific Advisory Board shall adopt its rules of procedure, including the nomination of the representatives that shall represent the Advisory Board where relevant and the duration of their nomination.	deleted	

Article 20				
235	Article 20 Tasks of the Industrial and Scientific Advisory Board	Article 20 Tasks of the Industrial and Scientific Advisory Board	deleted	
Article 20, first paragraph, introductory part				
236	The Industrial and Scientific Advisory Board shall advise the Competence Centre in respect of the performance of its activities and shall:	The Industrial and Scientific Advisory Board shall <u>regularly</u> advise the Competence Centre in respect of the performance of its activities and shall:	deleted	
Article 20(1), point(1)				
237	(1) provide to the Executive Director and the Governing Board strategic advice and input for drafting the work plan and multi-annual strategic plan within the deadlines set by the Governing Board;	(1) provide to the Executive Director and the Governing Board strategic advice and input for <u>deployment by, orientation and operations of the Competence Centre as far as industry and research is concerned,</u> and drafting the work plan and multi-annual strategic plan within the deadlines set by the Governing Board;	deleted	
Article 20, first paragraph, point(1a)				
237a		<u>(1a) advise the Governing Board on the establishment of working groups on specific issues relevant to the work of the Competence Centre;</u>		

Article 20(1), point(2)				
238	(2) organise public consultations open to all public and private stakeholders having an interest in the field of cybersecurity, in order to collect input for the strategic advice referred to in paragraph 1;	(2) organise public consultations open to all public and private stakeholders having an interest in the field of cybersecurity, in order to collect input for the strategic advice referred to in paragraph 1;	deleted	
Article 20(1), point(3)				
239	(3) promote and collect feedback on the work plan and multi-annual strategic plan of the Competence Centre.	(3) promote and collect feedback on the work plan and multi-annual strategic plan of the Competence Centre <u>and advise the Governing Board on how to improve the Competence Centre's strategic orientation and operation.</u>	deleted	
CHAPTER III				
240	CHAPTER III FINANCIAL PROVISIONS	CHAPTER III FINANCIAL PROVISIONS	CHAPTER III FINANCIAL PROVISIONS	CHAPTER III FINANCIAL PROVISIONS Text Origin: Commission Proposal
Article 21				
241	Article 21 Union financial contribution	Article 21 Union financial contribution	Article 21 Union <u>and Member States'</u> financial contribution	Article 21 Union <u>and Member States'</u> financial contribution Text Origin: Council Mandate

Article 21(-1)				
241a			<u>-1. The Centre shall be funded by the Union.</u>	Commission Legal Service has legal objections (partnership rules) Needs to be checked in conjunction with line 244
Article 21(1), introductory part				
242	1. The Union's contribution to the Competence Centre to cover administrative costs and operational costs shall comprise the following:	1. The Union's contribution to the Competence Centre to cover administrative costs and operational costs shall comprise the following:	1. The Union's contribution to the Competence Centre to cover administrative costs and operational costs shall comprise the following:	1. The Union's contribution to the Competence Centre to cover administrative costs and operational costs shall comprise the following: use of 'Competence' Text Origin: Commission Proposal
Article 21(1), point(a)				
243	(a) EUR 1 981 668 000 from the Digital Europe Programme, including up to EUR 23 746 000 for administrative costs;	(a) EUR 1 981 668 000 <u>1 780 954 875 in 2018 prices (EUR 1 998 696 000 in current prices)</u> from the Digital Europe Programme, including up to EUR 23 746 000 <u>21 385 465 in 2018 prices (EUR 23 746 000 in current prices)</u> for administrative costs;	(a) <u>EUR 1 981 668 000</u> from the Digital Europe programme, including up to <u>EUR 23 746 000</u> for administrative costs;	Commission: not all cybersecurity funds from DEP will necessarily go to the Centre, therefore addition of 'up to' Presidency: 'up to' is not acceptable Come back once final MFF figures are available

Article 21(1), point(b)				
244	(b) An amount from the Horizon Europe Programme, including for administrative costs, to be determined taking into account the strategic planning process to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation].	(b) An amount from the Horizon Europe Programme, including for administrative costs, to be determined taking into account the strategic planning process to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation].	(b) an amount from the Horizon Europe programme, including for administrative costs, <u>for joint actions, which shall be equal to the amount contributed by Member States pursuant to paragraph 5 of this Article but not exceed [the amount determined in</u> to be determined taking into account the strategic planning process <u>of the Horizon Europe programme]</u> to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation] <u>and the multiannual work programme and the annual work programme.</u>	all institutions to check
Article 21(1), point(ba)				
244a		<u>(ba) an amount from the European Defence Fund for defence-related actions of the Competence Centre, including for all related administrative costs such as costs that the Competence Centre may incur when acting as a project manager for actions carried out under the European Defence Fund.</u>		Defence/dual use aspect

Article 21(2)				
245	2. The maximum Union contribution shall be paid from the appropriations in the general budget of the Union allocated to [Digital Europe Programme] and to the specific programme implementing Horizon Europe, established by Decision XXX.	2. The maximum Union contribution shall be paid from the appropriations in the general budget of the Union allocated to [Digital Europe Programme] and to the specific programme implementing Horizon Europe, established by Decision XXX, <u>to the European Defence Fund and to other programmes and projects falling within the scope of the Competence Centre or the Network.</u>	2. The maximum Union contribution shall be paid from the appropriations in the general budget of the Union allocated to [Digital Europe Programme] and to the specific programme implementing Horizon Europe, established by Decision XXX.	2. The maximum Union contribution shall be paid from the appropriations in the general budget of the Union allocated to [Digital Europe Programme] and to the specific programme implementing Horizon Europe, established by Decision XXX, <u>(to the European Defence Fund) and to other programmes and projects falling within the scope of the Competence Centre or the Network.</u> Defence/dual use aspect Text Origin: EP Mandate
Article 21(3)				
246	3. The Competence Centre shall implement cybersecurity actions of [Digital Europe Programme] and [Horizon Europe Programme] in accordance with point (c) (iv) of Article 62 of Regulation (EU, Euratom) XXX ¹ [the financial regulation]. 1. [add full title and OJ reference]	3. The Competence Centre shall implement cybersecurity actions of [Digital Europe Programme] and [Horizon Europe Programme] in accordance with point (c) (iv) of Article 62 of Regulation (EU, Euratom) XXX ¹ [the financial regulation]. 1. [add full title and OJ reference]	3. The Competence Centre shall implement cybersecurity actions of [Digital Europe Programme] and [Horizon Europe Programme] in accordance with point (c) (iv) of <u>the first subparagraph of Article 62(1)</u> of Regulation (EU, Euratom) XXX² [the financial regulation] <u>2018/1046.</u> 1. [add full title and OJ reference]	3. The Competence Centre shall implement cybersecurity actions of [Digital Europe Programme] and [Horizon Europe Programme] in accordance with point (c) (iv) of <u>the first subparagraph of Article 62(1)</u> of Regulation (EU, Euratom) XXX² [the financial regulation] <u>2018/1046.</u> 1. [add full title and OJ reference] use of 'Competence' Text Origin: Council Mandate

Article 21(4)				
247	4. The Union financial contribution shall not cover the tasks referred to in Article 4(8)(b)	4. The Union financial contribution <u>from Digital Europe Programme and from Horizon Europe Programme</u> shall not cover the tasks referred to in Article 4(8)(b). <u>These may be covered by financial contributions from the European Defence Fund.</u>	4. The <u>Contributions from Union programmes other than those referred to in paragraphs 1 and 2 that are part of a</u> Union financial contribution <u>co-financing to a programme implemented by one of the Member States</u> shall not cover the <u>tasks</u> <u>be accounted for in the calculation of the Union maximum financial contribution</u> referred to in Article 4(8)(b) <u>paragraphs 1 and 2).</u>	4. The <u>Contributions from Union programmes other than those referred to in paragraphs 1 and 2 that are part of a</u> Union financial contribution <u>co-financing to a programme implemented by one of the Member States</u> shall not cover the <u>tasks</u> <u>be accounted for in the calculation of the Union maximum financial contribution</u> referred to in Article 4(8)(b) <u>paragraphs 1 and 2).</u> Commission to check Defence/dual use aspect Text Origin: Council Mandate
Article 21(5)				
247a			<u>5. Voluntary contributions made by one or more Member States for joint actions with the Union in accordance with the Horizon Europe programme and/or the Digital Europe programme, may take the form of financial and/or in-kind contributions.</u> <u>Financial contributions by Member States may take the form of support by Member States provided to participants in joint actions.</u> <u>In-kind contributions by Member States shall consist of eligible costs incurred by National Coordination Centres and other public entities when participating in projects funded through this Regulation less any Union contribution to those costs.</u>	EP, Commission to check

			<p><u>In the case of projects funded through Horizon Europe, eligible costs shall be calculated in line with Article 32 of the Regulation establishing Horizon Europe. In the case of projects funded through Digital Europe, eligible costs shall be calculated in line with Regulation (EU, Euratom) 2018/1046.</u></p> <p><u>The envisaged amount of total Member State voluntary contributions, including financial contributions for administrative costs, to joint actions under the Horizon Europe programme shall be determined in order to be taken into account in the strategic planning process of the Horizon Europe programme to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation], with input from the Governing Board.</u></p> <p><u>For actions under the Digital Europe programme, notwithstanding Article 15 of the [Regulation establishing the Digital Europe Programme], the Member States may make a contribution to the costs of the Centre that are co-financed from the Digital Europe programme that is lower than the amounts specified in [Article 21(1)(a) – reference to be checked] of this Regulation.</u></p>	
Article 22				
248	Article 22 Contributions of participating Member States	Article 22 Contributions of participating Member States	Article 22 Contributions of participating Member States	No need for separate article as merged with art 21

Article 22(1)				
249	1. The participating Member States shall make a total contribution to the operational and administrative costs of the Competence Centre of at least the same amounts as those in Article 21(1) of this Regulation.	1. The participating Member States shall make a total contribution to the operational and administrative costs of the Competence Centre of at least the same amounts as those in Article 21(1) of this Regulation.		Political point
Article 22(7)				
249a			<u>7. Member States' co-funding of actions supported by Union programmes other than Horizon Europe and Digital Europe shall be considered as contributions when those actions are in the remit of the Centre's mission and tasks.</u>	Commission to check
Article 22(2)				
250	2. For the purpose of assessing the contributions referred to in paragraph 1 and in point (b)ii of Article 23(3), the costs shall be determined in accordance with the usual cost accounting practices of the Member States concerned, the applicable accounting standards of the Member State, and the applicable International Accounting Standards and International Financial Reporting Standards. The costs shall be certified by an independent external auditor appointed by the Member State concerned. The valuation method may be verified by the Competence Centre should there be any uncertainty arising from the certification.	2. For the purpose of assessing the contributions referred to in paragraph 1 and in point (b)ii of Article 23(3), the costs shall be determined in accordance with the usual cost accounting practices of the Member States concerned, the applicable accounting standards of the Member State, and the applicable International Accounting Standards and International Financial Reporting Standards. The costs shall be certified by an independent external auditor appointed by the Member State concerned. The valuation method may be verified by the Competence Centre should there be any uncertainty arising from the certification.	28. For the purpose of assessing the contributions referred to in paragraph 1 <u>of this Article</u> and in point (b)ii of Article-23(3), the costs shall be determined in accordance with the usual cost accounting practices of the Member States concerned, the applicable accounting standards of the <u>that</u> Member State, and the applicable international accounting standards and international financial reporting standards. The costs shall be certified by an independent external auditor appointed by the Member State concerned. The valuation method may be verified by the the-Competence- Centre should there be any uncertainty arising from the certification.	28. For the purpose of assessing the contributions referred to in paragraph 1 <u>of this Article</u> and in point (b)ii of Article-23(3), the costs shall be determined in accordance with the usual cost accounting practices of the Member States concerned, the applicable accounting standards of the <u>that</u> Member State, and the applicable international accounting standards and international financial reporting standards. The costs shall be certified by an independent external auditor appointed by the Member State concerned. The valuation method may be verified by the the-Competence- Centre should there be any uncertainty arising from the certification.

				<p>lawyer linguists to check best wording</p> <p>use of 'Competence'</p> <p>Text Origin: Council Mandate</p>
Article 22(3)				
251	<p>3. Should any participating Member State be in default of its commitments concerning its financial contribution, the Executive Director shall put this in writing and shall set a reasonable period within which such default shall be remedied. If the situation is not remedied within that period, the Executive Director shall convene a meeting of the Governing Board to decide whether the defaulting participating Member State's right to vote is to be revoked or whether any other measures are to be taken until its obligations have been met. The defaulting Member State's voting rights shall be suspended until the default of its commitments is remedied.</p>	<p>3. Should any participating Member State be in default of its commitments concerning its financial contribution, the Executive Director shall put this in writing and shall set a reasonable period within which such default shall be remedied. If the situation is not remedied within that period, the Executive Director shall convene a meeting of the Governing Board to decide whether the defaulting participating Member State's right to vote is to be revoked or whether any other measures are to be taken until its obligations have been met. The defaulting Member State's voting rights shall be suspended until the default of its commitments is remedied.</p>	<p>39. Should any participating-Member State be in default of its commitments concerning its financial <u>and/or in-kind</u> contribution <u>pursuant to joint actions</u>, the Executive Director shall put this in writing and shall set a reasonable period within which such default shall be remedied. If the situation is not remedied within that period, the Executive Director shall convene a meeting of the Governing Board to decide whether the defaulting participating Member State's right to vote is to be revoked or whether any other measures are to be taken until its obligations have been met<u>that Member State meets its obligations</u>. The defaulting Member State's voting rights <u>concerning joint actions</u> shall be suspended until the default of its commitments is remedied.</p>	<p>39. Should any participating-Member State be in default of its commitments concerning its financial <u>and/or in-kind</u> contribution <u>pursuant to joint actions</u>, the Executive Director shall put this in writing and shall set a reasonable period within which such default shall be remedied. If the situation is not remedied within that period, the Executive Director shall convene a meeting of the Governing Board to decide whether the defaulting participating Member State's right to vote is to be revoked or whether any other measures are to be taken until its obligations have been met<u>that Member State meets its obligations</u>. The defaulting Member State's voting rights <u>concerning joint actions</u> shall be suspended until the default of its commitments is remedied.</p> <p>EP to check</p> <p>Text Origin: Council Mandate</p>

Article 22(4)				
252	4. The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to the Competence Centre if the participating Member States do not contribute, contribute only partially or contribute late with regard to the contributions referred to in paragraph 1.	4. The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to the Competence Centre if the participating Member States do not contribute, contribute only partially or contribute late <u>only partially</u> with regard to the contributions referred to in paragraph 1. <u>The Commission's termination, reduction or suspension of the Union's financial contribution shall be proportionate in amount and time to the reduction, termination or suspension of the Member States' contributions.</u>	410. The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to the Competence Centre <u>joint actions</u> if the participating <u>contributing</u> Member States do not contribute, contribute only partially or contribute late with regard to the contributions referred to in <u>point (b) of</u> paragraph 1.	410. The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to the Competence Centre <u>joint actions</u> if the participating <u>contributing</u> Member States do not contribute, contribute only partially or contribute late with regard to the contributions referred to in <u>point (b) of</u> paragraph 1. <u>The Commission's termination, reduction or suspension of the Union's financial contribution shall be proportionate in amount and time to the reduction, termination or suspension of the Member States' contributions.</u> EP and Commission to check
Article 22(5)				
253	5. The participating Member States shall report by 31 January each year to the Governing Board on the value of the contributions referred to in paragraphs 1 made in each of the previous financial year.	5. The participating Member States shall report by 31 January each year to the Governing Board on the value of the contributions referred to in paragraphs 1 made in each of the previous financial year.	§11. The participating <u>contributing</u> Member States shall report by 31 <u>31</u> January <u>of</u> each year to the Governing Board on the value of the contributions referred to in paragraphs 1 <u>paragraph 5 for joint action with the Union</u> made in each of the previous financial year.	§11. The participating <u>contributing</u> Member States shall report by 31 <u>31</u> January <u>of</u> each year to the Governing Board on the value of the contributions referred to in paragraphs 1 <u>paragraph 5 for joint action with the Union</u> made in each of the previous financial year. EP to check Text Origin: Council Mandate

Article 23				
254	Article 23 Costs and resources of the Competence Centre	Article 23 Costs and resources of the Competence Centre	Article 23 Costs and resources of the Competence Centre	Article 23 Costs and resources of the Competence Centre use of 'Competence' Text Origin: Commission Proposal
Article 23(1)				
255	1. The Competence Centre shall be jointly funded by the Union and Member States through financial contributions paid in instalments and contributions consisting of costs incurred by National Coordination Centres and beneficiaries in implementing actions that are not reimbursed by the Competence Centre.	1. The Competence Centre shall be jointly funded by the Union and Member States through financial contributions paid in instalments and contributions consisting of costs incurred by National Coordination Centres and beneficiaries in implementing actions that are not reimbursed by the Competence Centre.	deleted	broader discussion needed
Article 23(2)				
256	2. The administrative costs of the Competence Centre shall not exceed EUR [number] and shall be covered by means of financial contributions divided equally on an annual basis between the Union and the participating Member States. If part of the contribution for administrative costs is not used, it may be made available to cover the operational costs of the Competence Centre.	2. The administrative costs of the Competence Centre shall not exceed EUR [number] and shall be covered by means of financial contributions divided equally on an annual basis between the Union and the participating Member States. If part of the contribution for administrative costs is not used, it may be made available to cover the operational costs of the Competence Centre.	2. The administrative costs of the Competence Centre shall not exceed EUR [number] and shall be covered by means of financial contributions divided equally on an annual basis between <u>from</u> the Union. <u>Additional contributions shall be made by contributing and the participating</u> Member States <u>in proportion to their voluntary contributions to joint actions</u> . 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.	broader discussion needed

Article 23(3), introductory part				
Y	257	3. The operational costs of the Competence Centre shall be covered by means of:	3. The operational costs of the Competence Centre shall be covered by means of:	3. The operational costs of the Competence Centre shall be covered by means of: use of 'Competence' Text Origin: Commission Proposal
Article 23(3), point(a)				
G	258	(a) the Union's financial contribution;	(a) the Union's financial contribution;	(a) the Union's financial contribution; Text Origin: Commission Proposal
Article 23(3), point(b), introductory part				
	259	(b) contributions from the participating Member States in the form of:	(b) contributions from the participating Member States in the form of:	(b) <u>voluntary financial and/or in-kind</u> contributions from the <u>participatingcontributing</u> Member States in the form of: <u>case of joint actions</u> Lines 259-262 depend on COM and EP examination
Article 23(3), point(b)(i)				
	260	(i) Financial contributions; and	(i) Financial contributions; and	<div>deleted</div>
Article 23(3), point(b)(ii)				
	261	(ii) where relevant, in-kind contributions by the participating Member States of the costs incurred by National Coordination Centres and beneficiaries in implementing indirect actions less the contribution of the Competence Centre and any other Union contribution to those costs;	(ii) where relevant, in-kind contributions by the participating Member States of the costs incurred by National Coordination Centres and beneficiaries in implementing indirect actions less the contribution of the Competence Centre and any other Union contribution to those costs;	<div>deleted</div>

Article 23(4), introductory part				
262	4. The resources of the Competence Centre entered into its budget shall be composed of the following contributions:	4. The resources of the Competence Centre entered into its budget shall be composed of the following contributions:	4. The resources of the Competence Centre entered into its budget shall be composed of the following contributions:	
Article 23(4), point(a)				
263	(a) participating Member States' financial contributions to the administrative costs;	(a) <u>the Union's and</u> participating Member States' financial contributions to the administrative costs;	(a) participating Member States' <u>the Union's</u> financial contributions to the <u>operational and</u> administrative costs;	
Article 23(4), point(b)				
264	(b) participating Member States' financial contributions to the operational costs;	(b) <u>the Union's and</u> participating Member States' financial contributions to the operational costs;	(b) participating contributing Member States' <u>voluntary</u> financial contributions to the operational <u>administrative</u> costs <u>in case of joint actions</u> ;	
Article 23(4), point(c)				
265	(c) any revenue generated by Competence Centre;	(c) any revenue generated by Competence Centre;	(c) any revenue generated by Competence Centre <u>contributing Member States' voluntary financial contributions to the operational costs in case of joint actions</u> ;	
Article 23(4), point(d)				
266	(d) any other financial contributions, resources and revenues.	(d) any other financial contributions, resources and revenues.	(d) any other financial contributions, resources and revenues. <u>revenue generated by Centre;</u>	<div>(d) any other financial contributions, resources and revenues.<u>revenue generated by Centre;</u></div> <div>need to clarify that participation in community is free</div> <div>Text Origin: Council Mandate</div>

Article 23(4), point(e)				
G	266a		<u>(e) any other financial contributions, resources and revenues.</u>	<u>(da) any other financial contributions, resources and revenues.</u> Text Origin: Council Mandate
Article 23(5)				
Y	267	5. Any interest yielded by the contributions paid to the Competence Centre by the participating Member States shall be considered to be its revenue.	5. Any interest yielded by the contributions paid to the Competence Centre by the participating Member States shall be considered to be its revenue.	5. Any interest yielded by the contributions paid to the Competence Centre by the participating <u>contributing</u> Member States shall be considered to be its revenue. use of 'Competence' Text Origin: Council Mandate
Article 23(6)				
Y	268	6. All resources of the Competence Centre and its activities shall be aimed to achieve to the objectives set out in Article 4.	6. All resources of the Competence Centre and its activities shall be aimed to achieve to the objectives set out in Article 4.	6. All resources of the Competence Centre and its activities shall be aimed to achieve to the objectives set out in Article 4. use of 'Competence' Text Origin: Council Mandate

Article 23(7)				
269	7. The Competence Centre shall own all assets generated by it or transferred to it for the fulfilment of its objectives.	7. The Competence Centre shall own all assets generated by it or transferred to it for the fulfilment of its objectives.	7. The Competence Centre shall own all assets generated by it or transferred to it for the fulfilment of its objectives. <u>Without prejudice to the applicable rules of the relevant funding programme, ownership of assets generated or acquired in joint actions shall be decided in accordance with Article 15 (-2a).</u>	EP and Commission to check
Article 23(8)				
Y 270	8. Except when the Competence Centre is wound up, any excess revenue over expenditure shall not be paid to the participating members of the Competence Centre.	8. Except when the Competence Centre is wound up, any excess revenue over expenditure shall not be paid to the participating members of the Competence Centre.	8. Except when the Competence Centre is wound up, any excess revenue over expenditure shall <u>remain in the ownership of the Centre and</u> not be paid to the participating <u>contributing</u> members of the Competence Centre.	8. Except when the Competence Centre is wound up, any excess revenue over expenditure shall <u>remain in the ownership of the Centre and</u> not be paid to the participating <u>contributing</u> members of the Competence Centre. use of 'Competence' Text Origin: Council Mandate
Article 23(8a)				
G 270a		<u>8a. The Competence Centre shall cooperate closely with other Union institutions, agencies, and bodies in order to benefit from synergies and, where appropriate, to reduce administrative costs.</u>		<u>8a. The Competence Centre shall cooperate closely with other Union institutions, agencies and bodies, having due regard to their respective mandates and without duplicating existing cooperation mechanisms, in order to benefit from synergies and, where possible and appropriate, to reduce administrative costs.</u>

Article 24				
G	271	Article 24 Financial commitments	Article 24 Financial commitments	Article 24 Financial commitments Text Origin: Commission Proposal
Article 24, first paragraph				
Y	272	The financial commitments of the Competence Centre shall not exceed the amount of financial resources available or committed to its budget by its members.	The financial commitments of the Competence Centre shall not exceed the amount of financial resources available or committed to its budget by its members.	The financial commitments of the Competence Centre shall not exceed the amount of financial resources available or committed to its budget by its members. use of 'Competence' Text Origin: Commission Proposal
Article 25				
G	273	Article 25 Financial year	Article 25 Financial year	Article 25 Financial year Text Origin: Commission Proposal
Article 25, first paragraph				
G	274	The financial year shall run from 1 January to 31 December.	The financial year shall run from 1 January to 31 December.	The financial year shall run from 1 January to 31 December. Text Origin: Commission Proposal

Article 26				
G	275	Article 26 Establishment of the budget	Article 26 Establishment of the budget	Article 26 Establishment of the budget Text Origin: Commission Proposal
	Article 26(1)			
	276	1. Each year, the Executive Director shall draw up a draft statement of estimates of the Competence Centre's revenue and expenditure for the following financial year, and shall forward it to the Governing Board, together with a draft establishment plan. Revenue and expenditure shall be in balance. The expenditure of the Competence Centre shall include the staff, administrative, infrastructure and operational expenses. Administrative expenses shall be kept to a minimum.	1. Each year, the Executive Director shall draw up a draft statement of estimates of the Competence Centre's revenue and expenditure for the following financial year, and shall forward it to the Governing Board, together with a draft establishment plan. Revenue and expenditure shall be in balance. The expenditure of the Competence Centre shall include the staff, administrative, infrastructure and operational expenses. Administrative expenses shall be kept to a minimum.	1. Each year, the Executive Director shall draw up a draft statement of estimates of the Competence Centre's revenue and expenditure for the following financial year, and shall forward it to the Governing Board, together with a draft establishment plan <u>as referred to in point (g) of Article 13(3)</u> . 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, <u>also through redeployment of staff or posts</u> . EP reservation on redeployment. Also to be seen in connection with line 308. use of 'Competence' Text Origin: Council Mandate

Article 26(2)				
Y	277	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.	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.	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. use of 'Competence' Text Origin: Commission Proposal
Article 26(3)				
G	278	3. The Governing Board shall, by 31 January each year, send the statement of estimates referred to in paragraph 2, which shall be part of the draft single programming document, to the Commission.	3. The Governing Board shall, by 31 January each year, send the statement of estimates referred to in paragraph 2, which shall be part of the draft single programming document, to the Commission.	3. The Governing Board shall, by 31 January <u>31 January of</u> each year, send the statement of estimates referred to in paragraph 2, which shall be part of the draft single programming document <u>referred to in Article 32(1) of Commission Delegated Regulation (EU) 2019/715¹</u> , to the Commission. <u>1. [1] Commission Delegated Regulation (EU) 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (OJ L 122, 15.5.2019, p. 1).</u> Text Origin: Council Mandate

Article 26(4)				
G	279	4. On the basis of that statement of estimates, the Commission shall enter in the draft budget of the Union the estimates it deems necessary for the establishment plan and the amount of the contribution to be charged to the general budget, which it shall submit to the European Parliament and the Council in accordance with Article 313 and 314 TFEU.	4. On the basis of that statement of estimates, the Commission shall enter in the draft budget of the Union the estimates it deems necessary for the establishment plan and the amount of the contribution to be charged to the general budget, which it shall submit to the European Parliament and the Council in accordance with Article 313 and 314 TFEU.	4. On the basis of that <u>the</u> statement of estimates <u>referred to in paragraph 2 of this Article</u> , the Commission shall enter in the draft budget of the Union the estimates it deems necessary for the establishment plan <u>referred to in point (g) of Article 13(3)</u> and the amount of the contribution to be charged to the general budget, which it shall submit to the European Parliament and the Council in accordance with Article <u>Articles</u> 313 and 314 TFEU. Text Origin: Council Mandate
Article 26(5)				
Y	280	5. The European Parliament and the Council shall authorise the appropriations for the contribution to the Competence Centre.	5. The European Parliament and the Council shall authorise the appropriations for the contribution to the Competence Centre.	5. The European Parliament and the Council shall authorise the appropriations for the contribution to the Competence Centre. use of 'Competence' Text Origin: Commission Proposal
Article 26(6)				
G	281	6. The European Parliament and the Council shall adopt the establishment plan for the Competence Centre.	6. The European Parliament and the Council shall adopt the establishment plan for the Competence Centre.	6. The European Parliament and the Council shall adopt the establishment plan for the Competence Centre <u>referred to in point (g) of Article 13(3)</u> . Text Origin: Council Mandate

Article 26(7)				
Y	282	7. Together with the Work Plan, the Governing Board shall adopt the Centre's budget. It shall become final following definitive adoption of the general budget of the Union. Where appropriate, the Governing Board shall adjust the Competence Centre's budget and Work Plan in accordance with the general budget of the Union.	7. Together with the Work Plan, the Governing Board shall adopt the Centre's budget. It shall become final following definitive adoption of the general budget of the Union. Where appropriate, the Governing Board shall adjust the Competence Centre's budget and Work Plan in accordance with the general budget of the Union.	7. Together with the <u>annual work programme and multi annual work programme</u> Work Plan , the Governing Board shall adopt the Centre's budget. It shall become final following <u>the</u> definitive adoption of the general budget of the Union. Where appropriate, the Governing Board shall adjust the Competence Centre's budget and <u>the annual work programme</u> Work Plan in accordance with the general budget of the Union. use of 'Competence' Text Origin: Council Mandate
Article 27				
Y	283	Article 27 Presentation of the Competence Centre's accounts and discharge	Article 27 Presentation of the Competence Centre's accounts and discharge	Article 27 Presentation of the Competence Centre's accounts and discharge use of 'Competence' Text Origin: Commission Proposal

Article 27, first paragraph				
Y	284	The presentation of the Competence Centre's provisional and final accounts and the discharge shall follow the rules and timetable of the Financial Regulation and of its financial rules adopted in accordance with Article 29.	The presentation of the Competence Centre's provisional and final accounts and the discharge shall follow the rules and timetable of the Financial Regulation and of its financial rules adopted in accordance with Article 29.	<div>The presentation of the Competence Centre's provisional and final accounts and the discharge shall follow the rules and timetable of <u>Regulation (EU, Euratom) 2018/1046 the Financial Regulation</u> and of its the financial rules adopted in accordance with Article 29 of the Centre.</div> <div>use of 'Competence'</div> <div>Text Origin: Council Mandate</div>
Article 28				
G	285	Article 28 Operational and financial reporting	Article 28 Operational and financial reporting	<div>Article 28 Operational and financial reporting</div> <div>Text Origin: Commission Proposal</div>
Article 28(1)				
Y	286	1. The Executive Director shall report annually to the Governing Board on the performance of his/her duties in accordance with the financial rules of the Competence Centre.	1. The Executive Director shall report annually to the Governing Board on the performance of his/her duties in accordance with the financial rules of the Competence Centre.	<div>1. The Executive Director shall report annually to the Governing Board on the performance of his/her duties in accordance with the financial rules of the Competence Centre.</div> <div>use of 'Competence'</div> <div>Text Origin: Commission Proposal</div>

Article 28(2), introductory part				
Y	287	2. Within two months of the closure of each financial year, the Executive Director shall submit to the Governing Board for approval an annual activity report on the progress made by the Competence Centre in the previous calendar year, in particular in relation to the work plan for that year. That report shall include, inter alia, information on the following matters:	2. Within two months of the closure of each financial year, the Executive Director shall submit to the Governing Board for approval an annual activity report on the progress made by the Competence Centre in the previous calendar year, in particular in relation to the work plan for that year. That report shall include, inter alia, information on the following matters:	2. Within two months of the closure of each financial year, the Executive Director shall submit to the Governing Board for approval an annual activity report on the progress made by the Competence Centre in the previous calendar year, in particular in relation to the <u>annual work programme</u> work plan for that year <u>and the fulfilment of its strategic goals and priorities</u> . That report shall include, inter alia, information on the following matters: use of 'Competence' Text Origin: Council Mandate
Article 28(2), point(a)				
G	288	(a) operational actions carried out and the corresponding expenditure;	(a) operational actions carried out and the corresponding expenditure;	(a) operational actions carried out and the corresponding expenditure; Text Origin: Commission Proposal
Article 28(2), point(b)				
G	289	(b) the actions submitted, including a breakdown by participant type, including SMEs, and by Member State;	(b) the actions submitted, including a breakdown by participant type, including SMEs, and by Member State;	(b) the actions submitted, including a breakdown by participant type, including SMEs, and by Member State; Text Origin: Commission Proposal

Article 28(2), point(c)				
G	290	(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;	(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;	(c) the actions selected for funding, including a breakdown by participant type, including SMEs <u>and technology related SMEs</u> , and by Member State and indicating the contribution of the Competence Centre to the individual participants and actions; Text Origin: Commission Proposal
Article 28(2), point(d)				
G	291	(d) progress towards the achievement of the objectives set out in Article 4 and proposals for further necessary work to achieve these objectives.	(d) progress towards the achievement of the objectives set out in Article 4 and proposals for further necessary work to achieve these objectives.	(d) progress towards the achievement of the <u>mission set out in Article 3 and the</u> objectives set out in Article 4 and proposals for further necessary work to achieve these <u>that mission and those</u> objectives- i ; Text Origin: Council Mandate
Article 28(2), point(e)				
Y	291a			<u>(e) coherence of the implementation tasks in accordance with the Agenda and the multiannual work programme.</u> <u>(da) coherence of the implementation tasks in accordance with the Agenda and the multiannual work programme.</u> Text Origin: Council Mandate

Article 28(3)					
G	292	3. Once approved by the Governing Board, the annual activity report shall be made publicly available.	3. Once approved by the Governing Board, the annual activity report shall be made publicly available.	3. Once approved by the Governing Board, the annual activity report shall be made publicly available.	3. Once approved by the Governing Board, the annual activity report shall be made publicly available. Text Origin: Commission Proposal
Article 29					
G	293	Article 29 Financial rules	Article 29 Financial rules	Article 29 Financial rules	Article 29 Financial rules Text Origin: Commission Proposal
Article 29, first paragraph					
Y	294	The Competence Centre shall adopt its specific financial rules in accordance with Article 70 of Regulation XXX [new Financial Regulation].	The Competence Centre shall adopt its specific financial rules in accordance with Article 70 of Regulation XXX [new Financial Regulation].	The Competence Centre shall adopt its specific financial rules in accordance with Article 70 of Regulation XXX [new Financial Regulation] (EU, Euratom) 2018/1046 .	The Competence Centre shall adopt its specific financial rules in accordance with Article 70 of Regulation XXX [new Financial Regulation] (EU, Euratom) 2018/1046 . use of 'Competence' Text Origin: Council Mandate
Article 30					
G	295	Article 30 Protection of financial interests	Article 30 Protection of financial interests	Article 30 Protection of financial interests	Article 30 Protection of financial interests Text Origin: Commission Proposal

Article 30(1)					
Y	296	<p>1. The Competence Centre shall take appropriate measures to ensure that, when actions financed under this Regulation are implemented, the financial interests of the Union are protected by the application of preventive measures against fraud, corruption and any other illegal activities, by effective checks and, if irregularities are detected, by the recovery of the amounts wrongly paid and, where appropriate, by effective, proportionate and dissuasive administrative sanctions.</p>	<p>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 <u>regular and</u> effective checks and, if irregularities are detected, by the recovery of the amounts wrongly paid and, where appropriate, by effective, proportionate and dissuasive administrative sanctions.</p>	<p>1. The Competence Centre shall take appropriate measures to ensure that, when actions financed under this Regulation are implemented, the financial interests of the Union are protected by the application of preventive measures against fraud, corruption and any other illegal activities, by effective checks and, if irregularities are detected, by the recovery of the amounts wrongly paid and, where appropriate, by effective, proportionate and dissuasive administrative sanctions.</p> <p>use of 'Competence'</p> <p>Text Origin: EP Mandate</p>	Y
Article 30(2)					
Y	297	<p>2. The Competence Centre shall grant Commission staff and other persons authorised by the Commission, as well as the Court of Auditors, access to its sites and premises and to all the information, including information in electronic format that is needed in order to conduct their audits.</p>	<p>2. The Competence Centre shall grant Commission staff and other persons authorised by the Commission, as well as the Court of Auditors, access to its sites and premises and to all the information, including information in electronic format that is needed in order to conduct their audits.</p>	<p>2. The Competence Centre shall grant Commission staff and other persons authorised by the Commission, as well as the Court of Auditors, access to its sites and premises and to all the information, including information in electronic format that is needed in order to conduct their audits.</p> <p>use of 'Competence'</p> <p>Text Origin: Commission Proposal</p>	Y

G 298	<p>3. The European Anti-Fraud Office (OLAF) may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Council Regulation (Euratom, EC) No 2185/96¹ and Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council² 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.</p> <p>1. 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). 2. 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).</p>	<p>3. The European Anti-Fraud Office (OLAF) may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Council Regulation (Euratom, EC) No 2185/96¹ and Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council² 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.</p> <p>1. 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). 2. 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).</p>	<p>3. The European Anti-Fraud Office (OLAF) OLAF may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Council Regulation (Euratom, EC) No 2185/96¹ and Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council²—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.</p> <p>1. 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). 2. 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).</p>	<p>3. The European Anti-Fraud Office (OLAF) OLAF may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Council Regulation (Euratom, EC) No 2185/96¹ and Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council²—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.</p> <p>1. 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). 2. 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).</p> <p>Text Origin: Council Mandate</p>
----------	--	--	---	---

Article 30(4)						
Y	299	<p>4. Without prejudice to paragraphs 1, 2 and 3 of this Article, contracts and grant agreements resulting from the implementation of this Regulation shall contain provisions expressly empowering the Commission, the Competence Centre, the Court of Auditors and OLAF to conduct such audits and investigations in accordance with their respective competences. Where the implementation of an action is outsourced or sub-delegated, in whole or in part, or where it requires the award of a procurement contract or financial support to a third party, the contract, or grant agreement shall include the contractor's or beneficiary's obligation to impose on any third party involved explicit acceptance of those powers of the Commission, the Competence Centre, the Court of Auditors and OLAF.</p>	<p>4. Without prejudice to paragraphs 1, 2 and 3 of this Article, contracts and grant agreements resulting from the implementation of this Regulation shall contain provisions expressly empowering the Commission, the Competence Centre, the Court of Auditors and OLAF to conduct such audits and investigations in accordance with their respective competences. Where the implementation of an action is outsourced or sub-delegated, in whole or in part, or where it requires the award of a procurement contract or financial support to a third party, the contract, or grant agreement shall include the contractor's or beneficiary's obligation to impose on any third party involved explicit acceptance of those powers of the Commission, the Competence Centre, the Court of Auditors and OLAF.</p>	<p>4. Without prejudice to paragraphs 1, 2 and 3 of this Article, contracts and grant agreements resulting from the implementation of this Regulation shall contain provisions expressly empowering the Commission, the Competence Centre, the Court of Auditors and OLAF to conduct such audits and investigations in accordance with their respective competences. Where the implementation of an action is outsourced or sub-delegated, in whole or in part, or where it requires the award of a procurement contract or financial support to a third party, the contract, or contractor 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.</p> <p>use of 'Competence'</p> <p>Text Origin: Commission Proposal</p>	Y	
CHAPTER IV						
	300	CHAPTER IV COMPETENCE CENTRE STAFF	CHAPTER IV COMPETENCE CENTRE STAFF	CHAPTER IV COMPETENCE CENTRE STAFF	use of 'Competence'	
Article 31						
G	301	Article 31 Staff	Article 31 Staff	Article 31 Staff	Text Origin: Commission Proposal	G

Article 31(1)					
		<p>1. The Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union as laid down by Council Regulation (EEC, Euratom, ECSC) No 259/68¹ ('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.</p>	<p>1. The Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union as laid down by Council Regulation (EEC, Euratom, ECSC) No 259/68¹ ('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.</p>	<p>1. The Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union as laid down by Council Regulation (EEC, Euratom, ECSC) No 259/68¹ ('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.</p>	
Y	302	<p>1. Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1).</p>	<p>1. Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1).</p>	<p>1. Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1).</p> <p>use of 'Competence'</p> <p>Text Origin: Commission Proposal</p>	Y

Article 31(2)				
Y	303	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').	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').	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'). use of 'Competence' Text Origin: Commission Proposal
Article 31(3)				
G	304	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.	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.	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. Text Origin: Commission Proposal

Article 31(4)				
G	305	4. Where exceptional circumstances so require, the Governing Board may by decision temporarily suspend the delegation of the appointing authority powers to the Executive Director and any sub-delegation made by the latter. In such a case the Governing Board shall exercise itself the appointing authority powers or delegate them to one of its members or to a staff member of the Competence Centre other than the Executive Director.	4. Where exceptional circumstances so require, the Governing Board may by decision temporarily suspend the delegation of the appointing authority powers to the Executive Director and any sub-delegation made by the latter. In such a case the Governing Board shall exercise itself the appointing authority powers or delegate them to one of its members or to a staff member of the Competence Centre other than the Executive Director.	4. Where exceptional circumstances so require, the Governing Board may, <u>through a by</u> decision, temporarily suspend the delegation of the appointing authority powers to the Executive Director and any sub-delegation made by the latter. In such a case the Governing Board shall exercise itself the appointing authority powers or delegate them to one of its members or to a staff member of the Competence <u>staff of the</u> Centre other than the Executive Director.
				Text Origin: Council Mandate
Article 31(5)				
G	306	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.	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.	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.
				Text Origin: Commission Proposal

Article 31(6)				
G	307	6. The staff resources shall be determined in the staff establishment plan of the Competence Centre, indicating the number of temporary posts by function group and by grade and the number of contract staff expressed in full-time equivalents, in line with its annual budget.	6. The staff resources shall be determined in the staff establishment plan of the Competence Centre, indicating the number of temporary posts by function group and by grade and the number of contract staff expressed in full-time equivalents, in line with its annual budget.	6. The staff resources shall be determined in the staff establishment plan of the Competence Centre <u>referred to in point (g) of Article 13(3)</u> , indicating the number of temporary posts by function group and by grade and the number of contract staff expressed in full-time equivalents, in line with its annual budget.
				Text Origin: Council Mandate
Article 31(7)				
	308	7. The staff of the Competence Centre shall consist of temporary staff and contract staff.	7. The staff of The Competence Centre <u>shall aim to achieve gender balance among its staff. The staff</u> shall consist of temporary staff and contract staff.	7. The staff of the Competence <u>human resources required in the Centre shall be met primarily by redeployment of staff or posts from Union institutions, bodies, offices and agencies. The staff of the</u> Centre shall <u>may</u> consist of temporary staff and contract staff.
				1. EP to suggest general article on gender balance 2. 'primarily by redeployment' not acceptable to EP. 3. Council to consider combination lines 276 and 308 4. EP and Commission to check
Article 31(8)				
Y	309	8. All costs related to staff shall be borne by the Competence Centre.	8. All costs related to staff shall be borne by the Competence Centre.	8. All costs related to staff shall be borne by the Competence Centre.
				use of 'Competence' Text Origin: Commission Proposal

Article 32				
G	310	Article 32 Seconded national experts and other staff	Article 32 Seconded national experts and other staff	Article 32 Seconded national experts and other staff Text Origin: Commission Proposal
Article 32(1)				
Y	311	1. The Competence Centre may make use of seconded national experts or other staff not employed by the Competence Centre.	1. The Competence Centre may make use of seconded national experts or other staff not employed by the Competence Centre.	1. The Competence Centre may make use of seconded national experts or other staff not employed by the Competence Centre. use of 'Competence' Text Origin: Commission Proposal
Article 32(2)				
Y	312	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.	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.	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. use of 'Competence' Text Origin: Commission Proposal

Article 33				
G	313	Article 33 Privileges and Immunities	Article 33 Privileges and Immunities	Article 33 Privileges and Immunities Text Origin: Commission Proposal
Article 33, first paragraph				
Y	314	Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union shall apply to the Competence Centre and its staff.	Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union shall apply to the Competence Centre and its staff.	Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union shall apply to the Competence Centre and its staff. use of 'Competence' Text Origin: Commission Proposal
CHAPTER V				
G	315	CHAPTER V COMMON PROVISIONS	CHAPTER V COMMON PROVISIONS	CHAPTER V COMMON PROVISIONS Text Origin: Commission Proposal
Article 34				
G	316	Article 34 Security Rules	Article 34 Security Rules	Article 34 Security Rules Text Origin: Commission Proposal

Article 34(1)				
317	1. Article 12(7) Regulation (EU) No XXX [Digital Europe Programme] shall apply to participation in all actions funded by the Competence Centre.	1. Article 12(7) Regulation (EU) No XXX [Digital Europe Programme] shall apply to participation in all actions funded by the Competence Centre.	1. Article 12(7) 12 Regulation (EU) No XXX [Digital Europe Programme] shall apply to participation in all actions funded by the Competence Centre.	1. Article 12(7) 12 Regulation (EU) No XXX [Digital Europe Programme] shall apply to participation in all actions funded by the Competence Centre. use of 'Competence' Text Origin: Council Mandate
Article 34(2), introductory part				
G 318	2. The following specific security rules shall apply to actions funded from Horizon Europe:	2. The following specific security rules shall apply to actions funded from Horizon Europe:	2. The following specific security rules shall apply to actions funded from Horizon Europe:	2. The following specific security rules shall apply to actions funded from Horizon Europe: Text Origin: Commission Proposal
Article 34(2), point(a)				
319	(a) for the purposes of Article 34(1) [Ownership and protection] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan, the grant of non-exclusive licenses may be limited to third parties established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States;	(a) for the purposes of Article 34(1) [Ownership and protection] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan, the grant of non-exclusive licenses may be limited to third parties established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States;	(a) for the purposes of Article Article 34(1) [Ownership and protection] of Regulation (EU) No XXX [Horizon Europe], when provided for in the <u>annual work programme Work plan</u> , the grant of non-exclusive licenses may be limited to third parties established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States;	(a) for the purposes of Article Article 34(1) [Ownership and protection] of Regulation (EU) No XXX [Horizon Europe], when provided for in the <u>annual work programme Work plan</u> , the grant of non-exclusive licenses may be limited to third parties established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States; Text Origin: Council Mandate

Article 34(2), point(b)				
320	(b) for the purposes of Article 36(4)(b) [Transfer and licensing] of Regulation (EU) No XXX [Horizon Europe], the transfer or license to a legal entity established in an associated country or established in the Union but controlled from third countries shall also be a ground to object to transfers of ownership of results, or to grants of an exclusive license regarding results;	(b) for the purposes of Article 36(4)(b) [Transfer and licensing] of Regulation (EU) No XXX [Horizon Europe], the transfer or license to a legal entity established in an associated country or established in the Union but controlled from third countries shall also be a ground to object to transfers of ownership of results, or to grants of an exclusive license regarding results;	(b) for the purposes of Article 36(4)(b) [Transfer and licensing] of Regulation (EU) No XXX [Horizon Europe], the transfer or license to a legal entity established in an associated country or established in the Union but controlled from third countries shall also be a ground <u>for objection</u> to object to transfers of ownership of results, or to grants of an exclusive license regarding results;.	(b) for the purposes of Article 36(4)(b) [Transfer and licensing] of Regulation (EU) No XXX [Horizon Europe], the transfer or license to a legal entity established in an associated country or established in the Union but controlled from third countries shall also be a ground <u>for objection</u> to object to transfers of ownership of results, or to grants of an exclusive license regarding results;. Text Origin: Council Mandate
Article 34(2), point(c)				
321	(c) for the purposes of Article 37(3)(a) [Access rights] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan, granting of access to results and background may be limited only to a legal entity established or deemed to be established in Members States and/or nationals of Member States.	(c) for the purposes of Article 37(3)(a) [Access rights] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan, granting of access to results and background may be limited only to a legal entity established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States.	(c) for the purposes of Article 37(3)(a) [Access rights] of Regulation (EU) No XXX [Horizon Europe], when provided for in the <u>annual work programme</u> Work plan , granting of access to results and background may be limited only to a legal entity established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States.	(c) for the purposes of Article 37(3)(a) [Access rights] of Regulation (EU) No XXX [Horizon Europe], when provided for in the <u>annual work programme</u> Work plan , granting of access to results and background may be limited only to a legal entity established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States. Text Origin: Council Mandate

Article 34(2), point(ca)				
321a		<u>(ca) Articles 22 [Ownership of results], 23 [Ownership of results] and 30 [Application of the rules on classified information] of Regulation (EU) 2019/XXX [European Defence Fund] shall apply to participation in all defence-related actions by the Competence Centre, when provided for in the work plan, and the grant of non-exclusive licenses may be limited to third parties established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States.</u>		Defence/dual use aspect
Article 35				
G 322	Article 35 Transparency	Article 35 Transparency	Article 35 Transparency	Article 35 Transparency Text Origin: Commission Proposal
Article 35(1)				
Y 323	1. The Competence Centre shall carry out its activities with a high level of transparency.	1. The Competence Centre shall carry out its activities with a high <u>the highest</u> level of transparency.	1. The Competence Centre shall carry out its activities with a high level of transparency.	1. The Competence Centre shall carry out its activities with a high <u>[the highest]</u> level of transparency. use of 'Competence' Text Origin: EP Mandate

Article 35(2)					
Y	324	2. The Competence Centre shall ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information, in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Article 41.	2. The Competence Centre shall ensure that the public and any interested parties are <u>provided with comprehensive</u> , given appropriate, objective, reliable and easily accessible information <u>in due time</u> , in particular with regard to the results of <u>the work of the Competence Centre, the Network, the Industry and Scientific Advisory Board and the Community</u> its work . It shall also make public the declarations of interest made in accordance with Article 41 <u>42</u> .	2. The Competence Centre shall ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information, in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Article 41 <u>42</u> .	2. The Competence Centre shall ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information <u>in due time</u> , in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Article <u>42. The same transparency requirement applies to the national coordination centres, the community [and the advisory board] in accordance with relevant legislation</u> 41 . use of 'Competence'
Article 35(3)					
Y	325	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.	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.	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.	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. use of 'Competence' Text Origin: Commission Proposal

Article 35(4)				
Y	326	4. The Competence Centre shall lay down, in its rules of procedure, the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2. For actions funded from Horizon Europe this will take due account of the provisions in Annex III of the Horizon Europe Regulation.	4. The Competence Centre shall lay down, in its rules of procedure, the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2. For actions funded from Horizon Europe this will take due account of the provisions in Annex III of the Horizon Europe Regulation.	4. The Competence Centre shall lay down, in its rules of procedure, the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2. For actions funded from Horizon Europe this will take due account of the provisions in Annex III of the Horizon Europe Regulation. use of 'Competence' Text Origin: Council Mandate
Article 36				
G	327	Article 36 Security rules on the protection of classified information and sensitive non-classified information	Article 36 Security rules on the protection of classified information and sensitive non-classified information	Article 36 Security rules on the protection of classified information and sensitive non-classified information Text Origin: Commission Proposal
Article 36(1)				
G	328	1. Without prejudice to Article 35, the Competence Centre shall not divulge to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment, in whole or in part, has been made.	1. Without prejudice to Article 35, the Competence Centre shall not divulge to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment, in whole or in part, has been made.	<div>deleted</div> 1. Without prejudice to Article 35, the Competence Centre shall not divulge to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment, in whole or in part, has been made. deleted

Article 36(2)					
Y	329	<p>2. Members of the Governing Board, the Executive Director, the members of the Industrial and Scientific Advisory Board, external experts participating in ad hoc Working Groups, and members of the staff of the Centre shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union, even after their duties have ceased.</p>	<p>2. Members of the Governing Board, the Executive Director, the members of the Industrial and Scientific Advisory Board, external experts participating in ad hoc Working Groups, and members of the staff of the Centre shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union, even after their duties have ceased.</p>	<p>2. Members ofThe Governing Board,the Executive Director, the members of the Industrial and Scientific Advisory Board, external experts participating in ad hoc Working Groups, and members of the staff of the Centre shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union, even after their duties have ceased <u>shall adopt the Centre's security rules, following approval by the Commission, based on the principles and rules laid down in Commission Decisions (EU, Euratom) 2015/443¹ and 2015/444².</u></p> <p><u>1. Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).</u></p> <p><u>2. 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).</u></p>	
				<p>2. Members ofThe Governing Board,the Executive Director, the members of the Industrial and Scientific Advisory Board, external experts participating in ad hoc Working Groups, and members of the staff of the Centre shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union, even after their duties have ceased <u>shall adopt the Centre's security rules, following approval by the Commission, based on [and equivalent to] the principles and rules laid down in Commission Decisions (EU, Euratom) 2015/443¹ and 2015/444².</u></p> <p><u>1. Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).</u></p> <p><u>2. 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).</u></p> <p>Commission to check part in brackets</p> <p>Text Origin: Council Mandate</p>	Y

Article 36(3)						
Y	330	<p>3. The Governing Board of the Competence Centre shall adopt the Competence Centre's security rules, following approval by the Commission, based on the principles and rules laid down in the Commission's security rules for protecting European Union classified information (EUCI) and sensitive non-classified information including inter alia provisions for the processing and storage of such information as set out in Commission Decisions (EU, Euratom) 2015/443¹ and 2015/444².</p> <p>1. Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).</p> <p>2. 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).</p>	<p>3. The Governing Board of the Competence Centre shall adopt the Competence Centre's security rules, following approval by the Commission, based on the principles and rules laid down in the Commission's security rules for protecting European Union classified information (EUCI) and sensitive non-classified information including inter alia provisions for the processing and storage of such information as set out in Commission Decisions (EU, Euratom) 2015/443¹ and 2015/444².</p> <p>1. Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).</p> <p>2. 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).</p>	<p>3. The Governing Board <u>Members</u> of the Competence Centre shall adopt the Competence Centre's security rules, following approval by the Commission, based on the principles and rules laid down in the Commission's security rules for protecting European Union classified information (EUCI) and sensitive non-classified information including inter alia provisions for the processing and storage of such information as set out in Commission Decisions (EU, Euratom) 2015/443¹ and 2015/444² <u>Governing Board, the Executive Director, external experts participating in ad hoc Working Groups, and members of the staff of the Centre shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union, even after their duties have ceased.</u></p> <p>1. Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).</p> <p>2. 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).</p>	<p>3. The Governing Board <u>Members</u> of the Competence Centre shall adopt the Competence Centre's security rules, following approval by the Commission, based on the principles and rules laid down in the Commission's security rules for protecting European Union classified information (EUCI) and sensitive non-classified information including inter alia provisions for the processing and storage of such information as set out in Commission Decisions (EU, Euratom) 2015/443¹ and 2015/444² <u>Governing Board, the Executive Director, external experts participating in ad hoc Working Groups, and members of the staff of the Centre shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union, even after their duties have ceased.</u></p> <p>1. Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).</p> <p>2. 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).</p> <p>use of 'Competence'</p> <p>Text Origin: Council Mandate</p>	Y

Article 36(4)				
Y	331	4. The Competence Centre may take all necessary measures to facilitate the exchange of information relevant to its tasks with the Commission and the Member States and where appropriate, the relevant Union agencies and bodies. Any administrative arrangement concluded to this end on sharing EUCI or, in the absence of such arrangement, any exceptional ad hoc release of EUCI shall have received the Commission's prior approval.	4. The Competence Centre may take all necessary measures to facilitate the exchange of information relevant to its tasks with the Commission and the Member States and where appropriate, the relevant Union agencies and bodies. Any administrative arrangement concluded to this end on sharing EUCI or, in the absence of such arrangement, any exceptional ad hoc release of EUCI shall have received the Commission's prior approval.	4. The Competence Centre may take all necessary measures to facilitate the exchange of information relevant to its tasks with the Commission and the Member States and where appropriate, the relevant Union agencies and bodies. Any administrative arrangement concluded to this end on sharing EUCI or, in the absence of such arrangement, any exceptional ad hoc release of EUCI shall have received the Commission's prior approval. use of 'Competence' Text Origin: Commission Proposal
Article 37				
G	332	Article 37 Access to documents	Article 37 Access to documents	Article 37 Access to documents Text Origin: Commission Proposal
Article 37(1)				
Y	333	1. Regulation (EC) No 1049/2001 shall apply to documents held by the Competence Centre.	1. Regulation (EC) No 1049/2001 shall apply to documents held by the Competence Centre.	1. Regulation (EC) No 1049/2001 shall apply to documents held by the Competence Centre. use of 'Competence' Text Origin: Commission Proposal

Article 37(2)				
Y	334	2. The Governing Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001 within six months of the establishment of the Competence Centre.	2. The Governing Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001 within six months of the establishment of the Competence Centre.	2. The Governing Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001 within six months of the establishment of the Competence Centre. use of 'Competence' Text Origin: Commission Proposal
Article 37(3)				
Y	335	3. Decisions taken by the Competence Centre pursuant to Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the Ombudsman under Article 228 of Treaty on the Functioning of the European Union or of an action before the Court of Justice of the European Union under Article 263 of Treaty on the Functioning of the European Union.	3. Decisions taken by the Competence Centre pursuant to Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the Ombudsman under Article 228 of Treaty on the Functioning of the European Union or of an action before the Court of Justice of the European Union under Article 263 of Treaty on the Functioning of the European Union.	3. Decisions taken by the Competence Centre pursuant to Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the Ombudsman under Article 228 of Treaty on the Functioning of the European Union or of an action before the Court of Justice of the European Union under Article 263 of Treaty on the Functioning of the European Union. use of 'Competence' Text Origin: Commission Proposal
Article 38				
G	336	Article 38 Monitoring, evaluation and review	Article 38 Monitoring, evaluation and review	Article 38 Monitoring, evaluation and review Text Origin: Commission Proposal

Article 38(1)					
Y	337	<p>1. The Competence Centre shall ensure that its activities, including those managed through the National Coordination Centres and the Network, shall be subject to continuous and systematic monitoring and periodic evaluation. The Competence Centre shall ensure that the data for monitoring programme implementation and results are collected efficiently, effectively, and in timely manner and proportionate reporting requirements shall be imposed on recipients of Union funds and Member States. The outcomes of the evaluation shall be made public.</p>	<p>1. The Competence Centre shall ensure that its activities, including those managed through the National Coordination Centres and the Network, shall be subject to continuous and systematic monitoring and periodic evaluation. The Competence Centre shall ensure that the data for monitoring programme implementation and results are collected efficiently, effectively, and in timely manner and proportionate reporting requirements shall be imposed on recipients of Union funds and Member States. The outcomes of the evaluation shall be made public.</p>	<p>1. The Competence Centre shall ensure that its activities, including those managed through the National Coordination Centres and the Network, shall be subject to continuous and systematic monitoring and periodic evaluation. The Competence Centre shall ensure that the data for monitoring programme implementation and results are collected efficiently, effectively, and in <u>a</u> timely manner and proportionate reporting requirements shall be imposed on recipients of Union funds and Member States. The outcomes of the <u>conclusions of that</u> evaluation shall be made public.</p> <p>use of 'Competence'</p> <p>Text Origin: Council Mandate</p>	Y

Article 38(2)				
Y	338	<p>2. Once there is sufficient information available about the implementation of this Regulation, but no later than three and a half years after the start of the implementation of this Regulation, the Commission shall carry out an interim evaluation of the Competence Centre. The Commission shall prepare a report on that evaluation and shall submit that report to the European Parliament and to the Council by 31 December 2024. The Competence Centre and Member States shall provide the Commission with the information necessary for the preparation of that report.</p>	<p>2. Once there is sufficient information available about the implementation of this Regulation, but no later than three and a half years after the start of the implementation of this Regulation, the Commission shall carry out an interim evaluation of the Competence Centre. The Commission shall prepare a report on that evaluation and shall submit that report to the European Parliament and to the Council by 31 December 2024. The Competence Centre and Member States shall provide the Commission with the information necessary for the preparation of that report.</p>	<p>2. Once there is sufficient information available about the implementation of this Regulation, but no later than three and a half years after the start of the implementation<u>two years after the date referred to in Article 45 paragraph 4</u> of this Regulation, the Commission shall carry out an interim evaluation of the <u>Centre following the input of the Governing Board</u>Competence Centre. The Commission shall prepare a report on that evaluation and shall submit that report to the European Parliament and to the Council by 31 December 2024. The Competence<u>2023. The</u> Centre and Member States shall provide the Commission with the information necessary for the preparation of that report.</p> <p>Commission to check</p> <p>use of 'Competence'</p> <p>Text Origin: Council Mandate</p>

Article 38(3)				
339	<p>3. The evaluation referred to in paragraph 2 shall include an assessment of the results achieved by the Competence Centre, having regard to its objectives, mandate and tasks. If the Commission considers that the continuation of the Competence Centre is justified with regard to its assigned objectives, mandate and tasks, it may propose that the duration of the mandate of the Competence Centre set out in Article 46 be extended.</p>	<p>3. The evaluation referred to in paragraph 2 shall include an assessment of the results achieved by the Competence Centre, having regard to its objectives, mandate and tasks, <u>effectiveness, and efficiency</u>. If the Commission considers that the continuation of the Competence Centre is justified with regard to its assigned objectives, mandate and tasks, it may propose that the duration of the mandate of the Competence Centre set out in Article 46 be extended.</p>	<p>3. The evaluation referred to in paragraph 2 shall include <u>in particular:</u> <u>(a) an assessment of the working capacity of the Centre regarding objectives, mandate and tasks and the cooperation and coordination with other relevant actors, particularly National Coordination Centres, the Cybersecurity Competence Community and ENISA;</u> <u>(b) an assessment of the results achieved by the Competence Centre, having regard to its mission, objectives, mandate and tasks. If the Commission considers that the continuation, and in particular the efficiency of the Centre in coordinating Union funds and pooling expertise;</u> <u>(c) an assessment of the coherence of implementation tasks in accordance with the Agenda and the multiannual work programme;</u> <u>(d) an assessment of the Competence coordination and cooperation of the Centre is justified with regard to its assigned objectives, mandate and tasks, it may propose that the duration with the <u>Program Committee of the Horizon Europe programme and the Digital Europe programme, especially with a view to increasing coherence and synergy with the strategic planning</u> of the mandate of the Competence Centre set out in Article 46 be extended. <u>Centre, the Horizon Europe programme and the Digital Europe programme;</u></u></p>	Commission to suggest new text

			<u>(e) an assessment on joint actions;</u>	
Article 38(3), point(a)				
339a			<p><u>(a) After the submission of the report referred to in paragraph 2 of this Article, the Commission shall carry out a final evaluation of the Centre following the input of the Governing Board. That final evaluation shall refer to or update, as necessary, the assessments referred to in paragraph 3 of this Article and shall be carried out before the period specified in Article 46(1), in order to determine well in advance whether the duration of the Centre should be extended beyond that period. That final evaluation shall include legal and administrative considerations whether the mandate of the Centre could be transferred to a different Union body to create synergies and reduce fragmentation.</u></p> <p><u>If the Commission considers that the continuation of the Centre is justified with regard to its assigned objectives, mandate and tasks, it may make a legislative proposal to extend the duration of the mandate of the Centre set out in Article 46.</u></p>	
Article 38(4)				
340	4. On the basis of the conclusions of the interim evaluation referred to in paragraph 2 the Commission may act in accordance with [Article 22(5)] or take any other appropriate actions.	4. On the basis of the conclusions of the interim evaluation referred to in paragraph 2 the Commission may act in accordance with [Article 22(5)] or take any other appropriate actions.	4. On the basis of the conclusions of the interim evaluation referred to in paragraph 2, the Commission may act in accordance with [Article 22(5)] or take any other appropriate actions.	<p>4. On the basis of the conclusions of the interim evaluation referred to in paragraph 2, the Commission may act in accordance with [Article 22(5)] or take any other appropriate actions.</p> <p>Text Origin: Council Mandate</p>

Article 38(5)				
341	5. The monitoring, evaluation, phasing out and renewal of the contribution from Horizon Europe will follow the provisions of articles 8, 45 and 47 and Annex III of the Horizon Europe Regulation and agreed implementation modalities.	5. The monitoring, evaluation, phasing out and renewal of the contribution from Horizon Europe will follow the provisions of articles 8, 45 and 47 and Annex III of the Horizon Europe Regulation and agreed implementation modalities.	5. The monitoring, evaluation, phasing out and renewal of the contribution from Horizon Europe will follow the provisions of Articles 8, 45 and 47 and Annex III of the Horizon Europe Regulation and agreed implementation modalities <u>arrangements</u> .	5. The monitoring, evaluation, phasing out and renewal of the contribution from Horizon Europe will follow the provisions of Articles 8, 45 and 47 and Annex III of the Horizon Europe Regulation and agreed implementation modalities <u>arrangements</u> . check deletion of annex III Text Origin: Council Mandate
Article 38(6)				
342	6. The monitoring, reporting and evaluation of the contribution from Digital Europe will follow the provisions of articles 24, 25 of the Digital Europe programme.	6. The monitoring, reporting and evaluation of the contribution from Digital Europe will follow the provisions of articles 24, 25 of the Digital Europe programme.	6. The monitoring, reporting and evaluation of the contribution from Digital Europe will follow the provisions of Articles 24, 25 of the Digital Europe programme.	6. The monitoring, reporting and evaluation of the contribution from Digital Europe will follow the provisions of articles 24, 25 of the Digital Europe programme. Text Origin: Commission Proposal

Article 38(7)				
343	7. In case of a winding up of the Competence Centre, the Commission shall conduct a final evaluation of the Competence Centre within six months after the winding-up of the Competence Centre, but no later than two years after the triggering of the winding-up procedure referred to in Article 46 of this Regulation. The results of that final evaluation shall be presented to the European Parliament and to the Council.	7. In case of a winding up of the Competence Centre, the Commission shall conduct a final evaluation of the Competence Centre within six months after the winding-up of the Competence Centre, but no later than two years after the triggering of the winding-up procedure referred to in Article 46 of this Regulation. The results of that final evaluation shall be presented to the European Parliament and to the Council.	7. In case of a winding up of the Competence Centre, the Commission shall conduct a final evaluation of the Competence Centre within six months after the winding-up of the Competence Centre, but no later than two years after the triggering of the winding-up procedure referred to in Article 46 of this Regulation. The results of that final evaluation shall be presented to the European Parliament and to the Council.	7. In case of a winding up of the Competence Centre, the Commission shall conduct a final evaluation of the Competence Centre within six months after the winding-up of the Competence Centre, but no later than two years after the triggering of the winding-up procedure referred to in Article 46 of this Regulation. The results of that final evaluation shall be presented to the European Parliament and to the Council. use of 'Competence' Text Origin: Commission Proposal
Article 38a				
343a		<u>Article 38a</u> <u>Legal Personality of the Competence Centre</u> Moved from Article 1 (4) without modifications		<u>Article 38a</u> <u>Legal Personality of the Competence Centre</u> lawyer linguists to decide appropriate place Text Origin: EP Mandate
Article 38a(1)				
343b		<u>1. The Competence Centre shall have legal personality.</u>		<u>1. The Competence Centre shall have legal personality.</u> Text Origin: EP Mandate

Article 38a(2)				
343c		<u>2. In each Member State, the Competence Centre shall enjoy the most extensive legal capacity accorded to legal persons under the law of that Member State. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings.</u>		<u>2. [In each Member State, the Competence Centre shall enjoy the most extensive legal capacity accorded to legal persons under the law of that Member State. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings.]</u> Council to check Was part of initial Commission proposal in then Art 1(4) and is covered by Council mandate Text Origin: EP Mandate
Article 39				
344	Article 39 Liability of the Competence Centre	Article 39 Liability of the Competence Centre	Article 39 Liability of the Competence Centre	Article 39 Liability of the Competence Centre use of 'Competence' Text Origin: Commission Proposal
Article 39(1)				
345	1. The contractual liability of the Competence Centre shall be governed by the law applicable to the agreement, decision or contract in question.	1. The contractual liability of the Competence Centre shall be governed by the law applicable to the agreement, decision or contract in question.	1. The contractual liability of the Competence Centre shall be governed by the law applicable to the agreement, decision or contract in question.	1. The contractual liability of the Competence Centre shall be governed by the law applicable to the agreement, decision or contract in question. use of 'Competence' Text Origin: Commission Proposal

Article 39(2)				
Y	346	2. In the case of non-contractual liability, the Competence Centre shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its staff in the performance of their duties.	2. In the case of non-contractual liability, the Competence Centre shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its staff in the performance of their duties.	2. In the case of non-contractual liability, the Competence Centre shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its staff in the performance of their duties. use of 'Competence' Text Origin: Commission Proposal
Article 39(3)				
Y	347	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.	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.	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. use of 'Competence' Text Origin: Commission Proposal
Article 39(4)				
Y	348	4. The Competence Centre shall be solely responsible for meeting its obligations.	4. The Competence Centre shall be solely responsible for meeting its obligations.	4. The Competence Centre shall be solely responsible for meeting its obligations. use of 'Competence' Text Origin: Commission Proposal

Article 40				
G	349	Article 40 Jurisdiction of the Court of Justice of the European Union and applicable law	Article 40 Jurisdiction of the Court of Justice of the European Union and applicable law	Article 40 Jurisdiction of the Court of Justice of the European Union and applicable law Text Origin: Commission Proposal
Article 40(1), introductory part				
G	350	1. The Court of Justice of the European Union shall have jurisdiction:	1. The Court of Justice of the European Union shall have jurisdiction:	1. The Court of Justice of the European Union shall have jurisdiction: Text Origin: Commission Proposal
Article 40(1), point(1)				
Y	351	(1) pursuant to any arbitration clause contained in agreements, decisions or contracts concluded by the Competence Centre;	(1) pursuant to any arbitration clause contained in agreements, decisions or contracts concluded by the Competence Centre;	(1) pursuant to any arbitration clause contained in agreements, decisions or contracts concluded by the Competence Centre; use of 'Competence' Text Origin: Commission Proposal

Article 40(1), point(2)				
Y	352	(2) in disputes related to compensation for damage caused by the staff of the Competence Centre in the performance of their duties;	(2) in disputes related to compensation for damage caused by the staff of the Competence Centre in the performance of their duties;	(2) in disputes related to compensation for damage caused by the staff of the Competence Centre in the performance of their duties; use of 'Competence' Text Origin: Commission Proposal
Article 40(1), point(3)				
Y	353	(3) in any dispute between the Competence Centre and its staff within the limits and under the conditions laid down in the Staff Regulations.	(3) in any dispute between the Competence Centre and its staff within the limits and under the conditions laid down in the Staff Regulations.	(3) in any dispute between the Competence Centre and its staff within the limits and under the conditions laid down in the Staff Regulations. use of 'Competence' Text Origin: Commission Proposal
Article 40(2)				
Y	354	2. Regarding any matter not covered by this Regulation or by other Union legal acts, the law of the Member State where the seat of the Competence Centre is located shall apply.	2. Regarding any matter not covered by this Regulation or by other Union legal acts, the law of the Member State where the seat of the Competence Centre is located shall apply.	2. Regarding any matter not covered by this Regulation or by other Union legal acts, the law of the Member State where the seat of the Competence Centre is located shall apply. use of 'Competence' Text Origin: Commission Proposal

Article 41					
G	355	Article 41 Liability of members and insurance	Article 41 Liability of members and insurance	Article 41 Liability of members and insurance	Article 41 Liability of members and insurance Text Origin: Commission Proposal
Article 41(1)					
Y	356	1. The financial liability of the members for the debts of the Competence Centre shall be limited to their contribution already made for the administrative costs.	1. The financial liability of the members for the debts of the Competence Centre shall be limited to their contribution already made for the administrative costs.	1. The financial liability of the members for the debts of the Competence Centre shall be limited to their contribution already made for the administrative costs.	1. The financial liability of the members for the debts of the Competence Centre shall be limited to their contribution already made for the administrative costs. use of 'Competence' Text Origin: Commission Proposal
Article 41(2)					
Y	357	2. The Competence Centre shall take out and maintain appropriate insurance.	2. The Competence Centre shall take out and maintain appropriate insurance.	2. The Competence Centre shall take out and maintain appropriate insurance.	2. The Competence Centre shall take out and maintain appropriate insurance. use of 'Competence' Text Origin: Commission Proposal
Article 42					
G	358	Article 42 Conflicts of interest	Article 42 Conflicts of interest	Article 42 Conflicts of interest	Article 42 Conflicts of interest Text Origin: Commission Proposal

Article 42, first paragraph				
359	<p>The Competence Centre Governing Board shall adopt rules for the prevention and management of conflicts of interest in respect of its members, bodies and staff. Those rules shall contain the provisions intended to avoid a conflict of interest in respect of the representatives of the members serving in the Governing Board as well as the Scientific and Industrial Advisory Board in accordance with Regulation XXX [new Financial Regulation].</p>	<p><u>1</u> The Competence Centre Governing Board shall adopt rules for the prevention, <u>identification, and resolution</u> and management of conflicts of interest in respect of its members, bodies and staff. Those rules shall contain the provisions intended to avoid a conflict of interest in respect of the representatives of the members serving in, <u>including the Executive Director,</u> the Governing Board, as well as the Scientific and Industrial Advisory Board in accordance with Regulation XXX [new Financial Regulation], <u>and the Community.</u></p>	<p>The Competence Centre Governing Board shall adopt rules for the prevention and management of conflicts of interest in respect of its members, bodies and staff. Those rules shall contain the provisions intended to avoid a conflict of interest in respect of the representatives of the members serving in the Governing Board <u>in accordance with Regulation (EU, Euratom) 2018/1046, including provisions on any declarations of interest. Regarding conflict of interest, the National Coordination Centres shall be subject to national law as well as the Scientific and Industrial Advisory Board in accordance with Regulation XXX [new Financial Regulation].</u></p>	<p>The Competence Centre Governing Board shall adopt rules for the prevention, <u>identification and resolution</u> and management of conflicts of interest in respect of its members, bodies and staff, <u>including the Executive Director.</u> Those rules shall contain the provisions intended to avoid a conflict of interest in respect of the representatives of the members serving in the Governing Board as well as the Scientific and Industrial Advisory Board in accordance with Regulation XXX [new Financial Regulation] <u>in accordance with Regulation (EU, Euratom) 2018/1046, including provisions on any declarations of interest. Regarding conflict of interest, the National Coordination Centres shall be subject to national law.</u></p> <p>addition of Community to be checked</p> <p>Advisory board</p> <p>Text Origin: Council Mandate</p>
Article 42, first paragraph a				
359a		<p><u>2 Member States shall ensure the prevention, identification, and resolution of conflicts of interest in respect of the National Coordination Centres.</u></p>		<p>deleted</p>

Article 42, first paragraph b				
359b		<u>3 The rules referred to in the first paragraph shall comply with Regulation (EU,Euratom) 2018/1046.</u>		<u>deleted</u>
Article 43				
360	Article 43 Protection of Personal Data	Article 43 Protection of Personal Data	Article 43 Protection of Personal Data	Article 43 Protection of Personal Data Text Origin: Commission Proposal
Article 43(1)				
361	1. The processing of personal data by the Competence Centre shall be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council.	1. The processing of personal data by the Competence Centre shall be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council.	1. The processing of personal data by the Competence Centre shall be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council <u>1725/2018</u> .	1. The processing of personal data by the Competence Centre shall be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council <u>1725/2018</u> . Text Origin: Council Mandate
Article 43(2)				
362	2. The Governing Board shall adopt implementing measures referred to in Article xx(3) of Regulation (EU) No xxx/2018. The Governing Board may adopt additional measures necessary for the application of Regulation (EU) No xxx/2018 by the Competence Centre.	2. The Governing Board shall adopt implementing measures referred to in Article xx(3) of Regulation (EU) No xxx/2018. The Governing Board may adopt additional measures necessary for the application of Regulation (EU) No xxx/2018 by the Competence Centre.	2. The Governing Board shall adopt implementing measures referred to in Article xx(3) <u>45(3)</u> of Regulation (EU) No xxx/2018 <u>1725/2018</u> . The Governing Board may adopt additional measures necessary for the application of Regulation (EU) No xxx/2018 <u>No 1725/2018</u> by the Competence Centre.	2. The Governing Board shall adopt implementing measures referred to in Article xx(3) <u>45(3)</u> of Regulation (EU) No xxx/2018 <u>1725/2018</u> . The Governing Board may adopt additional measures necessary for the application of Regulation (EU) No xxx/2018 <u>No 1725/2018</u> by the Competence Centre. Text Origin: Council Mandate

Article 44				
363	Article 44 Support from the host Member State	Article 44 <u>Seat and</u> support from the host Member State Provisions regarding the seat have been moved from Article 1(3) to improve coherence of the text	Article 44 Support from the host Member State	
Article 44, first paragraph -a				
363a		<u>1 The seat of the Competence Centre shall be determined in a democratically accountable procedure, using transparent criteria and in accordance with Union law.</u>		Still under discussion
Article 44, first paragraph -b				
363b		<u>2 The host Member State shall provide the best possible conditions to ensure the proper functioning of the Competence Centre, including a single location, and further conditions such as the accessibility of the adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and partners.</u>		

Article 44, first paragraph				
364	An administrative agreement may be concluded between the Competence Centre and the Member State [Belgium] in which its seat is located concerning privileges and immunities and other support to be provided by that Member State to the Competence Centre.	<u>3</u> An administrative agreement may <u>shall</u> be concluded between the Competence Centre and the <u>host</u> Member State [Belgium] in which its seat is located concerning privileges and immunities and other support to be provided by that Member State to the Competence Centre.	An administrative agreement may be concluded between the Competence Centre and the Member State [Belgium] in which its seat is located concerning privileges and immunities and other support to be provided by that Member State to the Competence Centre.	
CHAPTER VI				
365	CHAPTER VI FINAL PROVISIONS	CHAPTER VI FINAL PROVISIONS	CHAPTER VI FINAL PROVISIONS	CHAPTER VI FINAL PROVISIONS Text Origin: Commission Proposal
Article 45				
366	Article 45 Initial actions	Article 45 Initial actions	Article 45 Initial actions	Article 45 Initial actions Text Origin: Commission Proposal

Article 45(1)				
Y	367	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.	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.	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. use of 'Competence' Text Origin: Commission Proposal
Article 45(2)				
Y	368	2. For the purpose of paragraph 1, until the Executive Director takes up his duties following his/her appointment by the Governing Board in accordance with Article 16, the Commission may designate an interim Executive Director and exercise the duties assigned to the Executive Director who may be assisted by a limited number of Commission officials. The Commission may assign a limited number of its officials on an interim basis.	2. For the purpose of paragraph 1, until the Executive Director takes up his duties following his/her appointment by the Governing Board in accordance with Article 16, the Commission may designate an interim Executive Director and exercise the duties assigned to the Executive Director who may be assisted by a limited number of Commission officials. The Commission may assign a limited number of its officials on an interim basis.	2. For the purpose of paragraph 1 <u>of this Article</u> , until the Executive Director takes up his <u>his/her</u> duties following his/her appointment by the Governing Board in accordance with Article 16, the Commission may designate an interim Executive Director. <u>That interim Executive Director shall</u> and exercise the duties assigned to the Executive Director who <u>and</u> may be assisted by a limited number of <u>members of staff of the Commission officials</u> . The Commission may assign a limited number of its <u>officials members of staff</u> on an interim basis. Text Origin: Council Mandate

Article 45(3)				
Y	369	3. The interim Executive Director may authorise all payments covered by the appropriations provided in the annual budget of the Competence Centre once approved by the Governing Board and may conclude agreements, decisions and contracts, including staff contracts following the adoption of the Competence Centre's staff establishment plan.	3. The interim Executive Director may authorise all payments covered by the appropriations provided in the annual budget of the Competence Centre once approved by the Governing Board and may conclude agreements, decisions and contracts, including staff contracts following the adoption of the Competence Centre's staff establishment plan.	3. The interim Executive Director may authorise all payments covered by the appropriations provided in the annual budget of the Competence Centre once approved by the Governing Board and may conclude agreements, decisions and contracts, including staff contracts following the adoption of the <u>establishment plan referred to in point (g) of Article 13(3)</u> . Competence Centre's staff establishment plan. use of 'Competence' Text Origin: Council Mandate
Article 45(4)				
Y	370	4. The interim Executive Director shall determine, in common accord with the Executive Director of the Competence Centre and subject to the approval of the Governing Board, the date on which the Competence Centre will have the capacity to implement its own budget. From that date onwards, the Commission shall abstain from making commitments and executing payments for the activities of the Competence Centre.	4. The interim Executive Director shall determine, in common accord with the Executive Director of the Competence Centre and subject to the approval of the Governing Board, the date on which the Competence Centre will have the capacity to implement its own budget. From that date onwards, the Commission shall abstain from making commitments and executing payments for the activities of the Competence Centre.	4. The interim Executive Director shall determine, in common accord with the Executive Director of the Competence Centre and subject to the approval of the Governing Board, the date on which the Competence Centre will <u>shall</u> 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. Commission to check if legal problem use of 'Competence' Text Origin: Council Mandate

Article 45a				
370a		<u>Article 45a</u> <u>Exercise of the delegation</u>		pending decision on delegated acts
Article 45a(1)				
370b		<u>1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.</u>		
Article 45a(2)				
370c		<u>2. The power to adopt delegated acts referred to in Article 6(5a) and Article 8(4b) shall be conferred on the Commission for an indeterminate period of time from ... [date of entry into force of this Regulation].</u>		
Article 45a(3)				
370d		<u>3. The delegation of power referred to in Article 6(5a) and Article 8(4b) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.</u>		

Article 45a(4)				
370e		<u>4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.</u>		
Article 45a(5)				
370f		<u>5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.</u>		
Article 45a(6)				
370g		<u>6. A delegated act adopted pursuant to Article 6(5a) and Article 8(4b) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.</u>		

Article 46				
G	371	Article 46 Duration	Article 46 Duration	Article 46 Duration Text Origin: Commission Proposal
Article 46(1)				
Y	372	1. The Competence Centre shall be established for the period from 1 January 2021 to 31 December 2029.	1. The Competence Centre shall be established for the period from 1 January 2021 to 31 December 2029.	1. The Competence Centre shall be established for the period from 1 January 2021 to 31 December 2029. use of 'Competence' Text Origin: Commission Proposal
Article 46(2)				
G	373	2. At the end of this period, unless decided otherwise through a review of this Regulation, the winding-up procedure shall be triggered. The winding-up procedure shall be automatically triggered if the Union or all participating Member States withdraw from the Competence Centre.	2. At the end of this period, unless decided otherwise through a review of this Regulation, the winding-up procedure shall be triggered. The winding-up procedure shall be automatically triggered if the Union or all participating Member States withdraw from the Competence Centre.	2. At the end of this <u>the</u> period, unless decided otherwise through a review referred to in paragraph 1 of this Regulation, the winding-up procedure shall be triggered. The winding-up procedure shall be automatically triggered if the Union or all participating Member States withdraw from the Competence Centre <u>Article, unless the mandate of the Centre is extended in accordance with the second subparagraph of Article 38(3), the winding-up procedure shall be triggered.</u> Text Origin: Council Mandate

Article 46(3)				
Y	374	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.	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.	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. use of 'Competence' use of 'Competence' Text Origin: Commission Proposal
Article 46(4)				
Y	375	4. When the Competence Centre is being wound up, its assets shall be used to cover its liabilities and the expenditure relating to its winding-up. Any surplus shall be distributed among the Union and the participating Member States in proportion to their financial contribution to the Competence Centre. Any such surplus distributed to the Union shall be returned to the Union budget.	4. When the Competence Centre is being wound up, its assets shall be used to cover its liabilities and the expenditure relating to its winding-up. Any surplus shall be distributed among the Union and the participating Member States in proportion to their financial contribution to the Competence Centre. Any such surplus distributed to the Union shall be returned to the Union budget.	4. When the Competence Centre is being wound up, its assets shall be used to cover its liabilities and the expenditure relating to its winding-up. Any surplus shall be distributed among the Union and the participating <u>contributing</u> 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. use of 'Competence' Text Origin: Council Mandate
Article 47				
G	376	Article 47 Entry into force	Article 47 Entry into force	Article 47 Entry into force Text Origin: Commission Proposal

Article 47, first paragraph				
G	377	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 enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. Text Origin: Commission Proposal
Article 47, second paragraph				
G	378	This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States.	This Regulation shall be binding in its entirety and directly applicable in all Member States. Text Origin: Commission Proposal
Formula				
G	379	Done at Brussels,	Done at Brussels,	Done at Brussels, Text Origin: Commission Proposal
Formula				
G	380	For the European Parliament	For the European Parliament	For the European Parliament Text Origin: Commission Proposal

Formula						
G	381	The President	The President	The President	The President Text Origin: Commission Proposal	G
Formula						
G	382	For the Council	For the Council	For the Council	For the Council Text Origin: Commission Proposal	G
Formula						
G	383	The President	The President	The President	The President Text Origin: Commission Proposal	G