Council of the European Union

Brussels, 29 April 2022
(OR. en)

8534/22

Interinstitutional File: 2020/0359(COD)

LIMITE

CODEC 560
CSC 173
CSCI 59
CYBER 140
DATAPROTECT 114
JAI 543
MI 320
TELECOM 172

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	8152/22
Subject:	Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148 - Examination of possible compromise proposals and preparation for the trilogue

Delegations will find attached the four column document which will be discussed at the HWP CI meeting on 3 May 2022.

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (Text with EEA relevance)

2020/0359(COD)

DRAFT [Draft after technical meeting 29 April]

29-04-2022 at 17h33

	Commission Proposal + Annexes	EP Mandate	Council Mandate	Draft Agreement
Formula				
1	2020/0359 (COD)	2020/0359 (COD)	2020/0359 (COD)	2020/0359 (COD) Text Origin: Commission Proposal + Annexes
Proposal Title				
2	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (Text with EEA relevance)	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union ***(NIS 2 Directive)***, repealing Directive (EU) 2016/1148 (Text with EEA relevance)	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (Text with EEA relevance)	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union ***(NIS 2 Directive)***, repealing Directive (EU) 2016/1148 (Text with EEA relevance) Text Origin: EP Mandate

		Commission Proposal + Annexes	EP Mandate	Council Mandate	Draft Agreement
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,	THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, Text Origin: Commission Proposal + Annexes
Citation 1					
G	4	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof, Text Origin: Commission Proposal + Annexes
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,	Having regard to the proposal from the European Commission, Text Origin: Commission Proposal + Annexes
Citation 3					
G	6				

	Commission Proposal + Annexes	EP Mandate	Council Mandate	Draft Agreement
	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments,	After transmission of the draft legislative act to the national parliaments, Text Origin: Commission Proposal + Annexes
Citation 4				
7	Having regard to the opinion of the European Economic and Social Committee[1], _____ 1. OJ C , , p. .	Having regard to the opinion of the European Economic and Social Committee[1], _____ 1. OJ C , , p. .	Having regard to the opinion of the European Economic and Social Committee[1], _____ 1. OJ C , , p. .	Having regard to the opinion of the European Economic and Social Committee[1], _____ 1. OJ C , , p. . Text Origin: Commission Proposal + Annexes
Citation 5				
8	Having regard to the opinion of the Committee of the Regions[1], _____ 1. OJ C , , p. .	Having regard to the opinion of the Committee of the Regions[1], _____ 1. OJ C , , p. .	Having regard to the opinion of the Committee of the Regions[1], _____ 1. OJ C , , p. .	Having regard to the opinion of the Committee of the Regions[1], _____ 1. OJ C , , p. . Text Origin: Commission Proposal + Annexes

Citation 6					
G	9	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 + Annexes
Formula					
G	10	Whereas:	Whereas:	Whereas:	Whereas: Text Origin: Commission Proposal + Annexes
Recital 1					
	11	(1) Directive (EU) 2016/1148 of the European Parliament and the Council[1] aimed at building cybersecurity capabilities across the Union, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the Union's economy and society to function effectively. _____ 1. Directive (EU) 2016/1148 of the European Parliament and of the Council of	(1) Directive (EU) 2016/1148 of the European Parliament and the Council[1]***, commonly known as the 'NIS directive'*** aimed at building cybersecurity capabilities across the Union, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the Union's ~~*economy and society to function effectively*~~***security and to the effective functioning of its economy and society***.	(1) Directive (EU) 2016/1148 of the European Parliament and the Council[1] aimed at building cybersecurity capabilities across the Union, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the Union's economy and society to function effectively. _____ 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 194/1, 19.7.2016 p. 1).	_____ 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 194/1, 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 194/1, 19.7.2016 p. 1).	
Recital 2				
12	(2) Since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union's level of cybersecurity resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks by defining national cybersecurity strategies, establishing national capabilities, and implementing regulatory measures covering essential infrastructures and actors identified by each Member State. It has also contributed to cooperation at Union level through the establishment of the Cooperation Group[1] and a network of national Computer Security Incident Response Teams ('CSIRTs	(2) Since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union's level of cybersecurity resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks by defining national cybersecurity strategies, establishing national capabilities, and implementing regulatory measures covering essential infrastructures and actors identified by each Member State. It has also contributed to cooperation at Union level through the establishment of the Cooperation Group[1] and a network of national Computer Security Incident Response Teams ('CSIRTs	(2) Since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union's level of cybersecurity resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks by defining national ~~*cybersecurity strategies*~~***strategies on security of network and information systems***, establishing national capabilities, and implementing regulatory measures covering essential infrastructures and actors identified by each Member State. It has also contributed to cooperation at Union level through the establishment of the Cooperation Group[1] and ~~*a*~~***the*** network of	

	network’)[2]. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges. __________ 1. Article 11 of Directive (EU) 2016/1148. 2. Article 12 of Directive (EU) 2016/1148.	network’)[2]. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges. __________ 1. Article 11 of Directive (EU) 2016/1148. 2. Article 12 of Directive (EU) 2016/1148.	national Computer Security Incident Response Teams (‘CSIRTs network’)[2]. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges. __________ 1. Article 11 of Directive (EU) 2016/1148. 2. Article 12 of Directive (EU) 2016/1148.	
Recital 3				
13	(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major	(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major	(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major	

	threat to the functioning of network and information systems. As a result, cyber incidents can impede the pursuit of economic activities in the internal market, generate financial losses, undermine user confidence and cause major damage to the Union economy and society. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market.	threat to the functioning of network and information systems. As a result, cyber incidents can impede the pursuit of economic activities in the internal market, generate financial losses, undermine user confidence and cause major damage to the Union economy and society. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market. ***Moreover, cybersecurity is a key enabler for many critical sectors to successfully embrace the digital transformation and to fully grasp the economic, social and sustainable benefits of digitalisation.***	threat to the functioning of network and information systems. As a result, cyber incidents can impede the pursuit of economic activities in the internal market, generate financial losses, undermine user confidence and cause major damage to the Union economy and society. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market.	
Recital 3a				
13a		***(3a) Large-scale cybersecurity incidents and crises at Union level require coordinated action to ensure a rapid and effective response, because of the high degree of interdependence between sectors and countries. The availability of cyber-resilient networks and information systems and the availability, confidentiality and integrity of***		

		<u>***data are vital for the security of the Union within as well as beyond its borders, as cyber threats could originate from outside the Union. The Union's ambition to acquire a more prominent geopolitical role also rests on credible cyber defence and deterrence, including the capacity to identify malicious actions in a timely and effective manner and to respond adequately.***</u>		
Recital 4				
14	(4) The legal basis of Directive (EU) 1148/2016 was Article 114 of the Treaty on the Functioning of the European Union (TFEU), the objective of which is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules. The cybersecurity requirements imposed on entities providing services or economically relevant activities vary considerably among Member States in terms of type of requirement, their level of detail and the method of supervision. Those disparities entail additional costs and create difficulties for	(4) The legal basis of Directive (EU) 1148/2016 was Article 114 of the Treaty on the Functioning of the European Union (TFEU), the objective of which is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules. The cybersecurity requirements imposed on entities providing services or economically relevant activities vary considerably among Member States in terms of type of requirement, their level of detail and the method of supervision. Those disparities entail additional costs and create difficulties for	(4) The legal basis of Directive (EU) 1148/2016 was Article 114 of the Treaty on the Functioning of the European Union (TFEU), the objective of which is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules. The cybersecurity requirements imposed on entities providing services or economically relevant activities vary considerably among Member States in terms of type of requirement, their level of detail and the method of supervision. Those disparities entail additional costs and create difficulties for	

	undertakings that offer goods or services cross-border. Requirements imposed by one Member State that are different from, or even in conflict with, those imposed by another Member State, may substantially affect those cross-border activities. Furthermore, the possibility of suboptimal design or implementation of cybersecurity standards in one Member State is likely to have repercussions on the level of cybersecurity of other Member States, notably given the intense cross-border exchanges. The review of Directive (EU) 2016/1148 has shown a wide divergence in its implementation by Member States, including in relation to its scope, the delimitation of which was very largely left to the discretion of the Member States. Directive (EU) 2016/1148 also provided the Member States with very wide discretion as regards implementing the security and incident reporting obligations set out therein. Those obligations were therefore implemented in significantly different ways at national level. Similar divergence in the implementation occurred in relation to that Directive's	undertakings that offer goods or services cross-border. Requirements imposed by one Member State that are different from, or even in conflict with, those imposed by another Member State, may substantially affect those cross-border activities. Furthermore, the possibility of suboptimal design or implementation of cybersecurity standards in one Member State is likely to have repercussions on the level of cybersecurity of other Member States, notably given the intense cross-border exchanges. The review of Directive (EU) 2016/1148 has shown a wide divergence in its implementation by Member States, including in relation to its scope, the delimitation of which was very largely left to the discretion of the Member States. Directive (EU) 2016/1148 also provided the Member States with very wide discretion as regards implementing the security and incident reporting obligations set out therein. Those obligations were therefore implemented in significantly different ways at national level. Similar divergence in the implementation occurred in relation to that Directive's	undertakings that offer goods or services cross-border. Requirements imposed by one Member State that are different from, or even in conflict with, those imposed by another Member State, may substantially affect those cross-border activities. Furthermore, the possibility of suboptimal design or implementation of cybersecurity ~~*standards*~~ ***measures*** in one Member State is likely to have repercussions on the level of cybersecurity of other Member States, notably given the intense cross-border exchanges. The review of Directive (EU) 2016/1148 has shown a wide divergence in its implementation by Member States, including in relation to its scope, the delimitation of which was very largely left to the discretion of the Member States. Directive (EU) 2016/1148 also provided the Member States with very wide discretion as regards implementing the security and incident reporting obligations set out therein. Those obligations were therefore implemented in significantly different ways at national level. Similar divergence in the implementation occurred in	

	provisions on supervision and enforcement.	provisions on supervision and enforcement.	relation to that Directive's provisions on supervision and enforcement.	
Recital 5				
15	(5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different standards. This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.	(5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different standards. ***Ultimately, those divergences could lead to higher vulnerability of some Member States to cybersecurity threats, with potential spill-over effects across the Union.*** This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the	(5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different ~~standards~~***measures***. This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.	

		effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive ***(NIS 2 Directive)***.		
Recital 5a				
15a				***(5a) Ensuring adequate resources to fulfill the objectives of this Directive and to carry out the tasks foreseen for competent authorities and CSIRTs is essential. The Member States can introduce at the national level financing mechanism for entities to cover necessary expenditure in relation to the conduct of tasks of public entities responsible for cybersecurity in the Member State pursuant to this Directive. Such mechanism should comply with Union law and should be proportionate, non-discriminatory and take into account different approaches to providing secure services. Abovementioned resources may be used to increase the general security posture of the Member State in question.*** EP to check for alternative wording
Recital 6				

16	(6) This Directive leaves unaffected the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their security, to safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[1], are of relevance. _____ 1. The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).	(6) This Directive leaves unaffected the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their security, to safeguard public policy and public security, and to allow for the ***prevention,*** investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[1], are of relevance. _____ 1. The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).	(6) ~~*This Directive leaves unaffected the ability of Member States*~~***Member States should be able*** to take the necessary measures to ensure the protection of the essential interests of their security, to safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences~~*, in compliance with Union law. In accordance with Article 346 TFEU*~~***. The Directive should not apply to certain public or private entities that carry out activities in these areas. It should also not apply to the activities of entities conducted in these areas. Furthermore***, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security.~~*In this context,*~~ National ~~*and*~~***or*** Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[1], are of relevance. _____ 1. The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is	

			used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).	
Recital 6a				
16a			***(6a) Union law on the protection of personal data and privacy applies to any processing of personal data under this Directive. In particular, this Directive is without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council and therefore should in particular not affect the tasks and powers of the independent supervisory authorities competent to monitor compliance with the respective Union data protection law.***	
Recital 6a				
16b				***(6a) In relation to public administration entities that carry out their activities in the areas of defence, national security, public security, or law enforcement, including the investigation, detection and prosecution of criminal offences, this Directive***

				should not apply insofar as those activities are predominant activities of these entities and not only marginal activities. ***Given the intensification and increased sophistication of cyber threats, Member States should strive to ensure a high level of cybersecurity for entities that are excluded from the scope of this Directive according to Article 2 paragraph 3, and to support the implementation of adequate cybersecurity risk management measures that reflect the sensitive nature of these entities.*** PCY proposal
Recital 6b				
16c				***(6b)***
Recital 7				
17	(7) With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy in light of the considerations set out in recitals (4) to (6). The sectors covered by	(7) With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy in light of the considerations set out in recitals (4) to (6). The sectors covered by	(7) With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy in light of the considerations set out in recitals (4) to (6). The sectors covered by	

	Directive (EU) 2016/1148 should therefore be extended to provide a comprehensive coverage of the sectors and services of vital importance for key societal and economic activities within the internal market. The rules should not be different according to whether the entities are operators of essential services or digital service providers. That differentiation has proven obsolete, since it does not reflect the actual importance of the sectors or services for the societal and economic activities in the internal market.	Directive (EU) 2016/1148 should therefore be extended to provide a comprehensive coverage of the sectors and services of vital importance for key societal and economic activities within the internal market. The ~~rules~~***risk management requirements and reporting obligations*** should not be different according to whether the entities are operators of essential services or digital service providers. That differentiation has proven obsolete, since it does not reflect the actual importance of the sectors or services for the societal and economic activities in the internal market.	Directive (EU) 2016/1148 should therefore be extended to provide a comprehensive coverage of the sectors and services of vital importance for key societal and economic activities within the internal market. The rules should not be different according to whether the entities are operators of essential services or digital service providers. That differentiation has proven obsolete, since it does not reflect the actual importance of the sectors or services for the societal and economic activities in the internal market.	
Recital 8				
18	(8) In accordance with Directive (EU) 2016/1148, Member States were responsible for determining which entities meet the criteria to qualify as operators of essential services (‘identification process’). In order to eliminate the wide divergences among Member States in that regard and ensure legal certainty for the risk management requirements and reporting obligations for all relevant entities, a uniform criterion should be	(8) In accordance with Directive (EU) 2016/1148, Member States were responsible for determining which entities meet the criteria to qualify as operators of essential services (‘identification process’). In order to eliminate the wide divergences among Member States in that regard and ensure legal certainty for the risk management requirements and reporting obligations for all relevant entities, a uniform criterion should be	(8) In accordance with Directive (EU) 2016/1148, Member States were responsible for determining which entities meet the criteria to qualify as operators of essential services (‘identification process’). In order to eliminate the wide divergences among Member States in that regard and ensure legal certainty for the risk management requirements and reporting obligations for all relevant entities, a uniform criterion should be	

	established that determines the entities falling within the scope of application of this Directive. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[1], that operate within the sectors or provide the type of services covered by this Directive, fall within its scope. Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion. _____ 1. Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	established that determines the entities falling within the scope of application of this Directive. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[1], that operate within the sectors or provide the type of services covered by this Directive, fall within its scope. ~~*Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion.*~~ _____ 1. Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	established that determines the entities falling within the scope of application of this Directive. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[1], that operate within the sectors or provide the type of services covered by this Directive, fall within its scope. ~~*Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion.*~~ _____ 1. Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	
Recital 8a				
18a			***(8a) In order to ensure a clear overview of the entities falling within the scope of this Directive, Member States should be able to establish national mechanisms for self-notification that require entities that are subject to this Directive to submit at least their name, address and contact details, as well as the sector in which they***	

			operate or type of service they provide and, where applicable, a list of Member States where the entity provides their services to the competent authorities under this Directive or bodies designated for that purpose by the Member States. Member States can decide on the appropriate mechanisms where registers exist at national level, that allow for the identification of entities falling within the scope of this Directive.	
Recital 9				
19	(9) However, small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit it to the Commission.	(9) However, small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. ~~*Member States should be responsible for establishing a list of such entities, and submit it to the Commission.*~~	(9) ~~*However, small or micro*~~***Micro or small*** entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. Member States should be responsible for ~~*establishing a list of such*~~***submitting to the Commission at least relevant information on the number of identified*** entities, ***the sector they belong to or type of service they provide, and the specific criteria based on which they were identified. Member States can also decide, where in accordance with***	

			national security rules, to submit ~~*and submit it*~~ to the Commission ***the names of these entities***.	
Recital 9a				
19a			***(9a) Public administration entities that carry out activities in the areas of national security, defence, public security, law enforcement, as well as the judiciary, parliaments and central banks are excluded from the scope of this Directive. For the purpose of this Directive, entities with regulatory competence are not considered as carrying out activities in the area of law enforcement and, therefore, they are not excluded on these grounds from the scope of this Directive. Furthermore public administration entities of central government that are jointly established with a third country in accordance with an international agreement are not within the scope of this Directive.***	
Recital 9a				
19b		***(9a) Member States should***		

		establish a list of all essential and important entities. That list should include the entities that meet the generally applicable size-related criteria as well as the small enterprises and microenterprises that fulfil certain criteria that indicate their key role for the economies or societies of Member States. In order for computer security incident response teams (CSIRTs) and competent authorities to provide assistance and to warn entities about cyber incidents that could affect them, it is important that those authorities have the correct contact details of the entities. Essential and important entities should therefore submit at least the following information to the competent authorities: the name of the entity, the address and up-to-date contact details, including email addresses, IP ranges, telephone numbers and relevant sector(s) and subsector(s) referred to in Annexes I and II. The entities should notify the competent authorities of any changes to that information. Member States should without undue delay, ensure that that information can be easily provided through a single entry		

		point. To that end, ENISA, in cooperation with the Cooperation Group, should without undue delay issue guidelines and templates regarding the notification obligations. Member States should notify to the Commission and the Cooperation Group of the number of essential and important entities. Member States should also notify the Commission for the purpose of the review referred to in this Directive of the names of the small enterprises and microenterprises identified as essential and important entities, in order to enable the Commission to assess consistency among the Member States' approaches. That information should be handled as strictly confidential.		
Recital 9aa				
19c			***(9aa) Member States should be able to establish that entities identified before the entry into force of this Directive as operators of essential services in accordance with Directive (EU) 2016/1148 are to be considered essential entities.***	
Recital 9aaa				

19d			***(9aaa) This Directive does not apply to Member States' diplomatic and consular missions abroad and to their ICT infrastructure used by such missions, insofar as such infrastructure is located abroad or is operated for users abroad.***	
Recital 10				
20	(10) The Commission, in cooperation with the Cooperation Group, may issue guidelines on the implementation of the criteria applicable to micro and small enterprises.	(10) The Commission, in cooperation with the Cooperation Group ***and relevant stakeholders, should*** ~~*, may*~~ issue guidelines on the implementation of the criteria applicable to ***microenterprises and small enterprises. The Commission should also ensure that appropriate guidance is given to all*** micro and small enterprises ***falling within the scope of this Directive. The Commission should, with the support of the Member States, provide microenterprises and small enterprises with information in that regard***.	(10) The Commission, in cooperation with the Cooperation Group, may issue guidelines on the implementation of the criteria applicable to micro and small enterprises.	
Recital 10a				
20a		***(10a) The Commission should***		

		also issue guidelines to support Member States in correctly implementing the provisions on the scope, and to evaluate the proportionality of the obligations set out by this Directive, in particular as regards entities with complex business models or operating environments, whereby an entity may simultaneously fulfil the criteria assigned to both essential and important entities, or may simultaneously conduct activities that are some within and some outside the scope of this Directive.		
Recital 11				
21	(11) Depending on the sector in which they operate or the type of service they provide, the entities falling within the scope of this Directive should be classified into two categories: essential and important. That categorisation should take into account the level of criticality of the sector or of the type of service, as well as the level of dependency of other sectors or types of services. Both essential and important entities should be subject to the same risk management requirements and	(11) Depending on the sector in which they operate or the type of service they provide, the entities falling within the scope of this Directive should be classified into two categories: essential and important. That categorisation should take into account the level of criticality of the sector or of the type of service, as well as the level of dependency of other sectors or types of services. Both essential and important entities should be subject to the same risk management requirements and	(11) ~~*Depending on the sector in which they operate or the type of service they provide, the*~~ Entities falling within the scope of this Directive should be classified into two categories: essential and important~~*. That categorisation should*~~ ***that*** take into account the level of criticality of the sector or of the type of ~~*service*~~***services they provide***, as well as ~~*the level of dependency of other sectors or types of services*~~***their size. In this regard, due account should also be taken of any relevant sectoral***	

	reporting obligations. The supervisory and penalty regimes between these two categories of entities should be differentiated to ensure a fair balance between requirements and obligations on one hand, and the administrative burden stemming from the supervision of compliance on the other hand.	reporting obligations. The supervisory and penalty regimes between these two categories of entities should be differentiated to ensure a fair balance between requirements and obligations on one hand, and the administrative burden stemming from the supervision of compliance on the other hand.	***risk assessments or guidance by competent authorities, where applicable***. Both essential and important entities should be subject to the ~~*same*~~ risk management requirements and reporting obligations. The supervisory and penalty regimes between these two categories of entities should be differentiated to ensure a fair balance between ***risk-based*** requirements and obligations on one hand, and the administrative burden stemming from the supervision of compliance on the other hand.	
Recital 12				
22	(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific	(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. ***Sector-specific Union legal acts that require essential or important entities to adopt cybersecurity risk management measures or to report significant incidents, should, where possible, be consistent with the terminology, and refer to the definitions laid down in this Directive.*** Where a	(12) ~~*Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector- specific*~~***This Directive sets out the baseline for cybersecurity risk management measures and reporting obligations across all sectors that fall within its scope. In order to avoid fragmentation of cybersecurity provisions of*** Union legal ~~*act requires essential or*~~	

	provisions, including on supervision and enforcement, should apply. The Commission may issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.	sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents***, and where those requirements are*** ~~*or significant cyber threats*~~ of at least an equivalent effect to the obligations laid down in this Directive, ***and apply to the entirety of the security aspects of the operations and services provided by essential and important entities,*** those sector-specific provisions, including on supervision and enforcement, should apply. The Commission ~~*may*~~***should*** issue ***comprehensive*** guidelines in relation to the implementation of the lex specialis***, taking into account relevant opinions, expertise and best practices of ENISA and the Cooperation Group***. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications ***that duly take into account the need for a comprehensive and consistent cybersecurity framework***. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission	~~*important entities to adopt*~~ ***acts, when additional sector-specific provisions pertaining to*** cybersecurity risk management measures ~~*or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down*~~***and reporting obligations are considered necessary to ensure a high level of cybersecurity, the Commission should assess whether such provisions could be stipulated in an implementing act under the empowerment provided for*** in this Directive~~*, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission may issue guidelines in relation to the implementation*~~***. Should such acts not be suitable for that purpose, sector-specific legislation could contribute to ensuring a high level of cybersecurity, while taking full account of the specificities and complexities*** of the ~~*lex specialis.*~~ ***sectors concerned. The reasoning why an implementing act under the empowerment provided for in*** this Directive ~~*does not preclude the adoption of additional*~~***was not appropriate is to be explained in the sector-specific legislation. At***	

		in a number of sectors, including transport and energy.	***the same time, such*** sector-specific ***provisions of*** Union ***legal acts should duly take into account the need for a comprehensive and harmonised cybersecurity framework*** ~~*acts addressing cybersecurity risk management measures and incident notifications. This Directive*~~ ***This*** is without prejudice to the existing implementing powers that have been conferred ~~*to*~~***on*** the Commission in a number of sectors, including transport and energy.	
Recital 12a				
22a			***(12a) Where a sector–specific Union legal act contains provisions requiring essential or important entities to adopt measures of at least equivalent effect to the obligations laid down in this Directive related to cybersecurity risk management and obligations to notify significant incidents or significant cyber threats , those sector-specific provisions, including on supervision and enforcement, should apply. When determining the equivalent effect of obligations set out in the sector-specific***	

			provisions of a Union legal act, the following aspects should be considered: (i) the cybersecurity risk management measures should consist of appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which the relevant entities use in the provision of their services, and should include as a minimum all the elements laid down in this Directive; (ii) the obligation to notify significant incidents and cyber threats should be at least equivalent to the obligations set out in this Directive as regards the content, format and timelines of the notifications; (iii) the reporting modalities by entities and the relevantauthorities of sector-specific Union legal acts should be at least equivalent to the requirements set out in this Directive as regards their content, format and timelines and should take into account the role of the CSIRTs; (iv) the cross-border cooperation requirements for the relevant authorities should be at least equivalent to those set out in this Directive. If the sector-specific provisions of a Union	

			legal act do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive should continue to apply to the entities not covered by those sector-specific provisions.	
Recital 12aa				
22b			***(12aa) The Commission should periodically review the application of the equivalent effect requirement in relation to sector-specific provisions of Union legal acts may. The Commission is to consult the Cooperation Group when preparing the periodical review.***	
Recital 12aaa				
22c			***(12aaa) Future sector-specific Union legal acts should take due account of the definitions outlined in Article 4 of this Directive and the supervisory and enforcement framework laid down in Chapter VI of this Directive.***	
Recital 12ab				
22d				

			(12ab) Where sector-specific provisions of Union legal acts require essential or important entities to adopt measures of at least equivalent effect to the reporting obligations laid down in this Directive, overlapping reporting obligations should be avoided, and coherence and effectiveness of handling of notifications of cyber threats or incidents should be ensured. For that purpose, those sector-specific provisions can allow Member States to establish a common, automatic and direct reporting mechanism for notifying significant incidents and cyber threats to both the authorities whose tasks are set out in the respective sector-specific provisions and the competent authorities, including the single point of contact and CSIRTs as appropriate, responsible for the cybersecurity tasks provided for in this Directive, or for a mechanism that ensures systematic and immediate sharing of information and cooperation among the relevant authorities and CSIRTs concerning the handling of such notifications. For the purposes of simplifying reporting and of implementing the common,	

			automatic and direct reporting mechanism, Member States may, in accordance with sector-specific legislations, utilise the single-entry point they establish according to Article 11(5a) of this Directive. To ensure harmonisation, reporting obligations of sector-specific Union legal acts should be aligned with those specified under this Directive. Member States can determine that competent authorities under this Directive or national CSIRTs are the addressees of the reporting, in accordance with sector-specific legislations.	
Recital 13				
23	(13) Regulation XXXX/XXXX of the European Parliament and of the Council[1] should be considered to be a sector-specific Union legal act in relation to this Directive with regard to the financial sector entities. The provisions of Regulation XXXX/XXXX relating to information and communications technology (ICT) risk management measures, management of ICT-related incidents and notably incident	(13) Regulation XXXX/XXXX of the European Parliament and of the Council[1] should be considered to be a sector-specific Union legal act in relation to this Directive with regard to the financial sector entities. The provisions of Regulation XXXX/XXXX relating to information and communications technology (ICT) risk management measures, management of ICT-related incidents and notably incident	(13) Regulation XXXX/XXXX of the European Parliament and of the Council~~[1]~~ should be considered to be a sector-specific Union legal act in relation to this Directive with regard to the financial sector entities. The provisions of Regulation XXXX/XXXX relating to information and communications technology (ICT) risk management measures, management of ICT-related incidents and notably incident	

	reporting, as well as on digital operational resilience testing, information sharing arrangements and ICT third party risk should apply instead of those set up under this Directive. Member States should therefore not apply the provisions of this Directive on cybersecurity risk management and reporting obligations, information sharing and supervision and enforcement to any financial entities covered by Regulation XXXX/XXXX. At the same time, it is important to maintain a strong relationship and the exchange of information with the financial sector under this Directive. To that end, Regulation XXXX/XXXX allows all financial supervisors, the European Supervisory Authorities (ESAs) for the financial sector and the national competent authorities under Regulation XXXX/XXXX, to participate in strategic policy discussions and technical workings of the Cooperation Group, and to exchange information and cooperate with the single points of contact designated under this Directive and with the national CSIRTs. The competent authorities under Regulation XXXX/XXXX should transmit details of major ICT-related incidents also to the	reporting, as well as on digital operational resilience testing, information sharing arrangements and ICT third party risk should apply instead of those set up under this Directive. Member States should therefore not apply the provisions of this Directive on cybersecurity risk management and reporting obligations, information sharing and supervision and enforcement to any financial entities covered by Regulation XXXX/XXXX. At the same time, it is important to maintain a strong relationship and the exchange of information with the financial sector under this Directive. To that end, Regulation XXXX/XXXX allows all financial supervisors, the European Supervisory Authorities (ESAs) for the financial sector and the national competent authorities under Regulation XXXX/XXXX, to participate in strategic policy discussions and technical workings of the Cooperation Group, and to exchange information and cooperate with the single points of contact designated under this Directive and with the national CSIRTs. The competent authorities under Regulation XXXX/XXXX should transmit details of major ICT-related incidents also to the	reporting, as well as on digital operational resilience testing, information sharing arrangements and ICT third party risk should apply instead of those set ~~*up under*~~***out in*** this Directive. Member States should therefore not apply the provisions of this Directive on cybersecurity risk management ~~*-*~~***,*** and reporting obligations, ~~*information sharing*~~ and supervision and enforcement to ~~*any*~~ financial entities covered by Regulation XXXX/XXXX. At the same time, it is important to maintain a strong relationship and the exchange of information with the financial sector under this Directive. To that end, Regulation XXXX/XXXX allows ~~*all financial supervisors,*~~ the European Supervisory Authorities (ESAs) for the financial sector and the national competent authorities under Regulation XXXX/XXXX~~*,*~~ to participate in ~~*strategic policy discussions and technical workings*~~***the work*** of the Cooperation Group, and to exchange information and cooperate with the single points of contact designated under this Directive***, as well as*** ~~*and*~~ with the national CSIRTs. The competent authorities under Regulation	

	single points of contact designated under this Directive. Moreover, Member States should continue to include the financial sector in their cybersecurity strategies and national CSIRTs may cover the financial sector in their activities. _____ 1. [insert the full title and OJ publication reference when known]	single points of contact designated under this Directive. Moreover, Member States should continue to include the financial sector in their cybersecurity strategies and national CSIRTs may cover the financial sector in their activities. _____ 1. [insert the full title and OJ publication reference when known]	XXXX/XXXX should transmit details of major ICT-related incidents ***and significant cyber threats*** also to the single points of contact, ***the competent authorities or the national CSIRTs*** designated under this Directive. ***This is achievable by automatic and direct forwarding of incident notifications or a common reporting platform.*** Moreover, Member States should continue to include the financial sector in their cybersecurity strategies and national CSIRTs ~~*may*~~***can*** cover the financial sector in their activities. _____ ~~*1. [insert the full title and OJ publication reference when known]*~~	
Recital 13a				
23a			***(13a) In order to avoid gaps between and duplications of cybersecurity obligations imposed on entities in the aviation sector referred to in point 2 (a) of Annex I, national authorities designated under Regulations (EC) No 300/2008[1] and (EU) 2018/1139[2] of the European Parliament and of the Council and competent authorities under this Directive should cooperate in relation to the***	

			implementation of cybersecurity risk management measures and the supervision of those measures at national level. The compliance of an entity with the cybersecurity risk management measures under this Directive could be considered by the national authorities designated under Regulations (EC) No 300/2008 and (EU) 2018/1139 as compliant with the requirements laid down in those, and the relevant delegated and implementing acts adopted pursuant to those Regulations. _____ ***1. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).*** ***2. Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).***	

Recital 14				
24	(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[1] and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent authority under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on incidents and cyber threats and the exercise of supervisory tasks. Authorities under both Directives should cooperate and exchange information, particularly in relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity measures	(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[1] and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent ~~*authority*~~ ***authorities within and between Member States,*** under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on incidents and cyber threats and the exercise of supervisory tasks. Authorities under both Directives should cooperate and exchange information ***without undue delay***, particularly in relation to the identification of critical entities, cyber threats, cybersecurity risks,	(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council~~[1]~~ and this Directive. To achieve this, Member States should ensure that critical entities, ***[***and equivalent entities***]***, pursuant to Directive (EU) XXX/XXX are considered ~~*to be*~~ ***as*** essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent authority under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on incidents***,*** and cyber threats***,*** and the exercise of supervisory tasks. ***Competent*** authorities under both Directives should cooperate and exchange information, particularly in relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents ***as well as on non-cyber risks, threats and incidents*** affecting critical	

	taken by critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information for this purpose. _____ 1. [insert the full title and OJ publication reference when known]	incidents affecting critical entities as well as on the cybersecurity measures taken by critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information ***where possible in real time,*** for this purpose. _____ 1. [insert the full title and OJ publication reference when known]	entities ~~*as well as on*~~***[or entities equivalent to critical entities], including*** the cybersecurity ***and physical*** measures taken by critical entities ***and the results of supervisory activities carried out with regard to such entities. Furthermore, in order to streamline supervisory activities between the competent authorities designated under both Directives and in order to minimise the administrative burden for the entities concerned, competent authorities should endeavour to harmonise incident notification templates and supervisory processes. Where appropriate,*** ~~*Upon request of*~~ competent authorities under Directive (EU) XXX/XXX~~,~~ ***can request*** competent authorities under this Directive ~~*should be allowed*~~ to exercise their supervisory and enforcement powers ~~*on*~~***in relation to*** an essential entity identified as critical. ~~*Both authorities should cooperate and exchange information for this purpose.*~~ _____ ~~*1. [insert the full title and OJ publication reference when known]*~~	
Recital 14a				

24a			***(14a) Entities belonging to the digital infrastructure sector are in essence based on network and information systems and therefore the obligations imposed on those entities by this Directive should address in a comprehensive manner the physical security of such systems as part of their cybersecurity risk management and reporting obligations. Since those matters are covered by this Directive, the obligations laid down in Chapters III to VI of Directive (EU) XXX/XXX [CER] do not apply to such entities.***	
Recital 15				
25	(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name	(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to ~~*all providers of DNS services along the DNS*~~***top-level-domain (TLD) name servers, publicly available recursive domain name*** resolution ~~*chain,*~~	(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to ~~*all*~~ providers of DNS services along the DNS ***provisioning and*** resolution chain~~,~~ ~~*including operators of root name servers*~~ ***that are of importance for***	

	servers, authoritative name servers for domain names and recursive resolvers.	~~*including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers*~~***services for internet end-users and authoritative domain name resolution services. This Directive does not apply to root name servers***.	***the internal market, including*** , top-level-domain (TLD) name ~~*servers,*~~ ***registries , the entities providing domain name registration services, operators of*** authoritative name servers for domain names and ***operators of*** recursive resolvers. ***The term 'DNS service provider' should not apply to DNS services operated for own purposes of the concerned entity and its affiliated entities. The cybersecurity obligations arising from this Directive for this category of providers are strictly limited to cybersecurity risk-management measures and reporting and, thus they are without prejudice to the governance of the global DNS by the multi-stakeholder community.***	
Recital 16				
26	(16) Cloud computing services should cover services that allow on-demand and broad remote access to a scalable and elastic pool of shareable and distributed computing resources. Those computing resources include resources such as networks, servers or other infrastructure, operating systems, software, storage,	(16) Cloud computing services should cover services that allow on-demand and broad remote access to a scalable and elastic pool of shareable and distributed computing resources. Those computing resources include resources such as networks, servers or other infrastructure, operating systems, software, storage,	(16) Cloud computing services should cover services that allow on-demand and broad remote access to a scalable and elastic pool of shareable and distributed computing resources. Those computing resources include resources such as networks, servers or other infrastructure, operating systems, software, storage,	

	applications and services. The deployment models of cloud computing should include private, community, public and hybrid cloud. The aforementioned service and deployment models have the same meaning as the terms of service and deployment models defined under ISO/IEC 17788:2014 standard. The capability of the cloud computing user to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the cloud computing service provider could be described as on-demand administration. The term 'broad remote access' is used to describe that the cloud capabilities are provided over the network and accessed through mechanisms promoting use of heterogeneous thin or thick client platforms (including mobile phones, tablets, laptops, workstations). The term 'scalable' refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term 'elastic pool' is used to describe those computing resources that are	applications and services. The deployment models of cloud computing should include private, community, public and hybrid cloud. The aforementioned service and deployment models have the same meaning as the terms of service and deployment models defined under ISO/IEC 17788:2014 standard. The capability of the cloud computing user to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the cloud computing service provider could be described as on-demand administration. The term 'broad remote access' is used to describe that the cloud capabilities are provided over the network and accessed through mechanisms promoting use of heterogeneous thin or thick client platforms (including mobile phones, tablets, laptops, workstations). The term 'scalable' refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term 'elastic pool' is used to describe those computing resources that are provisioned and	applications and services. The ***service models of cloud computing include, amongst others, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) and Network as a Service (NaaS). The*** deployment models of cloud computing should include private, community, public and hybrid cloud. The aforementioned service and deployment models have the same meaning as the terms of service and deployment models defined under ISO/IEC 17788:2014 standard. The capability of the cloud computing user to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the cloud computing service provider could be described as on-demand administration. The term 'broad remote access' is used to describe that the cloud capabilities are provided over the network and accessed through mechanisms promoting use of heterogeneous thin or thick client platforms (including mobile phones, tablets, laptops, workstations). The term 'scalable' refers to computing resources that are flexibly allocated by the cloud service provider,	

	provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term 'shareable' is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment. The term 'distributed' is used to describe those computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing.	released according to demand in order to rapidly increase and decrease resources available depending on workload. The term 'shareable' is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment. The term 'distributed' is used to describe those computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing.	irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term 'elastic pool' is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term 'shareable' is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment. The term 'distributed' is used to describe those computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing.	
Recital 17				
G 27	(17) Given the emergence of innovative technologies and new business models, new cloud computing deployment and service models are expected to appear on	(17) Given the emergence of innovative technologies and new business models, new cloud computing deployment and service models are expected to appear on	(17) Given the emergence of innovative technologies and new business models, new cloud computing deployment and service models are expected to appear on	G

		the market in response to evolving customer needs. In that context, cloud computing services may be delivered in a highly distributed form, even closer to where data are being generated or collected, thus moving from the traditional model to a highly distributed one ('edge computing').	the market in response to evolving customer needs. In that context, cloud computing services may be delivered in a highly distributed form, even closer to where data are being generated or collected, thus moving from the traditional model to a highly distributed one ('edge computing').	the market in response to evolving customer needs. In that context, cloud computing services may be delivered in a highly distributed form, even closer to where data are being generated or collected, thus moving from the traditional model to a highly distributed one ('edge computing').		
	Recital 18					
G	28	(18) Services offered by data centre service providers may not always be provided in a form of cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to the security of network and information systems, this Directive should cover also providers of such data centre services that are not cloud computing services. For the purpose of this Directive, the term 'data centre service' should cover provision of a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data	(18) Services offered by data centre service providers may not always be provided in a form of cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to the security of network and information systems, this Directive should cover also providers of such data centre services that are not cloud computing services. For the purpose of this Directive, the term 'data centre service' should cover provision of a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data	(18) Services offered by data centre service providers may not always be provided in a form of cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to the security of network and information systems, this Directive should cover also providers of such data centre services that are not cloud computing services. For the purpose of this Directive, the term 'data centre service' should cover provision of a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data		G

	storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control. The term 'data centre service' does not apply to in-house, corporate data centres owned and operated for own purposes of the concerned entity.	storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control. The term 'data centre service' does not apply to in-house, corporate data centres owned and operated for own purposes of the concerned entity.	storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control. The term 'data centre service' does not apply to in-house, corporate data centres owned and operated for own purposes of the concerned entity.	
Recital 19				
29	(19) Postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council[1], as well as express and courier delivery service providers, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain and in particular clearance, sorting or distribution, including pick-up services. Transport services that are not undertaken in conjunction with one of those steps should fall outside of the scope of postal services. _____ 1. Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service (OJ L	(19) Postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council[1], as well as express and courier delivery service providers, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain and in particular clearance, sorting or distribution, including pick-up services***, while taking into account the degree of their dependence on network and information systems***. Transport services that are not undertaken in conjunction with one of those steps should fall outside of the scope of postal services. _____ 1. Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the	(19) Postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council[1],~~ as well as express and~~ ***including*** courier ~~*delivery*~~ service providers, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain and in particular clearance, sorting or distribution, including pick-up services. Transport services that are not undertaken in conjunction with one of those steps should fall outside of the scope of postal services. _____ 1. Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service (OJ L	

	15, 21.1.1998, p. 14).	development of the internal market of Community postal services and the improvement of quality of service (OJ L 15, 21.1.1998, p. 14).	15, 21.1.1998, p. 14).	
Recital 20				
30	(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting	(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting	(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting	

	negative impacts in the delivery of services across the internal market. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.	negative impacts in the delivery of services across the internal market. The ***intensified attacks against network and information systems during the*** COVID-19 pandemic ~~has~~***have*** shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.	negative impacts in the delivery of services across the internal market. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.	
Recital 20a				
30a			***(20a) For the purpose of achieving and maintaining a high level of cybersecurity, the national cybersecurity strategies required by this Directive should consist of coherent frameworks that provide for a governance in the area ofcybersecurity. These strategies can be composed of one or several documents of legislative or non-legislative nature.***	
Recital 21				
31	(21) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, Member States should be able to designate more than one	(21) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, Member States should be able to designate more than one	(21) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, Member States should be able to designate more than one	

		national competent authority responsible for fulfilling the tasks linked to the security of the network and information systems of essential and important entities under this Directive. Member States should be able to assign this role to an existing authority.	national competent authority responsible for fulfilling the tasks linked to the security of the network and information systems of essential and important entities under this Directive. Member States should be able to assign this role to an existing authority.	national competent authority responsible for fulfilling the tasks linked to the security of the network and information systems of essential and important entities under this Directive. Member States should be able to assign this role to an existing authority.	
	Recital 22				
G	32	(22) In order to facilitate cross-border cooperation and communication among authorities and to enable this Directive to be implemented effectively, it is necessary for each Member State to designate a national single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at Union level.	(22) In order to facilitate cross-border cooperation and communication among authorities and to enable this Directive to be implemented effectively, it is necessary for each Member State to designate a national single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at Union level.	(22) In order to facilitate cross-border cooperation and communication among authorities and to enable this Directive to be implemented effectively, it is necessary for each Member State to designate a national single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at Union level.	G
	Recital 23				
	33	(23) Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way. The single points of contact should be tasked with forwarding incident notifications to the single	(23) Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way. The single points of contact should be tasked with forwarding incident notifications to the single	(23) Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way~~. The single points of contact should be tasked with forwarding incident notifications to the single~~	

	points of contact of other affected Member States. At the level of Member States' authorities, to ensure one single entry point in every Member States, the single points of contacts should also be the addressees of relevant information on incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should be able to forward, as appropriate, to the relevant national competent authorities or CSIRTs under this Directive.	points of contact of other affected Member States. At the level of Member States' authorities, to ensure one single entry point in every Member States, the single points of contacts should also be the addressees of relevant information on incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should be able to forward, as appropriate, to the relevant national competent authorities or CSIRTs under this Directive.	~~*points of contact of other affected Member States. At the level of Member States' authorities, to ensure one single entry point in every Member States,*~~ ***, also with a view to facilitate, where appropriate, a timely response to incidents and to provide a response to the notifying entity.*** The single points of ~~*contacts*~~***contact*** should ~~*also be the addressees of relevant information on incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should be able to forward, as appropriate,*~~ ***be tasked with forwarding incident notifications*** to the ~~*relevant national competent authorities or CSIRTs under this Directive*~~***single points of contact of other affected Member States***.	
Recital 23a				
33a			***(23a) The sector-specific Union legal acts which require cybersecurity risk management measures or reporting obligations of at least equivalent effect with those laid down in this Directive could provide that their designated competent authorities***	

			exercise their supervisory and enforcement powers in relation to such measures or obligations with the assistance of the competent authorities designated in accordance with this Directive. The competent authorities concerned could establish cooperation arrangements for this purpose. Such cooperation arrangements could specify, amongst others, the procedures concerning the coordination of supervisory activities, including the procedures of investigations and on-site inspections in accordance with the national law and a mechanism for the exchange of relevant information between competent authorities on supervision and enforcement, including access to cyber-related information requested by competent authorities designated in accordance with this Directive.	
Recital 24				
34	(24) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents	(24) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents	(24) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents	

	and risks. Member States should therefore ensure that they have well-functioning CSIRTs, also known as computer emergency response teams ('CERTs'), complying with essential requirements in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. In view of enhancing the trust relationship between the entities and the CSIRTs, in cases where a CSIRT is part of the competent authority, Member States should consider functional separation between the operational tasks provided by CSIRTs, notably in relation to information sharing and support to the entities, and the supervisory activities of competent authorities.	and risks. Member States should therefore ~~*ensure that they have well-functioning*~~***designate one or more*** CSIRTs~~*, also known as computer emergency response teams ('CERTs')*~~ ***under this Directive and ensure that they are well-functioning***, complying with essential requirements in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. ***Member States may designate existing computer emergency response teams (CERTs) as CSIRTs***. In view of enhancing the trust relationship between the entities and the CSIRTs, in cases where a CSIRT is part of the competent authority, Member States should consider functional separation between the operational tasks provided by CSIRTs, notably in relation to information sharing and support to the entities, and the supervisory activities of competent authorities.	and risks. Member States should therefore ensure that they have well-functioning CSIRTs, also known as computer emergency response teams ('CERTs'), complying with essential requirements in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. In view of enhancing the trust relationship between the entities and the CSIRTs, in cases where a CSIRT is part of the competent authority, Member States ~~*should*~~ ***may*** consider functional separation between the operational tasks provided by CSIRTs, notably in relation to information sharing and support to the entities, and the supervisory activities of competent authorities.	
Recital 25				
35	(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation	(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation	(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation	

	(EU) 2016/679 of the European Parliament and of the Council[1] as regards personal data, on behalf of and upon request by an entity under this Directive, a proactive scanning of the network and information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs. _____ 1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).	(EU) 2016/679 of the European Parliament and of the Council[1] as regards personal data, on behalf of and upon request by an entity under this Directive, ***or, in the case of a serious threat to national security,*** a proactive scanning of the network and information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs. _____ 1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).	(EU) 2016/679 of the European Parliament and of the Council[1] as regards personal data, on behalf of and upon request by an entity under this Directive, a proactive scanning of the network and information systems used for the provision of their services. ***Where applicable,*** Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs. _____ 1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).	
Recital 25a				
35a		***(25a) CSIRTs should have the ability to, upon an entity's request, continuously discover, manage and monitor all internet-facing assets, both on premises and off premises, to understand their***		

		overall organisational risk to newly discovered supply chain compromises or critical vulnerabilities. The knowledge whether an entity runs a privileged management interface, affects the speed of undertaking mitigating actions.		
Recital 26				
36	(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive.	(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks***, including with CSIRTs from third countries where information exchange is reciprocal and beneficial to the security of citizens and entities,*** in addition to the CSIRTs network established by this Directive***, in order to contribute to the development of Union standards that can shape the cybersecurity landscape at international level. Member States could also explore the possibility of increasing cooperation with like-minded partner countries and international organisations with the aim to secure multilateral agreements on cyber norms, responsible state and non-state***	(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive. ***Therefore, CSIRTs and competent authorities could exchange information, including personal data, with CSIRTs of third countries or their authorities for the purpose of carrying out their tasks in accordance with Regulation (EU) 2016/679. In cases of absence of an adequacy decision adopted in accordance with Article 45 of Regulation (EU) 2016/679 or appropriate safeguards pursuant to Article 46 of that Regulation, the exchange of personal data that is deemed necessary for the purposes of mitigating significant cyber***	

		behaviour in cyberspace and effective global digital governance as well as to create an open, free, stable and secure cyberspace based on international law.	***threats and responding to an ongoing significant incident could be considered to constitute an important reason of public interest within the meaning of Article 49 (1)(d) of Regulation (EU) 2016/679.***	
Recital 26a				
36a		***(26a) Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software and online application security, and business or end-user data on which entities rely upon. Cyber hygiene policies comprising a common baseline set of practices including, but not limited to, software and hardware updates, password changes, management of new installs, limitation of administrator-level access accounts, and backing up of data, enable a proactive framework of preparedness and overall safety and security in the event of incidents or threats. ENISA should monitor and assess Member States' cyber hygiene policies, and explore Union wide schemes to enable cross-border***		

		checks ensuring equivalence independent of Member State requirements.		
Recital 26b				
36b		***(26b) The use of artificial intelligence (AI) in cybersecurity has the potential of improving the detection and to stop attacks against network and information systems, enabling resources to be diverted towards more sophisticated attacks. Member States should therefore encourage in their national strategies the use of (semi-)automated tools in cybersecurity and the sharing of data needed to train and improve automated tools in cybersecurity. In order to mitigate risks of unduly interference with the rights and freedoms of individuals that AI-enabled systems might pose, the requirements of data protection by design and by default laid down in Article 25 of Regulation (EU) 2016/679 shall apply. Integrating appropriate safeguards such as pseudonymisation, encryption, data accuracy and data minimisation could furthermore mitigate such risks.***		***(26a) The use of artificial intelligence (AI) in cybersecurity has the potential of improving the detection of and to prevent attacks against network and information systems, enabling resources to be diverted towards more sophisticated attacks. Member States should therefore encourage in their national strategies research in and the development and use of (semi-) automated tools in cybersecurity and the sharing of data needed to train and improve automated tools in cybersecurity. In order to mitigate risks of unduly interference with the rights and freedoms of individuals that AI-enabled systems might pose, the requirements of data protection by design and by default laid down in Regulation (EU) 2016/679 are to apply. Integrating appropriate safeguard such as anonymization, encryption, data accuracy and data minimisation, could furthermore mitigate such risks.***

				EP proposal
Recital 26c				
36c		***(26c) Open-source cybersecurity tools and applications can contribute to a higher degree of transparency and can have a positive impact on the efficiency of industrial innovation. Open standards facilitate interoperability between security tools, benefitting the security of industrial stakeholders. Open-source cybersecurity tools and applications can leverage the wider developer community, enabling entities to pursue vendor diversification and open security strategies. Open security can lead to a more transparent verification process of cybersecurity related tools and a community-driven process of discovering vulnerabilities. Member States should therefore promote the adoption of open-source software and open standards by pursuing policies relating to the use of open data and open-source as part of security through transparency. Policies promoting the adoption and sustainable use of open-***		***(26b) Open-source cybersecurity tools and applications can contribute to a higher degree of openness and can have a positive impact on the efficiency of industrial innovation. Open standards facilitate interoperability between security tools, benefitting the security of industrial stakeholders. Open-source cybersecurity tools and applications can leverage the wider developer community, enabling diversification of suppliers. Open source can lead to a more transparent verification process of cybersecurity related tools and a community-driven process of discovering vulnerabilities. Member States should therefore be able to promote the adoption of open-source software and open standards by pursuing policies relating to the use of open data and open-source as part of security through transparency. Policies promoting the adoption and sustainable use of open-***

			source cybersecurity tools are of particular importance for small and medium-sized enterprises (SMEs) facing significant costs for implementation, which could be minimised by reducing the need for specific applications or tools.		***source cybersecurity tools are of particular importance for small and medium-sized enterprises (SMEs) facing significant costs for implementation, which could be minimised by reducing the need for specific applications or tools.***
Recital 26d					
G	36d		***(26d) Public-Private Partnerships (PPPs) in the field of cybersecurity can provide the right framework for knowledge exchange, sharing of best practices and the establishment of a common level of understanding among all stakeholders. Member States should adopt policies underpinning the establishment of cybersecurity-specific PPPs as part of their national cybersecurity strategies. Those policies should clarify, inter alia, the scope and stakeholders involved, the governance model, the available funding options and the interaction among participating stakeholders. PPPs can leverage the expertise of private sector entities to support Member States' competent authorities in developing state-of-***		***(26d) Public-Private Partnerships (PPPs) in the field of cybersecurity can provide the right framework for knowledge exchange, sharing of best practices and the establishment of a common level of understanding among all stakeholders. Member States should promote policies underpinning the establishment of cybersecurity-specific PPPs. Those policies should clarify, inter alia, the scope and stakeholders involved, the governance model, the available funding options and the interaction among participating stakeholders. PPPs can leverage the expertise of private sector entities to support Member States' competent authorities in developing state-of-the art services and processes including,***	G

		the art services and processes including, but not limited to, information exchange, early warnings, cyber threat and incident exercises, crisis management, and resilience planning.		***but not limited to, information exchange, early warnings, cyber threat and incident exercises, crisis management, and resilience planning.*** Text Origin: EP Mandate
Recital 27				
37	(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[1], a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response	(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[1], a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market ***or posing serious public security and safety risks for entities or citizens in several Member States or the Union as a whole***. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions,	(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[1], a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response	

	across the Union. _____ 1. Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).	bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union. _____ 1. Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).	across the Union. _____ 1. Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).	
Recital 27a				
G 37a		***(27a) Member States should, in their national cybersecurity strategies, address specific cybersecurity needs of SMEs. SMEs represent, in the Union context, a large percentage of the industrial and business market and they are often struggling to adapt to new business practices in a more connected world, navigating the digital environment, with employees working from home and business increasingly being conducted online. Some SMEs face specific cybersecurity challenges such as low cyber-awareness, a lack of remote IT security, the high cost of cybersecurity solutions and an increased level of threat, such as ransomware, for which they***		***(27a) Member States should, in their national cybersecurity strategies, address the specific cybersecurity needs of SMEs. SMEs represent, in the Union context, a large percentage of the industrial and business market and they often struggle to adapt to new business practices in a more connected world, navigating the digital environment, with employees working from home and business increasingly being conducted online. Some SMEs face specific cybersecurity challenges such as low cyber-awareness, a lack of remote IT security, the high cost of cybersecurity solutions and an increased level of threat, such as ransomware, for which they*** G

		should receive guidance and support. Member States should have a cybersecurity single point of contact for SMEs, which either provides guidance and support to SMEs or directs them to the appropriate bodies for guidance and support on cybersecurity related issues. Member States are encouraged to also offer services such as website configuration and logging enabling to small enterprises and microenterprises that lack those capabilities.		***should receive guidance and support. SMEs are increasingly becoming the target of supply chain attacks due to their less rigorous cybersecurity measures and attack management, and availability of dedicated security resources. Such supply chain attacks do not only impact SMEs and their operations in isolation but can also have a cascading effect for larger attacks on entities that they supply to. Member States should, through their national cybersecurity strategies, help SME's to address the challenges faced in their supply chains. Member States should have a point of contact for SMEs at national or regional level, which either provides guidance and support to SMEs or directs them to the appropriate bodies for guidance and support on cybersecurity related issues. Member States are also encouraged to offer services such as website configuration and logging enabling to small enterprises and microenterprises that lack those capabilities.*** EP proposal
Recital 27b				

Y	37b		***(27b) Member States should adopt policies on the promotion of active cyber defence as part of their national cybersecurity strategies. Active cyber defence is the proactive prevention, detection, monitoring, analysis and mitigation of network security breaches, combined with the use of capabilities deployed within and outside the victim network. The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enabling a unity of effort in successfully detecting, preventing and addressing attacks against network and information systems. Active cyber defence is based on a defensive strategy that excludes offensive measures against critical civilian infrastructure.***		***(27b) As part of their national cybersecurity strategies, Member States should adopt policies on the promotion of active cyber protection as part of a wider defensive strategy. Rather than responding reactively, active cyber protection is the prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner, combined with the use of capabilities deployed within and outside the victim network. This could include Member States offering free services or tools to eligible entities, including self-service checks, detection tools and takedown services. The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enable a unity of effort in successfully detecting, preventing, addressing and blocking attacks against network and information systems. Active cyber protection is based on a defensive strategy that excludes offensive measures.***	Y
Recital 28					

38	(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying those vulnerabilities is an important factor in reducing cybersecurity risk. Entities that develop such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and reported (disclosed) by third parties (reporting entities), the manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third parties. In this regard, international standards ISO/IEC 30111 and ISO/IEC 29417 provide guidance on vulnerability handling and vulnerability disclosure respectively. As regards vulnerability disclosure, coordination between reporting entities and manufacturers or providers of ICT products or services is particularly important. Coordinated vulnerability disclosure specifies a structured	(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying those vulnerabilities is an important factor in reducing cybersecurity risk. Entities that develop such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and reported (disclosed) by third parties (reporting entities), the manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third parties. In this regard, international standards ISO/IEC 30111 and ISO/IEC 29417 provide guidance on vulnerability handling and vulnerability disclosure respectively. ~~*As regards vulnerability disclosure,*~~ ***Strengthening the*** coordination between reporting entities and manufacturers or providers of ICT products or services is particularly important ***to facilitate the voluntary framework***	(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying those vulnerabilities is an important factor in reducing cybersecurity risk. Entities that develop ***or administer*** such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and reported (disclosed) by third parties (reporting entities), the manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third parties. In this regard, international standards ISO/IEC 30111 and ISO/IEC ~~*29417*~~***29147*** provide guidance on vulnerability handling and vulnerability disclosure respectively. As regards vulnerability disclosure, coordination between reporting entities and manufacturers or providers of ICT products or services is particularly important. Coordinated vulnerability disclosure specifies a structured	

	process through which vulnerabilities are reported to organisations in a manner allowing the organisation to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also comprise coordination between the reporting entity and the organisation as regards the timing of remediation and publication of vulnerabilities.	***of vulnerability disclosure***. Coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to organisations in a manner allowing the organisation to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also comprise coordination between the reporting entity and the organisation as regards the timing of remediation and publication of vulnerabilities.	process through which vulnerabilities are reported to organisations in a manner allowing the organisation to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also comprise coordination between the reporting entity and the organisation as regards the timing of remediation and publication of vulnerabilities.	
Recital 28a				
38a		***(28a) The Commission, ENISA and the Member States should continue to foster international alignment with standards and existing industry best practices in the area of risk management, for example in the areas of supply chain security assessments, information sharing and vulnerability disclosure.***		
Recital 29				
39				

	(29) Member States should therefore take measures to facilitate coordinated vulnerability disclosure by establishing a relevant national policy. In this regard, Member States should designate a CSIRT to take the role of 'coordinator', acting as an intermediary between the reporting entities and the manufacturers or providers of ICT products or services where necessary. The tasks of the CSIRT coordinator should in particular include identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure timelines, and managing vulnerabilities that affect multiple organisations (multi-party vulnerability disclosure). Where vulnerabilities affect multiple manufacturers or providers of ICT products or services established in more than one Member State, the designated CSIRTs from each of the affected Member States should cooperate within the CSIRTs Network.	(29) Member States***, in cooperation with ENISA,*** should therefore take measures to facilitate coordinated vulnerability disclosure by establishing a relevant national policy. In ~~*this regard*~~***that national policy***, Member States should ~~*designate a CSIRT to take the role of 'coordinator', acting as an intermediary between the reporting*~~***address problems encountered by vulnerability researchers.*** Entities and ~~*the manufacturers or providers of ICT products or services where necessary. The tasks of the CSIRT coordinator should in particular include identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure timelines, and managing vulnerabilities that affect multiple organisations (multi-party vulnerability disclosure). Where vulnerabilities affect multiple manufacturers or providers of ICT products or services established in more than one Member State, the designated CSIRTs from each of the affected Member States should cooperate within the CSIRTs Network*~~***natural persons researching vulnerabilities may in some Member States be exposed***	(29) Member States should therefore take measures to facilitate coordinated vulnerability disclosure by establishing a relevant national policy. ~~*In this regard*~~***As part of their national policy***, Member States should ***aim to address, to the extent possible, the challenges faced by vulnerability researchers, including their potential exposure to criminal liability, in accordance with their national legal order. Member States should*** designate a CSIRT to take the role of 'coordinator', acting as an intermediary between the reporting entities and the manufacturers or providers of ICT products or services where necessary. The tasks of the CSIRT coordinator should in particular include identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure timelines, and managing vulnerabilities that affect multiple organisations (multi-party ***coordinated*** vulnerability disclosure). Where ~~*vulnerabilities affect multiple manufacturers or providers of ICT products or services established*~~***the reported vulnerability could potentially have significant impact on entities***	

		to criminal and civil liability. Member States are therefore encouraged to issue guidelines as regards the non-prosecution of information security research and an exemption from civil liability for those activities.	in more than one Member State, the designated CSIRTs ~~*from each of the affected Member States*~~ should cooperate within the CSIRTs Network***, where appropriate***.	
Recital 29a				
39a		***(29a) Member States should designate a CSIRT to take the role of 'coordinator', acting as an intermediary between the reporting entities and the manufacturers or providers of ICT products or services, which are likely to be affected by the vulnerability, where necessary. The tasks of the CSIRT coordinator should in particular include identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure timelines, and managing vulnerabilities that affect multiple organisations (multi-party vulnerability disclosure). Where vulnerabilities affect multiple manufacturers or providers of ICT products or services established in more than one Member State, the designated CSIRTs from each of the affected***		

		Member States should cooperate within the CSIRTs Network.		
Recital 30				
40	(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an enhanced cybersecurity risk management. In that regard, sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability registry where, essential and important entities and their suppliers, as well as entities which do not fall in the scope of application of this Directive may, on a voluntary basis, disclose vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures.	(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an enhanced cybersecurity risk management. ~~*In that regard,*~~ Sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also ***for*** national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability ~~*registry*~~***database*** where, essential and important entities and their suppliers, as well as entities which do not fall ~~*in*~~***within*** the scope of application of this Directive may, on a voluntary basis, disclose vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures. ***The aim of that database is to address the unique challenges posed by cybersecurity risks to European entities. Furthermore, ENISA should establish a responsible procedure regarding the***	(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an enhanced cybersecurity risk management. In that regard, sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability registry where, essential and important entities and their suppliers, as well as entities which do not fall in the scope of application of this Directive ***or designated CSIRTs*** may, on a voluntary basis, disclose vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures.	

		publication process, in order to give entities the time to take mitigating measures as regards their vulnerabilities, and employ state of the art cybersecurity measures, as well as machine-readable datasets and corresponding interfaces (API). To encourage a culture of disclosure of vulnerabilities a disclosure should be without detriment of the reporting entity.		
Recital 31				
41	(31) Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A European vulnerability registry maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is officially disclosed, and resilience in cases of disruptions or interruptions on the provision of similar services. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements	(31) ~~*Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A*~~ ***The*** European vulnerability ~~*registry*~~***database*** maintained by ENISA ~~*would provide improved transparency regarding the publication process before the vulnerability is officially disclosed, and resilience in cases of disruptions or interruptions on the provision of similar services. To avoid duplication of efforts and seek complementarity to the extent possible*~~***should leverage the Common Vulnerabilities and Exposures (CVE) registry,***	(31) Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A European vulnerability registry maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is officially disclosed, and resilience in cases of disruptions or interruptions on the provision of similar services. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements with similar registries in third	

	with similar registries in third country jurisdictions.	***through the use of its framework for identification, tracking and scoring of vulnerabilities. Furthermore***, ENISA should explore the possibility ~~*of entering*~~***to enter*** into structured cooperation agreements with ***other*** similar registries ~~*in*~~***or databases under the*** third country jurisdictions***, to avoid duplications of efforts and to seek complementarity***.	country jurisdictions. ***In particular, ENISA should explore the possibility of a close cooperation with the operators of the Common Vulnerabilities and Exposures (CVE) system, including the possibility to become a root CVE numbering authority.***	
Recital 32				
42	(32) The Cooperation Group should establish a work programme every two years including the actions to be undertaken by the Group to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive should be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148 in order to avoid potential disruptions in the work of the Group.	(32) The Cooperation Group should establish a work programme every two years including the actions to be undertaken by the Group to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive should be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148 in order to avoid potential disruptions in the work of the Group.	(32) ***The Cooperation Group should continue to support and facilitate strategic cooperation and the exchange of information, as well as to strengthen trust and confidence among Member States.*** The Cooperation Group should establish a work programme every two years including the actions to be undertaken by the Group to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive should be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148 in order to avoid potential disruptions in the work of the Group.	

Recital 33				
43	(33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations to be addressed through better implementation of existing rules.	(33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations***, in particular as regards facilitating the alignment in the transposition of this Directive among Member States,*** to be addressed through better implementation of existing rules. ***The Cooperation Group should also map the national solutions in order to promote compatibility of cybersecurity solutions applied to each specific sector across the Union. This is particularly relevant for the sectors that have an international and cross-border nature.***	(33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations to be addressed through better implementation of existing rules.	
Recital 34				
44	(34) The Cooperation Group should remain a flexible forum and be able to react to changing and	(34) The Cooperation Group should remain a flexible forum and be able to react to changing and	(34) The Cooperation Group should remain a flexible forum and be able to react to changing and	

	new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should consider inviting Union bodies and agencies involved in cybersecurity policy, such as the European Cybercrime Centre (EC3), the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work.	new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should consider inviting ***relevant*** Union bodies and agencies involved in cybersecurity policy, such as ~~*the European Cybercrime Centre (EC3)*~~***Europol***, the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work.	new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should consider inviting Union bodies and agencies involved in cybersecurity policy, such as the European Cybercrime Centre (EC3), the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work.	
Recital 35				
45	(35) The competent authorities and CSIRTs should be empowered to participate in exchange schemes for officials from other Member States in order to improve cooperation. The competent authorities should take the necessary measures to enable officials from other Member States to play an effective role in the	(35) The competent authorities and CSIRTs should be empowered to participate in exchange schemes for officials from other Member States***, within structured rules and mechanisms underpinning the scope and, where applicable, the required security clearance of officials participating in such exchange schemes,*** in order to	(35) The competent authorities and CSIRTs should be empowered to participate in exchange schemes for officials from other Member States in order to improve cooperation. The competent authorities should take the necessary measures to enable officials from other Member States to play an effective role in the	

	activities of the host competent authority.	improve cooperation ***and strengthen trust among Member States***. The competent authorities should take the necessary measures to enable officials from other Member States to play an effective role in the activities of the host competent authority ***or CSIRT***.	activities of the host competent authority.	
Recital 35a				
45a			***(35a) The CSIRTs network should continue to contribute to strengthening confidence and trust and to promote swift and effective operational cooperation among Member States. In order to enhance operational cooperation at Union level, the CSIRTs network should consider inviting Union bodies and agencies involved in cybersecurity policy, such as Europol to participate in its work.***	
Recital 36				
46	(36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and	(36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and	~~*(36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations,*~~	

	organising their participation in some activities of the Cooperation Group and the CSIRTs network. Such agreements should ensure adequate protection of data.	organising their participation in some activities of the Cooperation Group and the CSIRTs network. Such agreements should ensure ***Union's interests and*** adequate protection of data. ***This shall not preclude the right of Member States to cooperate with likeminded third countries on management of vulnerabilities and cyber security risk management, facilitating reporting and general information sharing in accordance with Union law.***	~~*allowing and organising their participation in some activities of the Cooperation Group and the CSIRTs network. Such agreements should ensure adequate protection of data.*~~	
Recital 36a				
46a			***(36a) In order to facilitate the effective implementation of provisions of this Directive such as the management of vulnerabilities, cybersecurity risk management, reporting measures and information sharing arrangements, Member States may cooperate with third countries and undertake activities that are deemed appropriate for that purpose, including information exchanges on threats, incidents, vulnerabilities, tools and methods, tactics, techniques and procedures, cyber crisis***	

			management preparedness and exercises, training, trust building and structured information sharing arrangements. Such cooperation agreements should comply with Union law on data protection.	
Recital 37				
47	(37) Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework set out in Recommendation (EU) 2017/1584 through the existing cooperation networks, notably the Cyber Crisis Liaison Organisation Network (EU-CyCLONe), CSIRTs network and the Cooperation Group. EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements defining the modalities of that cooperation. The EU-CyCLONe's rules of procedures should further specify the modalities through which the network should function, including but not limited to roles, cooperation modes, interactions with other relevant actors and templates for information sharing, as well as means of communication. For crisis	(37) Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework set out in Recommendation (EU) 2017/1584 through the existing cooperation networks, notably the Cyber Crisis Liaison Organisation Network (EU-CyCLONe), CSIRTs network and the Cooperation Group. EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements defining the modalities of that cooperation. The EU-CyCLONe's rules of procedures should further specify the modalities through which the network should function, including but not limited to roles, cooperation modes, interactions with other relevant actors and templates for information sharing, as well as means of communication. For crisis	(37) Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework set out in Recommendation (EU) 2017/1584 through the existing cooperation networks, notably the ***European*** Cyber Crisis Liaison Organisation Network (EU-CyCLONe), CSIRTs network and the Cooperation Group. EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements defining the modalities of that cooperation ***and avoid any duplication of tasks***. The EU-CyCLONe's rules of procedures should further specify the modalities through which the network should function, including but not limited to roles, cooperation modes, interactions with other relevant actors and templates for information sharing,	

	management at Union level, relevant parties should rely on the Integrated Political Crisis Response (IPCR) arrangements. The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for this purpose. If the crisis entails an important external or Common Security and Defence Policy (CSDP) dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) should be activated.	management at Union level, relevant parties should rely on the Integrated Political Crisis Response (IPCR) arrangements. The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for this purpose. If the crisis entails an important external or Common Security and Defence Policy (CSDP) dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) should be activated.	as well as means of communication. For crisis management at ***political*** Union level, relevant parties should rely on the Integrated Political Crisis Response (IPCR) arrangements. The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for this purpose. If the crisis entails an important external or Common Security and Defence Policy (CSDP) dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) should be activated.	
Recital 37a				
47a			***(37a) EU-CyCLONe should work as an intermediary network between the technical and political level during large scale cybersecurity incidents and crises. It should enhance cooperation at operational level, building on CSIRTs network findings and using own capabilities to create impact analysis of the large-scale incidents and crises and supporting decision–making at political level. A competent authority responsible for the management of large-scale***	

			security incidents and crises should be designated by the EU institutions, bodies and agencies to become a member of EU-CyCLONe.	
Recital 38				
48	(38) For the purposes of this Directive, the term 'risk' should refer to the potential for loss or disruption caused by a cybersecurity incident and should be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of said incident.	~~*(38) For the purposes of this Directive, the term 'risk' should refer to the potential for loss or disruption caused by a cybersecurity incident and should be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of said incident.*~~	~~*(38) For the purposes of this Directive, the term 'risk' should refer to the potential for loss or disruption caused by a cybersecurity incident and should be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of said incident.*~~	
Recital 39				
49	(39) For the purposes of this Directive, the term 'near misses' should refer to an event which could potentially have caused harm, but was successfully prevented from fully transpiring.	~~*(39) For the purposes of this Directive, the term 'near misses' should refer to an event which could potentially have caused harm, but was successfully prevented from fully transpiring.*~~	~~*(39) For the purposes of this Directive, the term 'near misses' should refer to an event which could potentially have caused harm, but was successfully prevented from fully transpiring.*~~	
Recital 39a				
49a			***(39a) Responsibilities in ensuring the security of network and information system lie, to a great***	

			extent, with essential and important entities. A culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed.	
Recital 40				
50	(40) Risk-management measures should include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact. The security of network and information systems should comprise the security of stored, transmitted and processed data.	(40) Risk-management measures should include measures to identify any risks of incidents, to prevent, detect, ***respond to and recover from*** ~~*and handle*~~ incidents and to mitigate their impact. The security of network and information systems should comprise the security of stored, transmitted and processed data. ***Those systems should provide for systemic analysis, breaking down the various processes and the interactions between subsystems and taking into account the human factor, in order to have a complete picture of the security of the information system.***	(40) Risk-management measures should ***take into account the degree of dependence of the entity on network and information systems and*** include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact. The security of network and information systems should comprise the security of stored, transmitted and processed data.	
Recital 40a				
50a			***(40a) As threats to the security of***	

			network and information systems can have different origins, this Directive applies an "all-hazard" approach that includes the protection of network and information systems and their physical environment from any event such as theft, fire, flood, telecommunications or power failures or from any unauthorised physical access and damage to and interference with the entity's information and information processing facilities that could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. The risk management measures should therefore also address the physical and environmental security by including measures to protect the entity's network and information systems from system failures, human error, malicious actions or natural phenomena in line with European or internationally recognised standards, such as those included in the ISO 27000 series. In this regard, entities should, as part of their risk management measures, also	

			address human resources security and have in place appropriate access control policies. Those measures should be coherent with Directive XXXX [CER Directive].	
Recital 40b				
50b			***(40b) In the absence of appropriate European cybersecurity certification schemes adopted in accordance with Regulation (EU) 2019/881, Member States could require entities to use certified ICT products, services and processes or obtain a certificate under available national cybersecurity schemes for the purpose of complying with the cybersecurity risk management requirements under this Directive.***	
Recital 41				
51	(41) In order to avoid imposing a disproportionate financial and administrative burden on essential and important entities, the cybersecurity risk management requirements should be proportionate to the risk presented by the network and information	(41) In order to avoid imposing a disproportionate financial and administrative burden on essential and important entities, the cybersecurity risk management requirements should be proportionate to the risk presented by the network and information	(41) In order to avoid imposing a disproportionate financial and administrative burden on essential and important entities, the cybersecurity risk management requirements should be proportionate to the risk presented ~~by~~***to*** the network and information	

	system concerned, taking into account the state of the art of such measures.	system concerned, taking into account the state of the art of such measures ***and European or international standards, such as ISO31000 and ISA/IEC 27005***.	system concerned, taking into account the state of the art of such measures ***and the cost for their implementation. Due account should also be taken of the size of the entity, as well as the likelihood of occurrence of incidents and their severity***.	
Recital 41a				
51a			***(41a) With a view to easing regulatory burdens, the requirements for the implementation of cybersecurity risk management measures for medium, small or micro-sized entities, should in principle be lighter, unless criticality criteria or national risk assessments would justify stricter requirements, in particular with regard to entities that meet the criticality-related criteria set out in this Directive.***	
Recital 42				
G 52	(42) Essential and important entities should ensure the security of the network and information systems which they use in their activities. Those are primarily	(42) Essential and important entities should ensure the security of the network and information systems which they use in their activities. Those are primarily	(42) Essential and important entities should ensure the security of the network and information systems which they use in their activities. Those are primarily	G

	private network and information systems managed by their internal IT staff or the security of which has been outsourced. The cybersecurity risk management and reporting requirements pursuant to this Directive should apply to the relevant essential and important entities regardless of whether they perform the maintenance of their network and information systems internally or outsource it.	private network and information systems managed by their internal IT staff or the security of which has been outsourced. The cybersecurity risk management and reporting requirements pursuant to this Directive should apply to the relevant essential and important entities regardless of whether they perform the maintenance of their network and information systems internally or outsource it.	private network and information systems managed by their internal IT staff or the security of which has been outsourced. The cybersecurity risk management and reporting requirements pursuant to this Directive should apply to the relevant essential and important entities regardless of whether they perform the maintenance of their network and information systems internally or outsource it.	
Recital 42aa				
52a			***(42aa) Taking account of their cross-border nature, the DNS service providers, TLD name registries and entities providing domain name registration services for the TLD, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, and managed security service providers should be subject to a higher degree of harmonisation at Union level. The implementation of cyber security measures should therefore be facilitated by an implementing act.***	
Recital 43				

53	(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers***, such as providers of data storage and processing services or managed security services,*** is particularly important given the prevalence of incidents where entities have fallen victim to ~~*cyber-attacks*~~***attacks against network and information systems*** and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality ***and resilience*** of products and ***services, the cybersecurity measures embedded in them, and the*** cybersecurity practices of their suppliers and service providers, including their secure development procedures. ***Entities should in particular be encouraged to incorporate cybersecurity measures into contractual arrangements with their first-level suppliers and service providers. Entities could consider cybersecurity risks stemming from other levels of suppliers and***	(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	

		service providers.		
Recital 44				
54	(44) Among service providers, managed security services providers (MSSPs) in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to detect and respond to incidents. Those MSSPs have however also been the targets of cyberattacks themselves and through their close integration in the operations of operators pose a particular cybersecurity risk. Entities should therefore exercise increased diligence in selecting an MSSP.	(44) Among service providers, managed security services providers (MSSPs) in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to ~~*detect and*~~***prevent, detect,*** respond to ***or recover from*** incidents. Those MSSPs have however also been the targets of cyberattacks themselves and through their close integration in the operations of operators pose a particular cybersecurity risk. Entities should therefore exercise increased diligence in selecting an MSSP.	(44) Among service providers, managed security services providers (MSSPs) in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to detect and respond to incidents. Those MSSPs have however also been the targets of cyberattacks themselves and through their close integration in the operations of operators pose a particular cybersecurity risk. Entities should therefore exercise increased diligence in selecting an MSSP.	
Recital 44a				
54a			***(44a) National competent authorities, in the context of their supervisory tasks, may also benefit from cybersecurity services such as security audits and penetration testing or incident response. To assist entities, as well as national***	

			competent authorities, in selecting skilled and trustworthy cybersecurity service providers, the Commission, with the assistance of the Cooperation Group and ENISA, should consider the possibility to request European cybersecurity certification schemes in accordance with Article 48 of Regulation (EU) 2019/881.	
Recital 45				
55	(45) Entities should also address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem. In particular, entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data for the activities of the entities, when relying on data transformation and data analytics services from third	(45) Entities should also address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem***, including to counter industrial espionage and to protect trade secrets***. In particular, entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data for the activities of the entities, when	(45) Entities should also address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem. In particular, entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data for the activities of the entities, when relying on data transformation and data analytics services from third	

	parties, the entities should take all appropriate cybersecurity measures.	relying on data transformation and data analytics services from third parties, the entities should take all appropriate cybersecurity measures.	parties, the entities should take all appropriate cybersecurity measures.	
Recital 45a				
55a		***(45a) Entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust architecture, software updates, device configuration, network segmentation, identity and access management or user awareness, and organise training for their staff regarding corporate email cyber threats, phishing or social engineering techniques. Furthermore, entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies driven by artificial intelligence or machine learning systems to automate their capabilities and the protection of network architectures.***		
Recital 46				
56	(46) To further address key supply	(46) To further address key supply	(46) To further address key supply	

	chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[1], with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities. _____ 1. Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).	chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated ~~*sectoral*~~ supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[1], with the aim of identifying per sector which are the critical ICT ***and ICS*** services, systems or products, relevant threats and vulnerabilities. ***Such risk assessments should identify measures, mitigation plans and best practices against critical dependencies, potential single points of failure, threats, vulnerabilities and other risks associated with the supply chain and should explore ways to further encourage their wider adoption by entities. Potential non-technical risk factors, such as undue influence by a third country on suppliers and service providers, in particular in the case of alternative models of governance, include concealed***	chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[1], with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities. _____ 1. Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).	

		vulnerabilities or backdoors and potential systemic supply disruptions, in particular in case of technological lock-in or provider dependency. ——— 1. Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).		
Recital 47				
57	(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT	(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT	(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT	

	services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities.	services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products ***throughout their entire lifecycle*** against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities. ***Furthermore, particular emphasis should be placed on ICT services, systems or products that are subject to specific requirements stemming from third countries.***	services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities.	
Recital 47a				
57a		***(47a) The Stakeholder Cybersecurity Certification Group established pursuant to Article 22 of Regulation (EU) 2019/881 of the European Parliament and of the Council[1] should issue an opinion on security risk assessments of specific critical ICT and ICS services, systems or products supply chains. The Cooperation Group and ENISA should take into account that***		

		opinion. ***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 L 151, 7.6.2019, p.15).***		
Recital 48				
58	(48) In order to streamline the legal obligations imposed on providers of public electronic communications networks or publicly available electronic communications services, and trust service providers related to the security of their network and information systems, as well as to enable those entities and their respective competent authorities to benefit from the legal framework established by this Directive (including designation of CSIRT responsible for risk and incident handling, participation of competent authorities and bodies in the work of the Cooperation Group and the CSIRT network), they should be included in the scope of application of this	(48) In order to streamline the legal obligations imposed on providers of public electronic communications networks or publicly available electronic communications services, and trust service providers related to the security of their network and information systems, as well as to enable those entities and their respective competent authorities to benefit from the legal framework established by this Directive (including designation of CSIRT responsible for risk and incident handling, participation of competent authorities and bodies in the work of the Cooperation Group and the CSIRT network), they should be included in the scope of application of this Directive. The	(48) In order to streamline the legal obligations imposed on providers of public electronic communications networks or publicly available electronic communications services, and trust service providers related to the security of their network and information systems, as well as to enable those entities and their respective competent authorities to benefit from the legal framework established by this Directive (including designation of CSIRT responsible for risk and incident handling, participation of competent authorities and bodies in the work of the Cooperation Group and the CSIRT network), they should be included in the scope of application of this Directive. The	

	Directive. The corresponding provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council[1] and Directive (EU) 2018/1972 of the European Parliament and of the Council[2] related to the imposition of security and notification requirement on these types of entities should therefore be repealed. The rules on reporting obligations should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council[3]. __________ 1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73). 2. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36). 3. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).	corresponding provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council[1] and Directive (EU) 2018/1972 of the European Parliament and of the Council[2] related to the imposition of security and notification requirement on these types of entities should therefore be repealed. The rules on reporting obligations should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council[3]. __________ 1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73). 2. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36). 3. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).	corresponding provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council[1] and Directive (EU) 2018/1972 of the European Parliament and of the Council[2] related to the imposition of security and notification requirement on these types of entities should therefore be repealed. The rules on reporting obligations should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council[3]. __________ 1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73). 2. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36). 3. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).	

Recital 48a				
58a			***(48a) The security obligations laid down in this Directive should be considered complementary to the requirements imposed on trust service providers under Regulation (EU) No 910/2014 (eIDAS Regulation). Trust-service providers should be requested to take all appropriate and proportionate measures to manage the risks posed to their services, including in relation to customers and relying third parties, and to report security incidents under this Directive. Such security and reporting obligations should also concern the physical protection of the service provided. Article 24 of Regulation (EU) 910/2014 continues to apply.***	
Recital 48aa				
58b			***(48aa) Member States may assign the role of competent authorities for trust services to the eIDAS supervisory bodies in order to ensure the continuation of current practices and to build on the knowledge and experience gained in the application of the***	

			eIDAS Regulation. Where that role is assigned to a different body, the national competent authorities under this Directive should cooperate closely, in a timely manner, by exchanging the relevant information in order to ensure effective supervision and compliance of trust service providers with the requirements set out in this Directive and Regulation [XXXX/XXXX]. Where applicable, the national competent authority under this Directive should immediately inform the eIDAS supervisory body about any notified significant cyber threat or incident with impact on trust services as well as about any non-compliance of a trust service provider with the requirements under this Directive. For the purposes of reporting, Member States may use, where applicable, the single-entry point established to achieve a common and automatic incident reporting to both the eIDAS supervisory body and the competent authority under this Directive. The rules on reporting obligations should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European	

			Parliament and of the Council[1]. ***1. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).***	
Recital 49				
59	(49) Where appropriate and to avoid unnecessary disruption, existing national guidelines and national legislation adopted for the transposition of the rules related to security measures laid down in Article 40(1) of Directive (EU) 2018/1972, as well as of the requirements of Article 40(2) of that Directive concerning the parameters related to the significance of an incident, should continue to be used by the competent authorities in charge of supervision and enforcement for the purposes of this Directive.	(49) Where appropriate and to avoid unnecessary disruption, existing national guidelines and national legislation adopted for the transposition of the rules related to security measures laid down in Article 40(1) of Directive (EU) 2018/1972, as well as of the requirements of Article 40(2) of that Directive concerning the parameters related to the significance of an incident, should continue to be used by the competent authorities in charge of supervision and enforcement for the purposes of this Directive.	(49) Where appropriate and to avoid unnecessary disruption, existing national guidelines ~~*and national legislation*~~ adopted for the transposition of the rules related to security measures laid down in ~~*Article 40(1)*~~***Articles 40 and 41*** of Directive (EU) 2018/1972 ***should be taken into account in transposition arrangements implemented by the Member States in relation to this Directive, thereby building on the knowledge and skills already acquired under***~~*, as well as of the requirements of Article 40(2) of that*~~ Directive ***(EU) 2018/1972*** concerning ~~*the parameters related to the significance of an incident, should continue to be used by the*~~ ***security risk management measures and incident***	

			notifications. ENISA can also develop guidance on security and reporting requirements for providers of public electronic communication networks or publicly available electronic communication services to facilitate harmonisation, transition and minimise disruption. Member States can assign the role of competent authorities ***for electronic communications to the national regulatory authorities in order to ensure the continuation of current practices and to build on the knowledge and experience gained in*** ~~*in charge of supervision and enforcement for the purposes of this*~~ Directive ***(EU) 2018/1972***.	
Recital 50				
60	(50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of security of network and	(50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of security of network and	(50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of security of network and	

	information systems appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission.	information systems appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk ***to network security*** for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission. ***However, as the attack surface continues to expand, number-independent interpersonal communications services including, but not limited to, social media messengers, are becoming popular attack vectors. Malicious actors use platforms to communicate and attract victims to open compromised web pages, therefore increasing the likelihood of incidents involving the exploitation of personal data, and by extension, the security of information systems.***	information systems appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission.	
Recital 51				

61	(51) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report incidents in relation thereto.	(51) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that ***all*** public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report ***significant*** incidents in relation thereto. ***Member States should ensure that the integrity and availability of those public electronic communications networks are maintained and should consider their protection from sabotage and espionage of vital security interest. Information about incidents, for example on submarine communication cables should be shared actively between Member States.***	(51) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report incidents in relation thereto.	(51) ***The internal market is more reliant on the functioning of the internet than ever. The services of almost all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that all public electronic communication networks have appropriate cybersecurity measures in place and report significant incidents in relation thereto. Member States should ensure that the integrity and availability of the public electronic communication networks are maintained and protect their vital security interests from sabotage and espionage. Where relevant, Member States should investigate attribute incidents related to the undersea communication cables between Member States and Member States as well as between Member States and third countries. These incidents should be reported to the relevant CSIRT. The national cybersecurity strategy of Member States with undersea communication cables should include a mapping of potential***

				security risks and a targeted strategy for each of the cables present to secure the highest level of their protection. ~~*The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report incidents in relation thereto.*** EP proposal
Recital 52				
62	(52) Where appropriate, entities should inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves. The requirement to inform those recipients of such threats should	(52) Where appropriate, entities should inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves. ~~*The requirement to inform those recipients of such threats*~~***This***	(52) Where ~~*appropriate*~~ ***applicable***, entities should inform their service recipients of particular ~~*and significant threats and of*~~ measures they can take to mitigate the resulting risk ***from a significant cyber threat*** to themselves. The ***entities should,***	

	not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about security threats to the recipients should be free of charge.	should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about security threats to the recipients should be free of charge ***and drafted in an easily comprehensible language***.	***where appropriate and in particular in cases where the significant cyber threat can materialise, notify also their service recipients in parallel to the competent authorities or CSIRTs of the threat itself. The*** requirement to inform those recipients of such threats should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about ~~*security*~~***cyber*** threats to the recipients should be free of charge.	
Recital 53				
63	(53) In particular, providers of public electronic communications networks or publicly available electronic communications services, should inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their communications, for instance by using specific types of software or encryption technologies.	(53) ~~*In particular,*~~ Providers of public electronic communications networks or publicly available electronic communications services, should ***implement security by design and by default, and*** inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their ***devices and*** communications, for instance by using specific types of	(53) In particular, providers of public electronic communications networks or publicly available electronic communications services, should inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their communications, for instance by using specific types of software or encryption technologies.	

		encryption software or ~~*encryption*~~***other data-centric security*** technologies.		
Recital 54				
64	(54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective	(54) In order to safeguard the security of electronic communications networks and services, the use of encryption ***and other data-centric security technologies, such as, tokenisation, segmentation, throttle access, marking, tagging, strong identity and access management, and automated access decisions*** ~~*, and in particular end-to-end encryption*~~, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. ~~*Solutions for lawful access to*~~	(54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime.	

	response to crime.	~~*information in end-to-end encrypted communications should maintain the effectiveness of*~~***However, this should not lead to any efforts to weaken end-to-end*** encryption***, which is a critical technology for effective data protection and privacy*** ~~*in protecting privacy and security of communications, while providing an effective response to crime*~~.		
Recital 54a				
64a		***(54a) In order to safeguard the security and to prevent abuse and manipulation of electronic communications networks and services, the use of interoperable secure routing standards should be promoted to ensure the integrity and robustness of routing functions across the ecosystem of internet carriers.***		
Recital 54b				
64b		***(54b) In order to safeguard the functionality and integrity of the internet and to reduce security issues relating to DNS, relevant stakeholders including Union businesses, internet service***		

		providers and browser vendors should be encouraged to adopt a DNS resolution diversification strategy. Furthermore, Member States should encourage the development and use of a public and secure European DNS resolver service.		
Recital 55				
65	(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification within 24 hours, followed by a final report not later than one month after. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the	(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification ~~*within 24 hours,*~~ followed by a ~~*final*~~***comprehensive*** report not later than one month after~~*. The initial notification should only include the information strictly necessary to make the competent authorities*	(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification within 24 hours, followed by a final report not later than one month after. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the	(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. ~~*Where entities become aware of an incident, they should be required to submit*~~***In this regard, the Directive should also include reporting of incidents that, based on*** an initial ~~*notification within 24 hours, followed by a final report not later than one month after. The initial notification should only include the*~~

	entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines of 24 hours for the initial notification and one month for the final report.	~~aware~~ ***the submission*** of the ~~incident and allow the entity to seek assistance, if required. Such~~***initial*** notification~~, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States~~***. The initial incident notification timeline*** should ~~ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines of 24 hours for the initial notification and one month for the final report~~***not preclude entities from reporting incidents earlier, therefore allowing them to seek support from CSIRTs swiftly enabling the mitigation and the potential spread of the reported incident. CSIRTs can request an intermediate report on relevant***	entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines of 24 hours for the initial notification and one month for the final report.	~~information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable,~~***assessment performed by the entity, may be assumed to lead to substantial (severe) operational disruption or financial losses or affect other natural or legal persons by causing considerable material or non-material losses. Such initial assessment*** should ~~indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting~~ ***take into account, amongst other, the affected network and information systems and in particular their importance in the provision of the*** entity's ~~resources from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent~~

		status updates, while taking into account the incident response and remediation efforts of the reporting entity.		~~*authorities*~~***services, the severity and technical characteristics of a cyber threat and any underlying vulnerabilities that are being exploited as well as the entity's experience with similar incidents. Indicators such as the extent to which the functioning of the service is affected, the duration of an incident*** or the ~~*CSIRT, the entity concerned can deviate from the deadlines of 24 hours for the initial notification and one month for the final report*~~***number of affected recipients of services could play an important role in defining whether the operational disruption of the service is of substantial (severe) nature***.
Recital 55a				
65a			***(55a) A proactive approach to cyber threats is a vital component of cybersecurity risk management that should enable competent authorities to effectively prevent cyber threats from materialising into actual incidents that may cause considerable material or non-material losses. For that purpose, the notification of significant cyber threats is of key importance.***	***(55a) Where entities become aware of a significant incident, they should be required to submit an initial notification within 24 hours, followed by a comprehensive l report not later than one month after. The initial notification should only include the information strictly necessary to make the competent authority aware of the incident and allow the entity to seek assistance, if***

				required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect. In cases of ongoing incidents at the time of the submission of the comprehensive report, Member States should ensure that entities provide a final report within one month after the incident has been mitigated.
Recital 55a				
65b		***(55a) A significant incident may have an impact on the confidentiality, integrity or availability of the service. Essential and important entities should notify CSIRTs about significant incidents that have an***		

		impact on the availability of their service within 24 hours of becoming aware of the incident. They should notify CIRTs about significant incidents that breach the confidentiality and integrity of their services within 72 hours of becoming aware of the incident. The distinction between the types of incidents is not based on the seriousness of the incident, but on the difficulty for the reporting entity to assess the incident, its significance and the ability to report information that can be of use for the CSIRT. The initial notification should include the information necessary to make the CSIRT aware of the incident and allow the entity to seek assistance, if required. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the		

		CSIRT, the entity concerned can deviate from the deadlines for the initial notification and for the comprehensive report.		
Recital 56				
66	(56) Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents, Member States should establish a single entry point for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. ENISA, in cooperation with the Cooperation Group should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union	(56) Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents, Member States should establish a single entry point for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. ENISA, in cooperation with the Cooperation Group should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union	(56) Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents, Member States ~~*should*~~***could*** establish a single entry point for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. ENISA, in cooperation with the Cooperation Group should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union	

		law and decrease the burdens for companies.	law and decrease the burdens for companies.	law and decrease the burdens for companies.		
	Recital 57					
G	67	(57) Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage essential and important entities, on the basis of applicable criminal proceedings rules in compliance with Union law, to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, and without prejudice to the personal data protection rules applying to Europol, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the EC3 and ENISA.	(57) Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage essential and important entities, on the basis of applicable criminal proceedings rules in compliance with Union law, to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, and without prejudice to the personal data protection rules applying to Europol, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the EC3 and ENISA.	(57) Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage essential and important entities, on the basis of applicable criminal proceedings rules in compliance with Union law, to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, and without prejudice to the personal data protection rules applying to Europol, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the EC3 and ENISA.		G
	Recital 58					
G	68	(58) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities should cooperate and exchange	(58) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities should cooperate and exchange	(58) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities should cooperate and exchange		G

	information on all relevant matters with data protection authorities and the supervisory authorities pursuant to Directive 2002/58/EC.	information on all relevant matters with data protection authorities and the supervisory authorities pursuant to Directive 2002/58/EC.	information on all relevant matters with data protection authorities and the supervisory authorities pursuant to Directive 2002/58/EC.	
Recital 59				
69	(59) Maintaining accurate and complete databases of domain names and registration data (so called 'WHOIS data') and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law.	(59) Maintaining accurate, ***verified*** and complete databases of domain names ~~*and*~~ registration data (so called 'WHOIS data') ~~*and providing lawful access to such data*~~ is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union, ***and for tackling illegal activities. TLD registries and entities providing domain name registration services should therefore be required to collect domain name registration data, which should include at least the registrants' name, their physical and email address as well as their telephone number. In practice, the collected data may not always be thoroughly accurate, however TLD registries and entities providing domain name registration services should adopt and implement proportionate processes to verify that natural or***	(59) Maintaining accurate and complete databases of domain names and registration data (so called 'WHOIS data') and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law.	

		legal persons requesting or owning a domain name have provided contact details on which they can be reached and are expected to reply. Using a 'best efforts' approach, those verification processes should reflect the current best practices used within the industry. Those best practices in the verification process should reflect the advances being made in the electronic identification process. The TLD registries and entities providing domain name registration services should make publicly available their policies and procedures to ensure the integrity and availability of the domain name registration data. Where processing includes personal data such processing shall comply with Union data protection law.		
Recital 60				
70	(60) The availability and timely accessibility of these data to public authorities, including competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CERTs,	(60) The availability and timely accessibility of ~~these~~***the domain name registration*** data to ~~public authorities~~***legitimate access seekers is essential for cybersecurity purposes and tackling illegal activities in the***	(60) The availability and timely accessibility of these data to public authorities, including competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CERTs,	

	(CSIRTs, and as regards the data of their clients to providers of electronic communications networks and services and providers of cybersecurity technologies and services acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents. Such access should comply with Union data protection law insofar as it is related to personal data.	***online ecosystem. TLD registries and entities providing domain name registration services should therefore be required to enable lawful access to specific domain name registration data***, including ***personal data, to legitimate access seekers, in accordance with Union data protection law. Legitimate access seekers should make a duly justified request to access domain name registration data on the basis of Union or national law, and could include*** competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, ***and national*** CERTs~~, (~~ ***or*** CSIRTs~~, and as regards the data of their clients to providers of electronic communications networks and~~. ***Member States should ensure that TLD registries and entities providing domain name registration services should respond without undue delay and in any event within 72 hours to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and entities providing domain name registration*** services ~~and providers of cybersecurity technologies and~~	(CSIRTs, and as regards the data of their clients to providers of electronic communications networks and services and providers of cybersecurity technologies and services acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents. Such access should comply with Union data protection law insofar as it is related to personal data.	

		~~*services acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents. Such access should comply with Union data protection law insofar as it is related to personal data*~~***should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tools to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board***.		
Recital 61				
71	(61) In order to ensure the availability of accurate and complete domain name registration data, TLD registries and the	~~*(61) In order to ensure the availability of accurate and complete domain name registration data, TLD registries*~~	(61) In order to ensure the availability of accurate and complete domain name registration data, TLD registries and the	

	entities providing domain name registration services for the TLD (so-called registrars) should collect and guarantee the integrity and availability of domain names registration data. In particular, TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules.	~~*and the entities providing domain name registration services for the TLD (so-called registrars) should collect and guarantee the integrity and availability of domain names registration data. In particular, TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules.*~~	entities providing domain name registration services for the TLD (so-called registrars) should collect and guarantee the integrity and availability of domain names registration data. ***With regard to the registration data, the entities should*** in particular, ~~,~~ ***verify the name and the email address of the registrant.*** TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules.	
Recital 62				
72	(62) TLD registries and the entities providing domain name registration services for them should make publically available domain name registration data that fall outside the scope of Union data protection rules, such as data that concern legal persons[1]. TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain	(62) TLD registries and ~~*the*~~ entities providing domain name registration services ~~*for them should make publically*~~***should be required to make publicly*** available domain name registration data that ~~*fall outside the scope of Union data protection rules, such as data that concern*~~***does not contain personal data. A distinction should be made between natural and*** legal	(62) TLD registries and the entities providing domain name registration services for them should make publically available domain name registration data that fall outside the scope of Union data protection rules, such as data that concern legal persons[1]. TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain	

	name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should ensure that TLD registries and the entities providing domain name registration services for them should respond without undue delay to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and the entities providing domain name registration services for them should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board. _____ 1. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND	persons[1]. ~~*TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain name registration data concerning natural*~~***For legal*** persons ~~*to legitimate access seekers, in accordance with Union data protection law. Member States should ensure that*~~ **,** TLD registries and ~~*the*~~ entities ~~*providing domain name registration services for them*~~ should ~~*respond without undue delay to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and the entities providing domain name registration services for them should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the*~~	name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should ensure that TLD registries and the entities providing domain name registration services for them should respond without undue delay to requests ***for the disclosure of domain name registration data*** from legitimate access seekers***, such as competent authorities under Union or national law in the area of national security and criminal justice or CSIRTs*** ~~*for the disclosure of domain name registration data*~~. TLD registries and the entities providing domain name registration services for them should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. ***Member States should ensure that all type of access to domain registration data (both personal and non-personal***	

	OF THE COUNCIL recital (14) whereby "this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person".	~~competences of the European Data Protection Board~~ ***make publicly available at least the registrants' name, their physical and email address as well as their telephone number. The legal person should be required to either provide a generic email address that can be made publicly available or give consent to the publication of a personal email address. The legal person should be able to demonstrate such consent at the request of TLD registries and entities providing domain name registration services.*** _____ 1. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL recital (14) whereby "this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person".	***data) are free of charge.*** With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board ***in line with and complementary to international standards developed by the multi-stakeholder community***. _____ 1. ~~REGULATION~~***Regulation*** (EU) 2016/679 ~~OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL~~***of the European Parliament and of the Council,*** recital (14) whereby "this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person".	
Recital 63				
73	(63) All essential and important entities under this Directive should fall under the jurisdiction of the Member State where they provide their services. If the entity provides	(63) All essential and important entities under this Directive should fall under the jurisdiction of the Member State where they provide their services ***or carry out their***	(63) ~~All~~ Essential and important entities under this Directive should fall under the jurisdiction of the Member State where they provide their services. ***Entities referred to***	

	services in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of these Member States should cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions.	***activities***. If the entity provides services in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of these Member States should cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions.	***in points 1 to 7 and 10 of Annex I, trust service providers and Internet Exchange Point providers referred to in point 8 of Annex I and points 1 to 5 of Annex II of this Directive should fall under the jurisdiction of the Member State where they are established.*** If the entity provides services ***or has an establishment*** in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of these Member States should cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions. ***Where Member States decide to exercise jurisdiction, they should avoid that the same conduct is sanctioned more than once for the infringement of the obligations laid down in this Directive.***	
Recital 63a				
73a				***(63a) For the purpose of ensuring compliance of the entities with their obligations under this Directive, Member States should cooperate and assist each other in the performance of***

				supervisory and enforcement measures, notably when services are provided in more than one Member State or when the network and information systems are located in a different Member State than the ones where services are provided. When providing assistance, the competent authority the assistance of which was requested should carry out supervisory or enforcement measures in accordance with its national law. In order to ensure the smooth functioning of the mutual assistance mechanism established under this Directive, competent authorities should use the Cooperation Group as a forum to discuss cases and particular requests for assistance. new recital by the PR in relation to Art 24(1)
Recital 64				
74	(64) In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, content delivery network providers, cloud computing service providers, data centre service	(64) In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, content delivery network providers, cloud computing service providers, data centre service	(64) In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, ***entities providing domain name registration services for the TLD,*** content delivery network	

	providers and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are taken in the Union. This will typically correspond to the place of the companies' central administration in the Union. If such decisions are not taken in the Union, the main establishment	providers and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are taken in the Union. This will typically correspond to the place of the companies' central administration in the Union. If such decisions are not taken in the Union, the main establishment	providers, cloud computing service providers, data centre service providers and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are ***predominantly*** taken in the Union. This will typically correspond to the place of the companies' central administration	

	should be deemed to be in the Member States where the entity has an establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings.	should be deemed to be in the Member States where ***either*** the entity has an establishment with the highest number of employees in the Union ***or the establishment where cybersecurity operations are carried out***. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings.	in the Union. If ***the place where such decisions are predominantly taken cannot be determined or*** such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States where the entity has an establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings.	
Recital 64a				
74a			***(64a) When a recursive DNS service is provided by a provider of public electronic communications networks or publicly available electronic communications services only as a part of the internet access service, the entity should be deemed to be under the jurisdiction of all the Member States where its services are provided.***	
Recital 64b				
74b				

			(64aa) In order to ensure a clear overview of DNS service providers, TLD name registries, entities providing domain name registration services for the TLD, content delivery network providers, cloud computing service providers, data centre service providers and digital providers providing services across the Union under the scope of this Directive, ENISA should create and maintain a registry for such entities, based on notifications received by Member States, where applicable through their national mechanisms for self-notification. With a view to ensure accuracy and completeness of the information that should be included in this registry, Member States should submit to ENISA the information available in their national registries on these entities. ENISA and the Member States should take measures to facilitate the interoperability of such registries, while ensuring protection of confidential or classified information.	
Recital 65				
75				

	(65) In cases where a DNS service provider, TLD name registry, content delivery network provider, cloud computing service provider, data centre service provider and digital provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such an entity is offering services within the Union, it should be ascertained whether it is apparent that the entity is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the entity's or an intermediary's website or of an email address and of other contact details, or the use of a language generally used in the third country where the entity is established, is as such insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the entity is planning to offer services within the Union. The representative should act on behalf	(65) In cases where a DNS service provider, TLD name registry, content delivery network provider, cloud computing service provider, data centre service provider and digital provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such an entity is offering services within the Union, it should be ascertained whether it is apparent that the entity is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the entity's or an intermediary's website or of an email address and of other contact details, or the use of a language generally used in the third country where the entity is established, is as such insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the entity is planning to offer services within the Union. The representative should act on behalf of the entity and it should be	(65) In cases where a DNS service provider, TLD name registry, content delivery network provider, cloud computing service provider, data centre service provider and digital provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such an entity is offering services within the Union, it should be ascertained whether it is apparent that the entity is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the entity's or an intermediary's website or of an email address and of other contact details, or the use of a language generally used in the third country where the entity is established, is as such insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the entity is planning to offer services within the Union. The representative should act on behalf of the entity and it should be	

	of the entity and it should be possible for competent authorities or the CSIRTs to contact the representative. The representative should be explicitly designated by a written mandate of the entity to act on the latter's behalf with regard to the latter's obligations under this Directive, including incident reporting.	possible for competent authorities or the CSIRTs to contact the representative. The representative should be explicitly designated by a written mandate of the entity to act on the latter's behalf with regard to the latter's obligations under this Directive, including incident reporting.	possible for competent authorities or the CSIRTs to contact the representative. The representative should be explicitly designated by a written mandate of the entity to act on the latter's behalf with regard to the latter's obligations under this Directive, including incident reporting.	
Recital 65a				
75a		***(65a) ENISA should create and maintain a registry containing information about essential and important entities that comprise DNS service providers, TLD name registries and providers of cloud computing services, data centre services, content delivery networks, online marketplaces, online search engines and social networking platforms. Those essential and important entities should submit to ENISA their names, addresses and up-to-date contact details. They should notify ENISA about any changes to those details without delay and, in any event, within two weeks from the date on which the change took effect. ENISA should forward the information to the relevant single***		

		point of contact. The essential and important entities submitting their information to ENISA are therefore not required to separately inform the competent authority within the Member State. ENISA should develop a simple publicly available application programme that those entities could use to update their information. Furthermore, ENISA should establish appropriate information classification and management protocols to ensure the security and confidentiality of disclosed information, and restrict the access, storage, and transmission of such information to intended users.		
Recital 66				
76	(66) Where information considered classified according to national or Union law is exchanged, reported or otherwise shared under the provisions of this Directive, the corresponding specific rules on the handling of classified information should be applied.	(66) Where information considered classified ~~according to~~***in accordance with*** national or Union law is exchanged, reported or otherwise shared under the provisions of this Directive, the corresponding specific rules on the handling of classified information should be applied. ***In addition, ENISA should have the infrastructure, procedures and***	(66) Where information considered classified according to national or Union law is exchanged, reported or otherwise shared under the provisions of this Directive, the corresponding specific rules on the handling of classified information should be applied.	

			rules in place to handle sensitive and classified information in compliance with the applicable security rules for protecting EU classified information.			
	Recital 67					
G	77	(67) With cyber threats becoming more complex and sophisticated, good detection and prevention measures depend to a large extent on regular threat and vulnerability intelligence sharing between entities. Information sharing contributes to increased awareness on cyber threats, which, in turn, enhances the entities' capacity to prevent threats from materialising into real incidents and enables the entities to better contain the effects of incidents and recover more efficiently. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, notably uncertainty over the compatibility with competition and liability rules.	(67) With cyber threats becoming more complex and sophisticated, good detection and prevention measures depend to a large extent on regular threat and vulnerability intelligence sharing between entities. Information sharing contributes to increased awareness on cyber threats, which, in turn, enhances the entities' capacity to prevent threats from materialising into real incidents and enables the entities to better contain the effects of incidents and recover more efficiently. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, notably uncertainty over the compatibility with competition and liability rules.	(67) With cyber threats becoming more complex and sophisticated, good detection and prevention measures depend to a large extent on regular threat and vulnerability intelligence sharing between entities. Information sharing contributes to increased awareness on cyber threats, which, in turn, enhances the entities' capacity to prevent threats from materialising into real incidents and enables the entities to better contain the effects of incidents and recover more efficiently. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, notably uncertainty over the compatibility with competition and liability rules.		G
	Recital 68					
	78	(68) Entities should be encouraged	(68) Entities should be encouraged	(68) Entities should be encouraged		

	to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms. Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection Union law rules.	***and supported by Member States*** to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive***, such as entities focusing on cybersecurity services and research,*** to participate in such information-sharing mechanisms. Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection Union law rules.	to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms. Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection Union law rules.	
Recital 69				
79	(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs,	(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by ~~*entities, public authorities, CERTs*~~***essential***	(69) ~~*The processing of personal data,*~~ To the extent strictly necessary and proportionate for the purposes of ensuring network and information security***, the processing of personal data by***	

	CSIRTs, and providers of security technologies and services should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of the following types of personal data: IP addresses, uniform resources locators (URLs), domain names, and email addresses.	***and important entities***, CSIRTs~~,~~ and providers of security technologies and services***, is necessary for compliance with their legal obligations provided for in this Directive. Such processing of personal data might also be necessary for the purposes*** ~~*should constitute a legitimate interest*~~ of the ***legitimate interests pursued by essential and important entities. Where this Directive requires the processing of personal data for the purpose of cybersecurity and network and information security in accordance with the provisions set out in Article 18, 20 and 23 of the Directive, that processing is considered to be necessary for compliance with a legal obligation*** ~~*data controller concerned,*~~ as referred to in ***Article 6(1), point (c) of*** Regulation (EU) 2016/679. ~~*That should include*~~***For the purpose of Article 26 and 27 of this Directive, processing, as referred to in Article 6(1), point (f) of Regulation (EU) 2016/679, is considered to be necessary for the purposes of the legitimate interests pursued by the essential and important entities.*** Measures related to the prevention, detection, ***identification, containment,***	***essential and important entities*** ~~*by entities, public authorities, CERTs, CSIRTs*~~, and providers of security technologies and services ~~*should*~~ ***could be considered necessary for compliance with a legal obligation or*** constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. That ~~*should*~~ ***could*** include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, ~~*as well as*~~ cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of ~~*the following*~~ ***various*** types of personal data***, such as***: IP addresses, uniform resources locators (URLs), domain names, and email addresses. ***Processing of personal data by competent authorities, SPOCs and CSIRTs should be laid down in national law and considered***	

		analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools~~. Such measures may~~ require the processing of ~~the following types~~***certain categories*** of personal data~~:~~***, such as*** IP addresses, uniform resources locators (URLs), domain names, ~~and~~ email addresses***, time stamps, Operation System- or browser-related information, cookies or other information indicating the modus operandi***.	***necessary for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, as referred to in Article 6(1) point (c) or (e) of Regulation (EU) 2016/679.***	
Recital 69a				
79a			***(69a) Member States' laws may lay down rules allowing competent authorities, SPOCs and CSIRTs, to the extent that is strictly necessary and proportionate for the purpose of ensuring the security of network***	

			and information systems of essential and important entities, to process special categories of personal data in accordance with Article 9 of Regulation (EU) 2016/679, in particular by providing for suitable and specific measures to safeguard the fundamental rights and interests of natural persons, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.	
Recital 70				
80	(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance, this Directive should provide for a minimum list of supervisory actions and means through which competent authorities may supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to	(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance, this Directive should provide for a minimum list of supervisory actions and means through which competent authorities may supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to	(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance, this Directive should provide for a minimum list of supervisory actions and means through which competent authorities ~~*may*~~ ***can*** supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities	

	ensuring a fair balance of obligations for both entities and competent authorities. Thus, essential entities should be subject to a fully-fledged supervisory regime (ex-ante and ex-post), while important entities should be subject to a light supervisory regime, ex-post only. For the latter, this means that important entities should not document systematically compliance with cybersecurity risk management requirements, while competent authorities should implement a reactive ex -post approach to supervision and, hence, not have a general obligation to supervise those entities.	ensuring a fair balance of obligations for both entities and competent authorities. Thus, essential entities should be subject to a fully-fledged supervisory regime (ex-ante and ex-post), while important entities should be subject to a light supervisory regime, ex-post only. For the latter, this means that important entities should not document systematically compliance with cybersecurity risk management requirements, while competent authorities should implement a reactive ex -post approach to supervision and, hence, not have a general obligation to supervise those entities.	with a view to ensuring a fair balance of obligations for both entities and competent authorities. Thus, essential entities should be subject to a fully-fledged supervisory regime (ex-ante and ex-post), while important entities should be subject to a light supervisory regime, ex-post only. For the latter, this means that important entities should not ~~document~~***be required to*** systematically ***document*** compliance with cybersecurity risk management requirements, while competent authorities should implement a reactive ex -post approach to supervision and, hence, not have a general obligation to supervise those entities. ***For important entities, ex-post supervision may be triggered by evidence or any indication or information brought to the attention of competent authorities deemed by these authorities as suggesting potential non-compliance with the obligations laid down in this Directive. For example, such evidence, indication or information could be of the type provided to competent authorities by other authorities, entities, citizens, media or other sources, publicly***	

			available information, or may emerge from other activities conducted by the competent authorities in the fulfilment of their tasks.	
Recital 70(bis)				
80a			***(70bis) In the exercise of ex-ante supervision, competent authorities should be able to decide on the prioritisation of the use of supervisory actions and means at their disposal in a proportionate manner. This entails that competent authorities can decide on such prioritisation based on supervisory methodologies which should follow a risk-based approach. More specifically, such methodologies could include criteria or benchmarks for the classification of essential entities into risk categories and corresponding supervisory actions and means recommended per risk category, such as use, frequency or type of on-site inspections or targeted security audits or security scans, type of information to be requested and level of detail of that information. Such supervisory methodologies can also be accompanied by work***	

			programmes and be assessed and reviewed regularly, including on aspects such as resource allocation and needs.	
Recital 70 (bisa)				
80b			***70 (bisa)*** ***In relation to public administration entities, the supervisory powers should be exercised in line with the national frameworks and legal order. Member States should be able to decide on the imposition of appropriate, proportionate and effective measures of supervision and enforcement in relation to these entities.***	
Recital 70 (bisaa)				
80c			***70 (bisaa)*** ***In order to demonstrate compliance with certain cybersecurity risk management measures, Member States could require essential and important entities to use qualified trust services or notified electronic identification schemes under Regulation (EU) No 910/2014.***	

Recital 71				
81	(71) In order to make enforcement effective, a minimum list of administrative sanctions for breach of the cybersecurity risk management and reporting obligations provided by this Directive should be laid down, setting up a clear and consistent framework for such sanctions across the Union. Due regard should be given to the nature, gravity and duration of the infringement, the actual damage caused or losses incurred or potential damage or losses that could have been triggered, the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of	(71) In order to make enforcement effective, a minimum list of administrative ~~*sanctions*~~***penalties*** for breach of the cybersecurity risk management and reporting obligations provided by this Directive should be laid down, setting up a clear and consistent framework for such ~~*sanctions*~~***penalties*** across the Union. Due regard should be given to the nature, gravity and duration of the infringement, the ~~*actual*~~ damage caused or losses incurred ~~*or potential damage or losses that could have been triggered*~~, the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The ~~*imposition of*~~ penalties, including administrative fines, ***should be proportionate and their imposition*** should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the	(71) In order to make enforcement effective, a minimum list of administrative sanctions for breach of the cybersecurity risk management and reporting obligations provided by this Directive should be laid down, setting up a clear and consistent framework for such sanctions across the Union. Due regard should be given to the nature, gravity and duration of the infringement, the actual damage caused or losses incurred or potential damage or losses that could have been triggered, the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of	

	the European Union, including effective judicial protection and due process.	Charter of Fundamental Rights of the European Union ***(the 'Charter')***, including effective judicial protection***, due process, the presumption of innocence and the rights of defence*** ~~*and due process*~~.	the European Union, including effective judicial protection and due process.	
Recital 71a				
81a			***(71bis) The provisions relating to the liability of natural persons holding certain responsibilities within an entity for breach of their duty to ensure compliance with the obligations laid down in this Directive do not require Member States to ensure criminal prosecution or civil liability for damages caused by such breach to third parties.***	
Recital 72				
82	(72) In order to ensure effective enforcement of the obligations laid down in this Directive, each competent authority should have the power to impose or request the imposition of administrative fines.	(72) In order to ensure effective enforcement of the obligations laid down in this Directive, each competent authority should have the power to impose or request the imposition of administrative fines ***if the infringement was intentional, negligent or the entity concerned had received notice of***	(72) In order to ensure effective enforcement of the obligations laid down in this Directive, each competent authority should have the power to impose or request the imposition of administrative fines.	

			<u>the entity's non-compliance</u>.			
	Recital 73					
G	83	(73) Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine does not affect the application of other powers by the competent authorities or of other penalties laid down in the national rules transposing this Directive.	(73) Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine does not affect the application of other powers by the competent authorities or of other penalties laid down in the national rules transposing this Directive.	(73) Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine does not affect the application of other powers by the competent authorities or of other penalties laid down in the national rules transposing this Directive.		G
	Recital 74					
	84	(74) Member States should be	(74) Member States should be able	(74) Member States ~~*should be*~~		

		able to lay down the rules on criminal penalties for infringements of the national rules transposing this Directive. However, the imposition of criminal penalties for infringements of such national rules and of related administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice.	to lay down the rules on criminal penalties for infringements of the national rules transposing this Directive. However, the imposition of criminal penalties for infringements of such national rules and of related administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice.	~~able to~~***may*** lay down the rules on criminal penalties for infringements of the national rules transposing this Directive. However, the imposition of criminal penalties for infringements of such national rules and of related administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice.		
	Recital 75					
G	85	(75) Where this Directive does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of the obligations laid down in this Directive, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.	(75) Where this Directive does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of the obligations laid down in this Directive, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.	(75) Where this Directive does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of the obligations laid down in this Directive, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.		G
	Recital 76					
	86	(76) In order to further strengthen the effectiveness and	(76) In order to further strengthen the effectiveness and	(76) In order to further strengthen the effectiveness and		

	dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning part or all the services provided by an essential entity and the imposition of a temporary ban from the exercise of managerial functions by a natural person. Given their severity and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which	dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply ~~*sanctions consisting of the*~~*a temporary* suspension of a certification or authorisation concerning part or all ~~*the*~~*relevant* services provided by an essential entity and the ~~*imposition of a*~~ *request to impose a temporary ban from the exercise of managerial functions by a natural person at chief executive officer or legal representative level. Member States should develop specific procedures and rules concerning the* temporary ban from the exercise of managerial functions by a natural person *at chief executive officer or legal representative level in public administration entities. In the process of developing such procedures and rules, Member States should take into account the particularities of their respective levels and systems of governance within their public administrations*. Given their severity and impact on the entities' activities and ultimately on their consumers, such ~~*sanctions*~~*temporary suspensions*	dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning part or all the services provided by an essential entity and the imposition of a temporary ban from the exercise of managerial functions by a natural person. Given their severity and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such	

	such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection, due process, presumption of innocence and right of defence.	***or bans*** should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such ~~*sanctions*~~***temporary suspensions or bans*** should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such ~~*sanctions*~~***temporary suspensions or bans*** were applied. The imposition of such ~~*sanctions*~~***temporary suspensions or bans*** shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter ~~*of Fundamental Rights of the European Union*~~, including effective judicial protection, due process, presumption of innocence and right of defence.	sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection, due process, presumption of innocence and right of defence.	

Recital 76a					
	86a			***(76bis) In order to ensure effective supervision and enforcement, notably in cases with a cross-border dimension, Member States that have received a request for mutual assistance should, to the extent of the request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has the network and information system on their territory.***	
Recital 77					
G	87	(77) This Directive should establish cooperation rules between the competent authorities and the supervisory authorities in accordance with Regulation (EU) 2016/679 to deal with infringements related to personal data.	(77) This Directive should establish cooperation rules between the competent authorities and the supervisory authorities in accordance with Regulation (EU) 2016/679 to deal with infringements related to personal data.	(77) This Directive should establish cooperation rules between the competent authorities and the supervisory authorities in accordance with Regulation (EU) 2016/679 to deal with infringements related to personal data.	G
Recital 78					
G	88	(78) This Directive should aim at ensuring a high level of responsibility for the cybersecurity	(78) This Directive should aim at ensuring a high level of responsibility for the cybersecurity	(78) This Directive should aim at ensuring a high level of responsibility for the cybersecurity	G

	risk management measures and reporting obligations at the level of the organisations. For these reasons, the management bodies of the entities falling within the scope of this Directive should approve the cybersecurity risk measures and supervise their implementation.	risk management measures and reporting obligations at the level of the organisations. For these reasons, the management bodies of the entities falling within the scope of this Directive should approve the cybersecurity risk measures and supervise their implementation.	risk management measures and reporting obligations at the level of the organisations. For these reasons, the management bodies of the entities falling within the scope of this Directive should approve the cybersecurity risk measures and supervise their implementation.	
Recital 79				
89	(79) A peer-review mechanism should be introduced, allowing the assessment by experts designated by the Member States of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources.	(79) A peer-review mechanism should be introduced, allowing the assessment by ***independent*** experts designated by the Member States**,** of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources. ***Peer-reviews can lead to valuable insights and recommendations strengthening the overall cybersecurity capabilities. In particular, they can contribute in facilitating the transfer of technologies, tools, measures and processes among the Member States involved in the peer-review, creating a functional path for the sharing of best practices across Member States with different levels of maturity in cybersecurity, and enabling the***	(79) A ~~*peer-review mechanism*~~***peer-learning system*** should be introduced ***to help strengthen mutual trust and learn from good practices and experiences***, allowing ~~*the assessment*~~***peer exchanges*** by experts designated by the Member States ~~*of*~~***on*** the implementation of cybersecurity policies**.** ***When implementing the peer-learning system, particular consideration should be given to ensure that it does not place unnecessary or disproportionate burden on the relevant Member States' authorities. The Commission should explore all possibilities to potentially guarantee the financial coverage of the costs that may be resulting from the organisation of peer learning***	

		establishment of a high, common level of cybersecurity across the Union. The peer-review should be preceded by a self-assessment by the Member State under review, covering the reviewed aspects and any additional targeted issues communicated by the designated experts to the Member State under peer-review prior to the commencement of the process. The Commission, in cooperation with ENISA and the Cooperation Group, should develop templates for the self-assessment of the reviewed aspects in order to streamline the process and avoid procedural inconsistencies and delays, which Member States under peer-review should complete and provide to the designated experts carrying out the peer-review prior to the commencement of the peer-review process.	***missions. Furthermore, the peer-learning system should take account of the results of similar mechanisms, such as the peer-review system of the CSIRTs network, add value and avoid duplication. The implementation of the peer-learning system should be without prejudice to national or Union laws on protection of confidential and classified information. Prior to the commencement of the peer-learning rounds,*** ~~*, including the level of*~~ Member States~~'~~ ~~*capabilities and available resources*~~ ***can carry out a self-assessment of the relevant aspects. Upon request from the Cooperation Group, ENISA can provide guidance on the self-assessment and relevant templates, where necessary. Member States could decide to make their respective reports publicly available***.	
Recital 80				
90	(80) In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290	(80) In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290	~~*(80) In order to take into account new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article*~~	

	TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. The Commission should also be empowered to adopt delegated acts establishing which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes. 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 Inter-institutional Agreement of 13 April 2016 on Better Law-Making[1]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. _____ 1. OJ L 123, 12.5.2016, p. 1.	TFEU should be delegated to the Commission in respect of the elements in relation to ***cybersecurity*** risk management measures ***and reporting obligations*** required by this Directive. The Commission should also be empowered to adopt delegated acts establishing which categories of essential ***and important*** entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes. 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 Inter-institutional Agreement of 13 April 2016 on Better Law-Making[1]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. _____	~~*290 TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. The Commission should also be empowered to adopt delegated acts establishing which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes. 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 Inter-institutional Agreement of 13 April 2016 on Better Law-Making[1]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.*~~ _____ ~~*1. OJ L 123, 12.5.2016, p. 1.*~~	

		1. OJ L 123, 12.5.2016, p. 1.		
Recital 81				
91	(81) In order to ensure uniform conditions for the implementation of the relevant provisions of this Directive concerning the procedural arrangements necessary for the functioning of the Cooperation Group, the technical elements related to risk management measures or the type of information, the format and the procedure of incident notifications, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.[1] 1. Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).	(81) In order to ensure uniform conditions for the implementation of the relevant provisions of this Directive concerning the procedural arrangements necessary for the functioning of the Cooperation Group~~, the technical elements related to risk management measures or the type of information, the format~~ and the procedure of incident notifications, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council~~.~~[1]**.** 1. Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).	(81) In order to ensure uniform conditions for the implementation of the relevant provisions of this Directive concerning the procedural arrangements necessary for the functioning of the Cooperation Group, the technical elements related to risk management measures or the type of information, the format and the procedure of incident notifications, ***the categories of entities that are to be required to use certain certified ICT products, services and processes,*** implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.[1] 1. Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).	

Recital 82				
92	(82) The Commission should periodically review this Directive, in consultation with interested parties, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.	(82) The Commission should periodically review this Directive, in consultation with interested parties, in particular with a view to determining ~~*the need for modification*~~***whether it is appropriate to propose amendments*** in the light of changes to societal, political, technological or market conditions. ***As part of those reviews, the Commission should assess the relevance of the sectors, subsectors and types of entities referred to in the annexes for the functioning of the economy and society in relation to cybersecurity. The Commission should assess, inter alia, whether digital providers that are classified as very large online platforms within the meaning of Article 25 of Regulation (EU) XXXX/XXXX [Single Market For Digital Services (Digital Services Act) or as gatekeepers as defined in Article 2, point 1 of Regulation (EU) XXXX/XXXX [Contestable and fair markets in the digital sector (Digital Markets Act)], should be designated as essential entities under this Directive.***	(82) The Commission should periodically review this Directive, in consultation with interested parties, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.	

		Furthermore, the Commission should assess whether it is appropriate to amend Annex I to the Directive 2020/1828 of the European Parliament and of the Council[1] by adding a reference to this Directive. ***1. Directive 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p.1).***		
Recital 82a				
92a		***(82a) This Directive lays down cybersecurity requirements for Member States as well as essential and important entities established in the Union. Those cybersecurity requirements should also be applied by the Union institutions, bodies, offices and agencies on the basis of a Union legislative act.***		
Recital 82b				
92b		***(82b) This Directive creates new tasks for ENISA, thereby enhancing its role, and could also***		

		result in ENISA being required to carry out its existing tasks under Regulation (EU) 2019/881 to a higher standard than before. In order to ensure that ENISA has the necessary financial and human resources to carry out existing and new activities under its tasks, as well as to satisfy any higher standard resulting from its enhanced role, its budget should be increased accordingly. In addition, in order to ensure the efficient use of resources, ENISA should be given greater flexibility in the way that it is permitted to allocate resources internally, so as to enable it to carry out its tasks, and to satisfy expectations, effectively.		
Recital 83				
G	93	(83) Since the objective of this Directive, namely to achieve a high common level of cybersecurity in the Union, cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5	(83) Since the objective of this Directive, namely to achieve a high common level of cybersecurity in the Union, cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, 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	(83) Since the objective of this Directive, namely to achieve a high common level of cybersecurity in the Union, cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, 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	G

	of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.	European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.	European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.		
Recital 84					
94	(84) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles,	(84) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter ~~*of Fundamental Rights of the European Union*~~, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This ***includes the right to an effective remedy before a court for the recipients of services provided by essential and important entities. This*** Directive should be implemented in accordance with those rights and principles~~,~~.	(84) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles,		
Formula					
95	HAVE ADOPTED THIS DIRECTIVE:	HAVE ADOPTED THIS DIRECTIVE:	HAVE ADOPTED THIS DIRECTIVE:		

CHAPTER I					
G	96	CHAPTER I General provisions	CHAPTER I General provisions	CHAPTER I General provisions	CHAPTER I General provisions Text Origin: Commission Proposal + Annexes
Article 1					
G	97	Article 1 Subject matter	Article 1 Subject matter	Article 1 Subject matter	Article 1 Subject matter Text Origin: Commission Proposal + Annexes
Article 1(1)					
G	98	1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union.	1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union.	1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union ***so as to improve the functioning of the internal market***.	1. This Directive lays down measures ~~*with a view to ensuring*~~***aiming to achieve*** a high common level of cybersecurity within the Union***, while aiming at improving the functioning of the internal market***.
Article 1(2), introductory part					
G	99	2. To that end, this Directive:	2. To that end, this Directive:	2. To that end, this Directive:	2. To that end, this Directive: Text Origin: Commission Proposal + Annexes

Article 1(2), point (a)				
100	(a) lays down obligations on Member States to adopt national cybersecurity strategies, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs);	(a) lays down obligations on Member States to adopt national cybersecurity strategies, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs);	(a) lays down obligations on Member States to adopt national cybersecurity strategies, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs);	(a) lays down obligations on Member States to adopt national cybersecurity strategies, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs); Text Origin: Commission Proposal + Annexes
Article 1(2), point (b)				
101	(b) lays down cybersecurity risk management and reporting obligations for entities of a type referred to as essential entities in Annex I and important entities in Annex II;	(b) lays down cybersecurity risk management and reporting obligations for entities of a type referred to as essential entities in Annex I and important entities in Annex II;	(b) lays down cybersecurity risk management and reporting obligations for entities of a type referred to ~~*as essential entities in Annex*~~***in Annexes*** I and ~~*important entities in Annex*~~ II;	Linked to EIE
Article 1(2), point (c)				
102	(c) lays down obligations on cybersecurity information sharing.	(c) lays down obligations on cybersecurity information sharing.	(c) lays down ***rules and*** obligations on cybersecurity information sharing.	(c) lays down ***rules and*** obligations on cybersecurity information sharing. Text Origin: Council Mandate
Article 1(2), point (ca)				

G	102a		***(ca) lays down supervision and enforcement obligations on Member States.***		***(ca) lays down supervision and enforcement obligations on Member States.*** Text Origin: EP Mandate	G
	Article 2					
G	103	Article 2 Scope	Article 2 Scope	Article 2 Scope	Article 2 Scope Text Origin: Commission Proposal + Annexes	G
	Article 2(1)					
G	104	1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.[1] 1. Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	1. This Directive applies to public and private ***essential and important*** entities of a type referred to as essential entities in Annex I and as important entities in Annex II ***that provide their services or carry out their activities within the Union***. This Directive does not apply to ~~*entities that qualify as micro and small enterprises within the meaning of*~~***small enterprises or microenterprises within the meaning of Article 2(2) and (3) of the Annex to*** Commission Recommendation 2003/361/EC[1]. ~~*1*~~ ***Article 3(4) of the Annex of that***	1. This Directive applies to public and private entities of ~~*a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC*~~***the types listed in Annexes I and II which meet or exceed the ceilings for medium-sized enterprises within the meaning of Commission Recommendation 2003/361/EC[1]. Article 3(4) and Article 6(2) second and third subparagraphs of the Annex to***	1. This Directive applies to public and private ***essential and important*** entities of a type referred to ~~*as essential entities*~~ in Annex I and ~~*as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small*~~***Annex II that provide their services or carry out their activities within the Union and which meet or exceed the threshold for medium-sized*** enterprises within the meaning of Commission Recommendation 2003/361/EC.~~*1*~~ ***[1] Article 3(4) of the Annex to that Recommendation shall not apply for the purposes of***	G

			Recommendation is not applicable. 1. Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	***that Recommendation shall not apply for the purposes of this Directive.***[1] 1. Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	***this Directive.*** ~~1. Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).~~
Article 2(2), introductory part					
G	105	2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where:	2. ~~However,~~ Regardless of their size, this Directive also applies to ~~entities referred to in Annexes I and II~~***essential and important entities***, where:	2. ~~However,~~ Regardless of ~~their size, this Directive also applies to~~***the size of the*** entities referred to in ~~Annexes I and II,~~***paragraph 1, this Directive also applies*** where:	2. ~~However,~~ Regardless of their size, this Directive also applies to ~~entities referred to in Annexes I and II,~~***essential and important entities*** where:
Article 2(2), point (a), introductory part					
G	106	(a) the services are provided by one of the following entities:	(a) the services are provided by one of the following entities:	(a) the services are provided by one of the following entities:	(a) the services are provided by ~~one of the following entities~~:
Article 2(2), point (a)(i)					
G	107	(i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I;	(i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I;	(i) ***providers of*** public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I;	(i) ***providers of*** public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I; Text Origin: Council Mandate

	Article 2(2), point (a)(ii)				
G	108	(ii) trust service providers referred to point 8 of Annex I;	(ii) trust service providers referred to point 8 of Annex I;	(ii) ***qualified*** trust service providers referred to ***in*** point ~~8~~***XX*** of Annex I;	(ii) trust service providers referred to point 8 of Annex ~~I;~~ distinction to be made in 2bis if agreed by EP
	Article 2(2), point (a)(iia)				
G	108a			***iii non-qualified trust service providers referred to in point XX of Annex I;***	
	Article 2(2), point (a)(iii)				
G	109	(iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;	(iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;	(~~iii~~***iv***) top–level domain name registries ~~*and domain name system (DNS) service providers*~~ referred to in point 8 of Annex I;	(iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;
	Article 2(2), point (b)				
R	110	(b) the entity is a public administration entity as defined in point 23 of Article 4;	(b) the entity is a public administration entity as defined in point 23 of Article 4;	~~*(b) the entity is a public administration entity as defined in point 23 of Article 4;*~~	Public Administration - political
	Article 2(2), point (c)				
G	111	(c) the entity is the sole provider of a service in a Member State;	(c) the entity is the sole provider of a service in a Member State;	(c) the entity is the sole provider ***in a Member State of a service***	(c) the entity is the sole provider ***in a Member State of a service***

				which is essential for the maintenance of critical societal or economic activities ~~*of a service in a Member State*~~;	***which is essential for the maintenance of critical societal or economic activities*** ~~*of a service in a Member State*~~; Text Origin: Council Mandate
Article 2(2), point (d)					
G	112	(d) a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health;	(d) a ~~*potential*~~ disruption of the service provided by the entity could have an impact on public safety, public security or public health;	(d) a potential disruption of the service provided by the entity could have ~~*an*~~***a significant*** impact on public safety, public security or public health;	(d) a ~~*potential*~~ disruption of the service provided by the entity could have ~~*an*~~***a significant*** impact on public safety, public security or public health; Text Origin: Council Mandate
Article 2(2), point (e)					
G	113	(e) a potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;	(e) a ~~*potential*~~ disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;	(e) a potential disruption of the service provided by the entity could induce ***a significant*** systemic risks, in particular for the sectors where such disruption could have a cross-border impact;	(e) a ~~*potential*~~ disruption of the service provided by the entity could induce ***a significant*** systemic risks, in particular for the sectors where such disruption could have a cross-border impact; Text Origin: Council Mandate
Article 2(2), point (f)					
G	114	(f) the entity is critical because of its specific importance at regional or national level for the particular	(f) the entity is critical because of its specific importance at regional or national level for the particular	~~*(f) the entity is critical because of its specific importance at regional or national level for the particular*~~	(f) the entity is critical because of its specific importance at regional or national level for the particular

		sector or type of service, or for other interdependent sectors in the Member State;	sector or type of service, or for other interdependent sectors in the Member State;	~~sector or type of service, or for other interdependent sectors in the Member State;~~	sector or type of service, or for other interdependent sectors in the Member State; Text Origin: EP Mandate
	Article 2(2), point (g)				
Y	115	(g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council[1] [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive. _____ 1. [insert the full title and OJ publication reference when known]	(g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council[1] [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive. _____ 1. [insert the full title and OJ publication reference when known]	(g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council[1] [Resilience of Critical Entities Directive], ***[***or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive***]***. _____ 1. [insert the full title and OJ publication reference when known]	(g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council[1] [Resilience of Critical Entities Directive], ***[***or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive***]***. _____ 1. [insert the full title and OJ publication reference when known] to be aligned with the CER directive Text Origin: Council Mandate
	Article 2(2), first paragraph -a				
R	115a			***2a Regardless of their size, this Directive also applies to public administration entities of central governments recognised as such in a Member State in accordance with national law and referred to in point 9 of Annex I. Member***	Council will provide wording to balance their suggestion on art 5.

				States may establish that this Directive also applies to public administration entities at regional and local levels.		
Article 2(2), first paragraph						
G	116	Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.	~~*Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.*~~	~~*Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.*~~	Deleted	G
Article 2(2), first paragraph a						
G	116a		***By ... [6 months after the transposition deadline], Member States shall establish a list of essential and important entities, including the entities referred to in paragraph 1 and the entities identified pursuant to paragraph 2, points (b) to (f) and Article 24 (1). Member States shall review and, where appropriate update, that list, on a regular basis, and at least every two years thereafter.***		Deleted, included in new Art 2a	G
Article 2(2), first paragraph b						

G	116b		***Member States shall ensure that essential and important entities submit at least the following information to competent authorities:*** ***(a) the name of the entity;*** ***(b) address and up-to-date contact details, including email addresses, IP ranges, telephone numbers; and*** ***(c) the relevant sector(s) and subsector(s) referred to in Annexes I and II.*** ***The essential and important entities shall notify any changes to the details submitted pursuant to the first subparagraph without delay, and, in any event, within two weeks from the date on which the change takes effect. To that end, the Commission, with the assistance of ENISA, shall without undue delay issue guidelines and templates regarding the obligations set out in this paragraph.***		Deleted, included in new Art 2a	G
	Article 2(2), first paragraph c					
G	116c		***By …[6 months after the transposition deadline] and every two years thereafter, Member States shall notify:***		Deleted, included in new Art 2a	G

			(a) the Commission and the Cooperation Group of the number of all essential and important entities identified for each sector and subsector referred to in Annexes I and II, and (b) the Commission, of the names of the entities identified pursuant to paragraph 2, points (b) to (f).			
	Article 2(3)					
G	117	3. This Directive is without prejudice to the competences of Member States concerning the maintenance of public security, defence and national security in compliance with Union law.	3. This Directive is without prejudice to the competences of Member States concerning the maintenance of public security, defence and national security in compliance with Union law.	3. This Directive is without prejudice to the ~~*competences of Member States concerning the maintenance of public security, defence and national security in compliance with Union law*~~***Member States' responsibilities to safeguard national security or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order***.	3. This Directive is without prejudice to the ~~*competences of Member States concerning the maintenance of public security, defence and national security in compliance with Union law*~~***Member States' responsibilities to safeguard national security or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order***. Commission compromise proposal - Exclusion clause package	G
	Article 2(3a), introductory part					
Y	117a			***3a. (1) This Directive does not***	***3a. This Directive does not apply***	Y

				apply to:	***to public administration entities that predominantly carry out activities in the areas of defence, national security, public security, or law enforcement, including the investigation, detection and prosecution of criminal offences.*** Commission compromise proposal - Exclusion clause package - "predominantly" to be sorted out - PSY proposal: "predominantly" to be taken out and addition of "their activities" + recital 6a
Article 2(3a), point (a), introductory part					
Y	117b			***(a) entities that fall outside the scope of Union law and in any event all entities that mainly carry out activities in the areas of defence, national security, public security or law enforcement regardless of which entity is carrying out those activities and whether it is a public entity or a private entity, without prejudice to point (2);***	***3b. Member States may decide that specific essential and important entities which carry out activities in the areas of defence, national security or law enforcement, including activities relating to the investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in paragraph 3a are not obliged to comply with the obligations laid down in Article 18 or Article 20 as regards those activities or those services. In such case, the supervision and***

					enforcement measures referred to in Chapter VI shall not apply in relation to those specific activities or services. In cases when these essential and important entities exclusively carry out activities or exclusively provide services of the type referred to in this paragraph, Member States may decide for these entities to be also exempted from the notification obligations laid down in Article 2a and Article 25. Commission compromise proposal - Exclusion clause package - "predominantly" to be sorted out. LL: "whose services are provided exclusively to"?
Article 2(3a), point (a)(1), introductory part					
Y	117c			***(b) entities that carry out activities in the areas of the judiciary, parliaments or central banks.***	***(3c) Paragraphs 3a and 3b shall not apply when entities act as trust service providers referred to in Annex I, point 8.*** Commission compromise proposal - Exclusion clause package Council to check 'trust service providers'
Article 2(3a), point (a)(1)(i), introductory part					

Y	117d			***(2) Where public administration entities carry out activities in these areas only as part of their overall activities, they shall be excluded in their entirety from the scope of this Directive.***	***(3d) This Directive does not apply to entities which Member State have exempted from the scope of Regulation (EU) XXXX/XXXX of the European Parliament and of the Council [the DORA Regulation] in accordance with Article 2 paragraph 4 of that Regulation.*** Commission compromise proposal - Exclusion clause package	Y
	Article 2(3a), point (a)(1)(i), first indent					
Y	117e				***(3e) The obligations laid down in this Directive do not entail the supply of information the disclosure of which is contrary to the Member States' essential interests of national security, public security or defence.***	Y
	Article 2(3b), introductory part					
Y	117f			***3aa. This Directive does not apply to:***	***(3f) This Directive is without prejudice to Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC.***	Y

					Commission compromise proposal - Exclusion clause package
	Article 2(3b), point (a)				
Y	117g			***(i) activities of entities which fall outside the scope of Union law and in any event all activities concerning national security or defence, regardless of which entity is carrying out those activities and whether it is a public entity or a private entity;***	Deleted
	Article 2(3b), point (b)				
Y	117h			***(ii) activities of entities in the judiciary, the parliaments, central banks and in the area of public security, including public administration entities carrying out law enforcement activities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.***	Deleted
	Article 2(3c)				
Y	117i			***3aaa. The obligations laid down in this Directive do not entail the***	Deleted

				supply of information the disclosure of which is contrary to the Member States' essential interests of national security, public security or defence.		
	Article 2(3d)					
Y	117j			***3aaaa. This Directive is without prejudice to Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC.***	Deleted	Y
	Article 2(3e)					
Y	117k			***3b. This Directive does not apply to entities which are exempted from the Regulation (EU) XXXX/XXXX of the European Parliament and of the Council [the DORA Regulation] in accordance with Art 2 para 4 of the DORA Regulation.***	Deleted	Y
	Article 2(4)					
G	118	4. This Directive applies without prejudice to Council Directive 2008/114/EC[1] and Directives 2011/93/EU[2] and 2013/40/EU[3] of	4. This Directive applies without prejudice to Council Directive 2008/114/EC[1] and Directives 2011/93/EU[2] ~~*and*~~, 2013/40/EU[3]	4. This Directive applies without prejudice to ~~*Council Directive 2008/114/EC[4] and*~~ Directives 2011/93/EU[21] and 2013/40/EU[32] of	4. This Directive applies without prejudice to Council Directive 2008/114/EC[1] and Directives 2011/93/EU[2] ~~*and*~~, 2013/40/EU[3]	G

		the European Parliament and of the Council. _____ 1. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75). 2. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1). 3. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).	***and 2002/58/EC[4]*** of the European Parliament and of the Council. _____ 1. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75). 2. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1). 3. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8). ***4. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).***	the European Parliament and of the Council. _____ 1. ~~Council~~ Directive ~~2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75)~~***2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1)***. 2. Directive ~~2011/93/EU~~***2013/40/EU*** of the European Parliament and of the Council of ~~13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography,~~***12 August 2013 on attacks against information systems*** and replacing Council Framework Decisio~~n 2004/68/JHA (OJ L 335, 17.12.2011, p. 1)~~***n 2005/222/JHA (OJ L 218, 14.8.2013, p. 8)***. ~~3. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).~~	***and 2002/58/EC[4]*** of the European Parliament and of the Council. _____ 1. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75). 2. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1). 3. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8). ***4. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).*** Lawyer Linguists to look at it in relation to CER Text Origin: EP Mandate
Article 2(5)					
G	119	5. Without prejudice to Article	5. Without prejudice to Article	5. Without prejudice to Article	5. Without prejudice to Article G

		346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities.	346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities.	346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities ***according to this Directive*** only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities.	346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities ***according to this Directive*** only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities. Text Origin: Council Mandate
Article 2(6)					
G	120	6. Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive,	6. Where provisions of sector–specific acts of Union law require essential or important entities ~~either~~ to adopt cybersecurity risk management measures or to notify incidents ~~or significant cyber threats~~, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive,	~~6. Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions~~	~~6. Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions~~

		including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.	including the provision on supervision and enforcement laid down in Chapter VI, shall not apply. ***The Commission shall, without undue delay, issue guidelines in relation to the implementation of the sector–specific acts of Union law in order to ensure that cybersecurity requirements established by this Directive are fulfilled by those acts and that there is no overlap or legal uncertainty. When preparing those guidelines, the Commission shall take into account the best practices and expertise of ENISA and the Cooperation Group.***	~~*of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.*~~	~~*of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply.*~~ Deleted - covered by line 120ab Text Origin: EP Mandate
	Article 2(6a)				
˅	120a		***6a. Essential and important entities, CSIRTs and providers of security technologies and services, shall process personal data, to the extent strictly necessary and proportionate for the purposes of cybersecurity and network and information security, to meet the obligations set out in this Directive. That processing of personal data under this Directive shall be carried out in compliance with Regulation (EU) 2016/679,***		***6a. Essential and important entities, CSIRTs and competent authorities, to the extent necessary for the purposes of this Directive, shall process personal data in compliance with Regulation (EU) 2016/679.*** Text Origin: EP Mandate

			in particular Article 6 thereof.		
Article 2(6b)					
Y	120b		***6b. The processing of personal data pursuant to this Directive by providers of public electronic communications networks or providers of publicly available electronic communications referred to in Annex I, point 8, shall be carried out in accordance with Directive 2002/58/EC.***		***6b. The processing of personal data pursuant to this Directive by providers of public electronic communications networks or providers of publicly available electronic communications referred to in Annex I, point 8, shall be carried out in accordance with Directive 2002/58/EC.*** COM proposal: deletion Text Origin: EP Mandate
Article 2a					
	120c			***Article 2bis*** ***Essential and important entities***	***Article 2bis*** ***Essential and important entities*** Text Origin: Council Mandate
Article 2a(1), introductory part					
	120d			***1. Of the entities to which this Directive applies, the following shall be considered essential:***	***1. For the purposes of this Directive, essential entities shall be considered all entities of the type listed in Annex I which exceed the ceilings for medium-sized enterprises as well as the***

				following entities:
Article 2a(1), point (a)				
120e			***(i) entities of a type provided for in points 1 to 8a and 10 of Annex I to this Directive which exceed the ceilings for medium-sized enterprises as defined in Commission Recommendation 2003/361/EC;***	***(a) qualified trust service providers and top-level domain name registries as well as DNS service providers referred to in Article 2(2)(b) and 2(2)(d);*** Council to check
Article 2a(1), point (b)				
120f			***(ii) medium-sized entities referred to in Article 2(2), points (a) (i);***	***(b) providers of public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I meeting the ceiling for medium-sized enterprises;***
Article 2a(1), point (c)				
120g			***(iii) entities referred to in Article 2(2), points (a) (ii) and (iv) of this Directive, irrespective of the size;***	***(c) public administration entities referred to in Article 2(2)(e);***
Article 2a(1), point (d)				
120h			***(iv) entities referred to in Article***	***(d) any other entities of the types***

			2(2) point (g) and Article 2(2a) of this Directive, irrespective of the size;	***listed in Annex I and Annex II established by a Member State on the basis of national risk assessments following the criteria laid down in Article 2(2)(c) to (f);***
Article 2a(1), point (e)				
120i			***(v) if established by the Member States, entities which the Member States identified before the entry into force of this Directive as operators of essential services in accordance with Directive (EU) 2016/1148 or national law;***	***(e) entities identified as a critical entity pursuant to Directive (EU) X/X of the European Parliament and of the Council [Resilience of Critical Entities Directive], referred to in Article 2(2)(j);***
Article 2a(1), point (f)				
120j				***(f) if established by the Member States, entities which the Member States identified before the entry into force of this Directive as operators of essential services in accordance with Directive (EU) 2016/1148 or national law;***
Article 2a(1), point (f)				
120k			***(vi) entities which exceed the ceilings for medium-sized enterprises as defined in Commission Recommendation***	***(2) For the purpose of this Directive, all entities which do not qualify as essential pursuant to paragraph 1 shall be considered***

			2003/361/EC of the type provided for in Annex II that Member States determine that are essential on the basis of criteria referred to in Article 2(2), points (c) to (e);	***important entities.***
Article 2a(1), point (g)				
120l			***(vii) medium-sized entities within the meaning of Commission Recommendation 2003/361/EC that Member States determine that are essential on the basis of criteria referred to in Article 2(2), points (c) to (e);***	
Article 2a(1), point (h)				
120m			***(viii) micro or small-sized entities within the meaning of Commission Recommendation 2003/361/EC provided for in paragraph (2), point (a) (i) or identified pursuant to paragraph (2), points (c) to (e) of this Article that Member States determine that are essential on the basis of national risk assessments.***	
Article 2a(2), introductory part				
120n			***2. The entities to which this***	

			Directive applies, the following shall be considered important entities:	
Article 2a(2), point (a)				
120o			***(i) entities of a type provided for in Annex I to this Directive which qualify as medium-sized enterprises within the meaning of Commission Recommendation 2003/361/EC and entities of the type provided for in Annex II which meet or exceed the ceilings for medium-sized enterprises within the meaning of Commission Recommendation 2003/361/EC[1];*** ***1. Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition off micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).***	
Article 2a(2), point (b)				
120p			***(ii) entities referred to in Article 2(2) point (iii) of this Directive, irrespective of the size;***	
Article 2a(2), point (c)				
120q				

			(iii) small and micro entities referred to in Article 2(2) (a) (i);	
Article 2a(2), point (d)				
120r			***(iv) small and micro entities that Member States determine that are important entities on the basis of Article 2(2)(c) to (e).***	
Article 2b				
120s			***Article 2a Notification mechanisms***	***Article 2a Notification mechanisms*** new title tbc Text Origin: Council Mandate
Article 2a(1)				
120t			***1. Member States may establish national mechanism for self-notification that require all entities under the scope of this Directive to submit at least their name, address, contact details, the sector in which they operate or type of service that they provide and, where applicable, the list of Member States where they provide services subject to this Directive,***	***1. By ... [6 months after the transposition deadline], Member States shall establish a list of essential and important entities, including the entities referred to in Article 2 (1), Article 2 (2), points (a) and (g) and the entities identified pursuant to Article 2 (2), points (b) to (f) and Article 24 (1). Member States shall review and, where appropriate, update***

				to the competent authorities under this Directive or bodies designated for this purpose by the Member States.	***that list on a regular basis and at least every two years thereafter.***
Article 2a(2)					
G	120u			***2. Member States shall submit to the Commission in relation to the entities that they identified pursuant to Article 2(2) points (b) to (e), at least relevant information on the number of identified entities, the sector they belong to or type of service they provide as per the Annexes, and the specific provision(s) of Article 2(2) based on which they were identified by [12 months after the transposition deadline of this Directive]. Member States shall review this information on a regular basis, and at least every two years thereafter and, where appropriate, update it.***	***2. For the purpose of establishing the list referred to in paragraph 1, Member States shall require that the essential and important entities submit at least the following information to competent authorities:*** ***(a) the name of the entity;*** ***(b) address and up-to-date contact details, including email addresses, IP ranges, telephone numbers;*** ***(c) the relevant sector(s) and subsector(s) referred to in Annexes I and II; and*** ***(d) where applicable, the list of Member States where they provide services subject to this Directive*** ***The essential and important entities shall notify any changes to the details submitted pursuant to the first subparagraph without delay, and, in any event, within***

					two weeks from the date on which the change takes effect. To that end, the Commission, with the assistance of ENISA, shall without undue delay issue guidelines and templates regarding the obligations set out in this paragraph.
	Article 2b(3)				
G	120v				***3. For the purpose of establishing and updating the list referred to in paragraph 1, Member States may establish national mechanism for self-identification.***
	Article 2b(4)				
R	120w				***4. By …[6 months after the transposition deadline] and every two years thereafter, Member States shall notify:*** ***(a) the Commission and the Cooperation Group of the number of all essential and important entities identified for each sector and subsector referred to in the Annexes, and*** ***(b) the Commission upon request, of the names of the entities***

					identified, and the specific provision(s) based on which they were identified, pursuant to paragraph 2, points (b) to (f).
	Article 2b				
G	120x			***Article 2b*** ***Sector-specific Union acts***	***Article 2b*** ***Sector-specific Union acts*** Text Origin: Council Mandate
	Article 2b(1)				
G	120y			***1. Where sector–specific Union legal acts require essential or important entities to adopt cybersecurity risk management measures or to notify significant incidents or cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VI, shall not apply to such entities. If sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this***	***1. Where sector–specific Union legal acts require essential or important entities to adopt cybersecurity risk management measures or to notify significant incidents, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VI, shall not apply to such entities. If sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this***

				Directive shall continue to apply to the entities not covered by those sector-specific provisions.	***Directive shall continue to apply to the entities not covered by those sector-specific provisions.*** PCY recital on cyber threats to be added
Article 2b(2), introductory part					
G	120z			***2. The requirements referred in paragraph 1 of this Article shall be considered equivalent in effect to the obligations laid down in this Directive if the respective sector specific Union act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the competent authorities under this Directive or the designated CSIRTs and if:***	***2. The requirements referred in paragraph 1 of this Article shall be considered equivalent in effect to the obligations laid down in this Directive if :***
Article 2b(2), point (a)					
G	120aa			***(a) cybersecurity risk management measures, are at least equivalent in effect to those laid down in Article 18 (1) and (2) of this Directive; or***	***(a) cybersecurity risk management measures, are at least equivalent in effect to those laid down in Article 18 (1) and (2) of this Directive; or*** Text Origin: Council Mandate
Article 2b(2), point (b)					

G	120ab			***(b) requirements to notify significant incidents are at least equivalent in effect to those laid down in Article 20 (1) to (6).***	***(b) the sector specific Union legal act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the competent authorities under this Directive or the designated CSIRTs and if requirements to notify significant incidents are at least equivalent in effect to those laid down in Article 20 (1) to (6).*** To check alignment with DORA + COM to draft recital on immediate access	G
	Article 2b(3)				
G	120ac			***3. The Commission shall periodically review the application of the equivalent effect requirements provided for in paragraphs 1 and 2 of this Article in relation to sector-specific provisions of Union legal acts. The Commission shall consult the Cooperation Group and ENISA when preparing those periodical reviews.***	***3. The Commission shall within six months after the entry into force of this Directive, issue guidelines clarifying the application of paragraphs 1 and 2. The Commission shall review the guidelines on a regular basis. When preparing those guidelines, the Commission shall take into account the views of the Cooperation Group and ENISA.***	G
	Article 3				
G	121	Article 3	Article 3	Article 3	Article 3	G

		Minimum harmonisation	Minimum harmonisation	Minimum harmonisation	Minimum harmonisation Text Origin: Commission Proposal + Annexes
	Article 3, first paragraph				
G	122	Without prejudice to their other obligations under Union law, Member States may, in accordance with this Directive, adopt or maintain provisions ensuring a higher level of cybersecurity.	Without prejudice to their other obligations under Union law, Member States may, in accordance with this Directive, adopt or maintain provisions ensuring a higher level of cybersecurity.	Without prejudice to their other obligations under Union law, Member States may, ~~*in accordance with this Directive,*~~ adopt or maintain provisions ensuring a higher level of cybersecurity ***in the areas covered by this Directive***.	~~*Without prejudice to their other obligations under Union law, Member States may, in accordance with this Directive, adopt or maintain*~~***This Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such*** provisions ~~*ensuring a higher level of cybersecurity*~~***are consistent with their obligations under Union law***.
	Article 4				
G	123	Article 4 Definitions	Article 4 Definitions	Article 4 Definitions	Article 4 Definitions Text Origin: Commission Proposal + Annexes
	Article 4, first paragraph, introductory part				
G	124	For the purposes of this Directive, the following definitions apply:	For the purposes of this Directive, the following definitions apply:	For the purposes of this Directive, the following definitions apply:	For the purposes of this Directive, the following definitions apply:

					Text Origin: Commission Proposal + Annexes
Article 4, first paragraph, point (1), introductory part					
G	125	(1) ‘network and information system’ means:	(1) ‘network and information system’ means:	(1) ‘network and information system’ means:	(1) ‘network and information system’ means: Text Origin: Commission Proposal + Annexes
Article 4, first paragraph, point (1)(a)					
G	126	(a) an electronic communications network within the meaning of Article 2(1) of Directive (EU) 2018/1972;	(a) an electronic communications network within the meaning of Article 2(1) of Directive (EU) 2018/1972;	(a) an electronic communications network within the meaning of Article 2(1) of Directive (EU) 2018/1972;	(a) an electronic communications network within the meaning of Article 2(1) of Directive (EU) 2018/1972; Text Origin: Commission Proposal + Annexes
Article 4, first paragraph, point (1)(b)					
G	127	(b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data;	(b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data;	(b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data;	(b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; Text Origin: Commission Proposal + Annexes
Article 4, first paragraph, point (1)(c)					

G	128	(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;	(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;	(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;	(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance; Text Origin: Commission Proposal + Annexes
	Article 4, first paragraph, point (2)				
G	129	(2) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;	(2) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;	(2) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any ~~action that compromises~~***event that may compromise*** the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or ***of*** the ~~related~~ services offered by, or accessible via, those network**,** and information systems;	(2) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any ~~action that compromises~~***event that may compromise*** the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or ***of*** the ~~related~~ services offered by, or accessible via, those network**,** and information systems; Text Origin: Council Mandate
	Article 4, first paragraph, point (2a)				
G	129a			***(2a) 'electronic communications services' means electronic communications services within***	in 155b included

				the meaning of Article 2(4) of Directive (EU) 2018/1972;		
	Article 4, first paragraph, point (3)					
G	130	(3) 'cybersecurity' means cybersecurity within the meaning of Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council[1]; 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 L 151, 7.6.2019, p.15).	(3) 'cybersecurity' means cybersecurity within the meaning of Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council[1]; 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 L 151, 7.6.2019, p.15).	(3) 'cybersecurity' means cybersecurity within the meaning of Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council[1]; 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 L 151, 7.6.2019, p.15).	(3) 'cybersecurity' means cybersecurity within the meaning of Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council[1]; 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 L 151, 7.6.2019, p.15). Text Origin: Commission Proposal + Annexes	G
	Article 4, first paragraph, point (4)					
G	131	(4) 'national strategy on cybersecurity' means a coherent framework of a Member State providing strategic objectives and priorities on the security of network and information systems in that Member State;	(4) 'national strategy on cybersecurity' means a coherent framework of a Member State providing strategic objectives and priorities on the security of network and information systems in that Member State;	(4) 'national ~~strategy on~~ cybersecurity~~'~~ ***strategy*** means a coherent framework of a Member State providing ***a governance to achieve*** strategic objectives and priorities ~~on the security of network and information systems~~***in the area ofcybersecurity*** in that Member State;	(4) 'national ~~strategy on~~ cybersecurity~~'~~ ***strategy*** means a coherent framework of a Member State providing strategic objectives and priorities ~~on the security of network and information systems~~***in the area of cybersecurity and the governance to achieve them*** in that Member State;	G

Article 4, first paragraph, point (4a)					
G	131a		***(4a) 'near miss' means an event which could have compromised the availability, authenticity, integrity or confidentiality of data, or could have caused harm, but was successfully prevented from producing their negative impact;***		***(4a) 'near miss' means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but was successfully prevented from transpiring or did not materialise;*** G
Article 4, first paragraph, point (5)					
G	132	(5) 'incident' means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems;	(5) 'incident' means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems;	(5) 'incident' means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the ~~*related*~~ services offered by, or accessible via, network and information systems;	(5) 'incident' means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the ~~*related*~~ services offered by, or accessible via, network and information systems; Text Origin: Council Mandate G
Article 4, first paragraph, point (5a)					
G	132a			***(5a) 'large-scale cybersecurity incident' means an incident with a significant impact on at least***	***(5a) 'large-scale cybersecurity incident' means an incident whose disruption exceeds a*** G

				two Member States or whose disruption exceeds a Member State's capacity to respond to it.	***Member State's capacity to respond to it or with a significant impact on at least two Member States.***
Article 4, first paragraph, point (6)					
G	133	(6) 'incident handling' means all actions and procedures aiming at detection, analysis and containment of and a response to an incident;	(6) 'incident handling' means all actions and procedures aiming at ***prevention,*** detection, analysis**,** and containment of and a response to an incident;	(6) 'incident handling' means all actions and procedures aiming at detection, analysis and containment of and a response to an incident;	(6) 'incident handling' means all actions and procedures aiming at ***prevention,*** detection, analysis**,** and containment of ~~and a~~**,** response to**,** ***and recovery from*** an incident; Text Origin: EP Mandate
Article 4, first paragraph, point (6a)					
G	133a			***(6a) 'risk' means the potential for loss or disruption caused by an incident and shall be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of said incident.***	***(6a)*** included in 134 b
Article 4, first paragraph, point (7)					
G	134	(7) 'cyber threat' means a cyber threat within the meaning Article 2(8) of Regulation (EU) 2019/881;	(7) 'cyber threat' means a cyber threat within the meaning Article 2(8) of Regulation (EU) 2019/881;	(7) 'cyber threat' means a cyber threat within the meaning Article 2(8) of Regulation (EU) 2019/881;	(7) 'cyber threat' means a cyber threat within the meaning Article 2(8) of Regulation (EU) 2019/881; Text Origin: Commission Proposal + Annexes

	Article 4, first paragraph, point (7a)				
G	134a			***(7a) 'significant cyber threat' means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to severely impact the network and information systems of an entity or its users by causing considerable material or non-material losses;***	***(7a) 'significant cyber threat' means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to severely impact the network and information systems of an entity or its users by causing considerable material or non-material losses;*** Text Origin: Council Mandate
	Article 4, first paragraph, point (7a)				
G	134b		***(7a) 'risk' means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident;***		***(7a) 'risk' means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident;*** Text Origin: EP Mandate
	Article 4, first paragraph, point (8)				
G	135	(8) 'vulnerability' means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a cyber	(8) 'vulnerability' means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a cyber	(8) 'vulnerability' means a weakness, susceptibility or flaw of an ~~*asset, system, process or control*~~ ***ICT asset or a system*** that can be	(8) 'vulnerability' means a weakness, susceptibility or flaw of ~~*an asset, system, process or control*~~***ICT products or ICT***

		threat;	threat;	exploited by a cyber threat;	***services*** that can be exploited by a cyber threat;	
Article 4, first paragraph, point (8a)						
G	135a			***(8a) 'near misses' means an event that could potentially have caused harm to the network and information systems of an entity or its users, but was successfully prevented from fully transpiring;***	included in row 131a	G
Article 4, first paragraph, point (9)						
G	136	(9) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of i) a DNS service provider, a top-level domain (TLD) name registry, a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point 6 of Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive;	(9) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of i) a DNS service provider, a top-level domain (TLD) name registry, a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point 6 of Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive;	(9) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of i) a DNS service provider, a top-level domain (TLD) name registry, a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point 6 of Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive;	(9) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of i) a DNS service provider, a top-level domain (TLD) name registry, a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point 6 of Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive;	G

					Text Origin: Commission Proposal + Annexes	
Article 4, first paragraph, point (10)						
G	137	(10) ‘standard’ means a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[1]; ______ 1. Regulation (EU) No 1025/2012 of the European Parliament and of the Council 25 October 2012 on European standardization, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316,14.11.2012,p.12).	(10) ‘standard’ means a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[1]; ______ 1. Regulation (EU) No 1025/2012 of the European Parliament and of the Council 25 October 2012 on European standardization, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316,14.11.2012,p.12).	(10) ‘standard’ means a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[1]; ______ 1. Regulation (EU) No 1025/2012 of the European Parliament and of the Council 25 October 2012 on European standardization, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316,14.11.2012,p.12).	(10) ‘standard’ means a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[1]; ______ 1. Regulation (EU) No 1025/2012 of the European Parliament and of the Council 25 October 2012 on European standardization, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316,14.11.2012,p.12). Text Origin: Commission Proposal + Annexes	G
Article 4, first paragraph, point (11)						
G	138	(11) ‘technical specification’ means a technical specification within the meaning of Article 2(4) of Regulation (EU) No 1025/2012;	(11) ‘technical specification’ means a technical specification ~~within the meaning of Article 2(4)~~***as defined in Article 2, point (20)*** of Regulation (EU) ~~No~~	(11) ‘technical specification’ means a technical specification within the meaning of Article 2(4) of Regulation (EU) No 1025/2012;	(11) ‘technical specification’ means a technical specification within the meaning of Article 2(4) of Regulation (EU) No 1025/2012; Text Origin: Commission	G

			~~1025/2012~~***No 2019/881***;		Proposal + Annexes	
Article 4, first paragraph, point (12)						
G	139	(12) ‘internet exchange point (IXP)’ means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;	(12) ‘internet exchange point (IXP)’ means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;	(12) ‘internet exchange point (IXP)’ means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;	(12) ‘internet exchange point (IXP)’ means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic; Text Origin: Commission Proposal + Annexes	G
Article 4, first paragraph, point (13)						
G	140	(13) ‘domain name system (DNS)’ means a hierarchical distributed naming system which allows end-users to reach services and resources on the internet;	(13) ‘domain name system (DNS)’ means a hierarchical distributed naming system which ~~allows end-users to reach~~***enables the identification of internet*** services and resources***, allowing end-user***	(13) ‘domain name system (DNS)’ means a hierarchical distributed naming system which allows end-users to reach services and resources on the internet;	(13) ‘domain name system (DNS)’ means a hierarchical distributed naming system which ~~allows end-users to reach~~***enables the identification of internet*** services and resources***, allowing end-user***	G

			devices to utilise ~~*on the*~~ internet ***routing and connectivity services, to reach those services and resources***;		***devices to utilise*** ~~*on the*~~ internet ***routing and connectivity services, to reach those services and resources***; Text Origin: EP Mandate
Article 4, first paragraph, point (14)					
G	141	(14) 'DNS service provider' means an entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers;	(14) 'DNS service provider' means an entity that provides ~~*recursive or authoritative domain name resolution services to internet end-users and other DNS service providers:*~~***:***	(14) 'DNS service provider' means an entity that provides recursive or authoritative domain name resolution services ~~*to internet end-users and other DNS service providers*~~***for third-party usage, with the exception of the root name servers*** ;	(14) 'DNS service provider' means an entity that provides ~~*recursive or authoritative domain name resolution services to internet end-users and other DNS service providers;*~~***:*** Text Origin: EP Mandate
Article 4, first paragraph, point (14a)					
G	141a		***(14a) open and public recursive domain name resolution services to internet end-users; or***		***(a) publicly available recursive domain name resolution services to internet end-users; or***
Article 4, first paragraph, point (14b)					
G	141b		***(14b) authoritative domain name resolution services as a service procurable by third-party entities;***		***(b) authoritative domain name resolution services for third-party usage, with the exception of the root name servers;***
Article 4, first paragraph, point (15)					

G	142	(15) 'top–level domain name registry' means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers;	(15) 'top–level domain name registry' means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers***, irrespective of whether any of those operations are being performed by the entity or are outsourced***;	(15) 'top–level domain name registry' means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers***, while excluding the situations where top-level domain names are used by a registry only for own use***;	(15) 'top–level domain name registry' means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers***, irrespective of whether any of those operations are being performed by the entity or are outsourced, while excluding the situations where top-level domain names are used by a registry only for own use***;	G
	Article 4, first paragraph, point (15a)					
Y	142a		***(15a) 'domain name registration services' means services provided by domain name registries and registrars, privacy or proxy registration service providers, domain brokers or resellers, and any other services which are related to the registration of domain names;***		EC to look at them together with 142b	Y
	Article 4, first paragraph, point (15a)					

G	142b			***(15a) ‘entities providing domain name registration services for the TLD’ means TLD name registries, registrars for the TLDs and agents of registrars such as resellers and providers of proxy services;***	***(15b) ‘entities providing domain name registration services ’ means registrars and agents acting on behalf of registrars, such as privacy or proxy registration service providers or resellers.***	G
	Article 4, first paragraph, point (16)					
G	143	(16) ‘digital service’ means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council [1]; __________ 1. Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L. 241, 17.9.2015, p.1).	(16) ‘digital service’ means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council [1]; __________ 1. Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L. 241, 17.9.2015, p.1).	(16) ‘digital service’ means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council [1]; __________ 1. Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L. 241, 17.9.2015, p.1).	(16) ‘digital service’ means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council [1]; __________ 1. Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L. 241, 17.9.2015, p.1). `Text Origin: Commission Proposal + Annexes`	G
	Article 4, first paragraph, point (16a)					
G	143a			***(16a) ‘trust services’ means trust services within the meaning of Article 3(16) of Regulation (EU) No 910/2014;***	***(16a) ‘trust services’ means trust services within the meaning of Article 3(16) of Regulation (EU) No 910/2014;***	G

					EC and PCY asking for the following addition:(16a) 'trust services' means trust services within the meaning of Article 3(16) of Regulation (EU) No 910/2014; with the exclusion of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants as mentioned in article 2 (2) of Regulation (EU) No 910/2014 Text Origin: Council Mandate
	Article 4, first paragraph, point (16b)				
Y	143b			***(16b) 'qualified trust service provider' means a qualified trust service provider within the meaning of Article 3(20) of Regulation (EU) No 910/2014;***	***(16b) 'qualified trust service provider' means a qualified trust service provider within the meaning of Article 3(20) of Regulation (EU) No 910/2014;*** lawyer linguist check Text Origin: Council Mandate
	Article 4, first paragraph, point (17)				
G	144	(17) 'online marketplace' means a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC of the European Parliament and of the Council[1];	(17) 'online marketplace' means a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC of the European Parliament and of the Council[1]; _____	(17) 'online marketplace' means a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC of the European Parliament and of the Council[1]; _____	(17) 'online marketplace' means a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC of the European Parliament and of the Council[1]; _____

		--- 1. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’) (OJ L 149, 11.6.2005, p. 22).	1. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’) (OJ L 149, 11.6.2005, p. 22).	1. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’) (OJ L 149, 11.6.2005, p. 22).	1. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’) (OJ L 149, 11.6.2005, p. 22). Text Origin: Commission Proposal + Annexes	
	Article 4, first paragraph, point (18)					
G	145	(18) ‘online search engine’ means a digital service within the meaning of Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council[1]; --- 1. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, p. 57).	(18) ‘online search engine’ means a digital service within the meaning of Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council[1]; --- 1. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, p. 57).	(18) ‘online search engine’ means a digital service within the meaning of Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council[1]; --- 1. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, p. 57).	(18) ‘online search engine’ means a digital service within the meaning of Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council[1]; --- 1. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, p. 57). Text Origin: Commission Proposal + Annexes	G
	Article 4, first paragraph, point (19)					
G	146					G

		(19) ‘cloud computing service’ means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable and distributed computing resources;	(19) ‘cloud computing service’ means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable and distributed computing resources;	(19) ‘cloud computing service’ means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable ~~and~~***computing resources, including when those are*** distributed ~~computing resources~~***over several locations***;	(19) ‘cloud computing service’ means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable ~~and~~***computing resources, including when those are*** distributed ~~computing resources~~***over several locations***; Text Origin: Council Mandate
Article 4, first paragraph, point (20)					
G	147	(20) ‘data centre service’ means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;	(20) ‘data centre service’ means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;	(20) ‘data centre service’ means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;	(20) ‘data centre service’ means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control; Text Origin: Commission Proposal + Annexes
Article 4, first paragraph, point (21)					
G	148	(21) ‘content delivery network’	(21) ‘content delivery network’	(21) ‘content delivery network’	(21) ‘content delivery network’

		means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;	means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;	means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;	means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers; Text Origin: Commission Proposal + Annexes
	Article 4, first paragraph, point (22)				
G	149	(22) 'social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, and in particular, via chats, posts, videos and recommendations);	(22) 'social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, and in particular, via chats, posts, videos and recommendations);	(22) 'social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, and in particular, via chats, posts, videos and recommendations);	(22) 'social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, and in particular, via chats, posts, videos and recommendations); Text Origin: Commission Proposal + Annexes
	Article 4, first paragraph, point (23), introductory part				
Y	150	(23) 'public administration entity' means an entity in a Member State that complies with the following criteria:	(23) 'public administration entity' means an entity in a Member State that complies with the following criteria:	(23) -'public administration entity' means, an entity ***recognised as such*** in a Member State ***in accordance with national law,*** that complies with the following criteria:	(23) -'public administration entity' means, an entity ***recognised as such*** in a Member State ***in accordance with national law,*** that complies with the following criteria:

					Text Origin: Council Mandate	
	Article 4, first paragraph, point (23)(a)					
G	151	(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;	(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;	(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;	(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character; Text Origin: Commission Proposal + Annexes	G
	Article 4, first paragraph, point (23)(b)					
G	152	(b) it has legal personality;	(b) it has legal personality;	(b) it has legal personality ***or it is entitled by law to act on behalf of another entity with legal personality***;	(b) it has legal personality ***or it is entitled by law to act on behalf of another entity with legal personality***; 150, 152and 155 to be considered Text Origin: Council Mandate	G
	Article 4, first paragraph, point (23)(c)					
G	153	(c) it is financed, for the most part, by the State, regional authority, or by other bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it has an administrative, managerial or supervisory board, more than half of whose members	(c) it is financed, for the most part, by the State, regional authority, or by other bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it has an administrative, managerial or supervisory board, more than half of whose members	(c) it is financed, for the most part, by the State, regional authority, or by other bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it has an administrative, managerial or supervisory board, more than half of whose members	(c) it is financed, for the most part, by the State, regional authority, or by other bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it has an administrative, managerial or supervisory board, more than half of whose members	G

		are appointed by the State, regional authorities, or by other bodies governed by public law;	are appointed by the State, regional authorities, or by other bodies governed by public law;	are appointed by the State, regional authorities, or by other bodies governed by public law;	are appointed by the State, regional authorities, or by other bodies governed by public law; Text Origin: Commission Proposal + Annexes
	Article 4, first paragraph, point (23)(d)				
G	154	(d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.	(d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.	(d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.	(d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital. Text Origin: Commission Proposal + Annexes
	Article 4, first paragraph, point (23), first paragraph				
G	155	Public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded.	Public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded.		
	Article 4, first paragraph, point (23a)				
G	155a		***(23a) 'public electronic communications network' means a public electronic communications network as***		***(23a) 'public electronic communications network' means a public electronic communications network as***

			defined in Article 2, point (8) of Directive (EU) 2018/1972;		***defined in Article 2, point (8) of Directive (EU) 2018/1972;*** Text Origin: EP Mandate
	Article 4, first paragraph, point (23b)				
G	155b		***(23b) 'electronic communications service' means a electronic communications service as defined in Article 2, point (4) of Directive (EU) 2018/1972;***		***(23b) 'electronic communications service' means a electronic communications service as defined in Article 2, point (4) of Directive (EU) 2018/1972;*** Text Origin: EP Mandate
	Article 4, first paragraph, point (24)				
G	156	(24) 'entity' means any natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;	(24) 'entity' means any natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;	(24) 'entity' means any natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;	(24) 'entity' means any natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations; Text Origin: Commission Proposal + Annexes
	Article 4, first paragraph, point (25)				
R	157	(25) 'essential entity' means any entity of a type referred to as an essential entity in Annex I;	(25) 'essential entity' means any entity of a type referred to as an essential entity in Annex I;	(25) 'essential entity' means any entity of a type ~~*referred to as an essential entity in Annex I*~~***provided***	(25) 'essential entity' means any entity of a type ~~*referred to as an essential entity in Annex I*~~***provided***

				for in the Annex I and designated as 'essential' in accordance with Article 2bis(1);	***for in the Annex I and designated as 'essential' in accordance with Article 2bis(1)***; discussion "proportionality" Text Origin: Council Mandate	
	Article 4, first paragraph, point (26)					
R	158	(26) 'important entity' means any entity of a type referred to as an important entity in Annex II.	(26) 'important entity' means any entity of a type referred to as an important entity in Annex II.	(26) 'important entity' means any entity of ~~*a type referred to as an*~~ ***the type provided for in Annexes I and II and designated '***important ~~*entity in Annex II*~~***' in accordance with Article 2bis(2)***.	(26) 'important entity' means any entity of ~~*a type referred to as an*~~ ***the type provided for in Annexes I and II and designated '***important ~~*entity in Annex II*~~***' in accordance with Article 2bis(2)***. Text Origin: Council Mandate	R
	Article 4, first paragraph, point (26a)					
G	158a			***(26a) 'ICT product' means an ICT product within the meaning of Article 2(12) of Regulation (EU) 2019/881;***	***(26a) 'ICT product' means an ICT product within the meaning of Article 2(12) of Regulation (EU) 2019/881;*** Text Origin: Council Mandate	G
	Article 4, first paragraph, point (26b)					
G	158b			***(26aa) 'ICT service' means an ICT service within the meaning of Article 2(13) of Regulation (EU)***	***(26aa) 'ICT service' means an ICT service within the meaning of Article 2(13) of Regulation (EU)***	G

				2019/881;	***2019/881;*** Text Origin: Council Mandate
Article 4, first paragraph, point (26c)					
G	158c			***(26ab) 'ICT process' means an ICT process within the meaning of Article 2(14) of Regulation (EU) 2019/881.***	***(26ab) 'ICT process' means an ICT process within the meaning of Article 2(14) of Regulation (EU) 2019/881.*** Text Origin: Council Mandate
Article 4, first paragraph, point (26d)					
G	158d			***(26ac) 'Managed service provider' means any entity that delivers services, such as network, application, infrastructure and security, via ongoing and regular management, support and active administration on customers' premises, in their MSP's data centre (hosting), or in a third-party data centre.***	***(26ac) 'Managed service provider' means any entity that delivers services, such as network, application, infrastructure and security, via ongoing and regular management, support and active administration on customers' premises, in their MSP's data centre (hosting), or in a third-party data centre.*** new COM text: means an entity that provides services related to the installation, operation and maintenance of electronic communications networks, applications and any other network and information systems, via ongoing and regular support and active

					administration performed either on customer's premises or remotely; Text Origin: Council Mandate
Article 4, first paragraph, point (26e), introductory part					
G	158e			***(26ad) 'Managed security service provider' means any entity which provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. It also includes the use of high-availability security operation centres (either from their own facilities or from other data centre providers) to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture.***	***(26ad) 'Managed security service provider' means any entity which provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. It also includes the use of high-availability security operation centres (either from their own facilities or from other data centre providers) to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture.*** new COM text: means a MSP that performs or supports cybersecurity risk-management related activities; Text Origin: Council Mandate	G
Article 4, first paragraph, point (26e)(i)					

Y	158f				***(26e) 'Research organisation' means an entity which has as its primary goal to conduct applied research or experimental development in view of the exploitation of the results of that research for commercial purposes. Education institutions are excluded.***	Y
	CHAPTER II					
G	159	CHAPTER II Coordinated cybersecurity regulatory frameworks	CHAPTER II Coordinated cybersecurity regulatory frameworks	CHAPTER II Coordinated cybersecurity regulatory frameworks	CHAPTER II Coordinated cybersecurity regulatory frameworks Text Origin: Commission Proposal + Annexes	G
	Article 5					
G	160	Article 5 National cybersecurity strategy	Article 5 National cybersecurity strategy	Article 5 National cybersecurity strategy	Article 5 National cybersecurity strategy Text Origin: Commission Proposal + Annexes	G
	Article 5(1), introductory part					
G	161	1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives	1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives,	1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives	1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives,	G

		and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:	***the required technical, organisational and financial resources to achieve those objectives, as well as the*** ~~*and*~~ appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:	and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:	***the required resources to achieve those objectives, as well as the*** ~~*and*~~ appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:
Article 5(1), point (a)					
G	162	(a) a definition of objectives and priorities of the Member States' strategy on cybersecurity;	(a) a definition of objectives and priorities of the Member ~~*States'*~~***State's*** strategy on cybersecurity;	(a) ~~*a definition*~~ of objectives and priorities of the Member States' strategy on cybersecurity;	(a) ~~*a definition of*~~ objectives and priorities of the Member ~~*States'*~~***State's*** strategy on cybersecurity ***covering in particular the sectors listed in annexes 1 and 2***;
Article 5(1), point (b)					
G	163	(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 and the roles and responsibilities of public bodies and entities as well as other relevant actors;	(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 ~~*and the roles and responsibilities of public bodies and entities as well as other relevant actors*~~;	(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 and the roles and responsibilities of ~~*public bodies and entities as well as other relevant actors*~~;	(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 ~~*and the roles and responsibilities of public bodies and entities as well as other relevant actors;*~~
Article 5(1), point (ba)					

	163a		***(ba) a framework allocating the roles and responsibilities of public bodies and entities as well as other relevant actors, underpinning the cooperation and coordination, at the national level, between the competent authorities designated pursuant to Articles 7(1) and Article 8(1), the single point of contact designated pursuant to Article 8(3), and the CSIRTs designated pursuant to Article 9;***		***(ba) a governance framework clarifying the roles and responsibilities of relevant actors at national level, underpinning the cooperation and coordination at the national level between the CSIRTs, the single points of contact, and the competent authorities designated under this Directive, as well as the coordination and cooperation between these authorities and competent authorities designated under sector-specific legislation;***
	Article 5(1), point (c)				
	164	(c) an assessment to identify relevant assets and cybersecurity risks in that Member State;	(c) an assessment to identify relevant assets and cybersecurity risks in that Member State;	(c) ~~*an assessment*~~***guidance*** to identify relevant assets and ***assess*** cybersecurity risks in that Member State~~;~~	(c) ~~*an assessment*~~***a mechanism*** to identify relevant assets and ***an assessment of the*** cybersecurity risks in that Member State~~;~~
	Article 5(1), point (d)				
	165	(d) an identification of the measures ensuring preparedness, response and recovery to incidents, including cooperation between the public and private sectors;	(d) an identification of the measures ensuring preparedness, response and recovery to incidents, including cooperation between the public and private sectors;	(d) an identification of the measures ensuring preparedness, response and recovery to incidents, including cooperation between the public and private sectors;	(d) an identification of the measures ensuring preparedness, response and recovery to incidents, including cooperation between the public and private sectors; Text Origin: Commission Proposal + Annexes

Article 5(1), point (e)					
Y	166	(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;	(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy***, including a cybersecurity single point of contact for SMEs that provides support for implementing the specific cybersecurity measures***;	~~(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;~~	(e) ~~a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;~~ Council to make proposal
Article 5(1), point (f)					
G	167	(f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[1] [Resilience of Critical Entities Directive] for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks. _____ 1. [insert the full title and OJ publication reference when known]	(f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[1] [Resilience of Critical Entities Directive]***, both within and between Member States,*** for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks. _____ 1. [insert the full title and OJ publication reference when known]	(f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[1] [Resilience of Critical Entities Directive] for the purposes of information sharing on ***cybersecurity risks, cyber threats and*** incidents ~~and cyber~~***as well as on non-cyber risks,*** threats and ***incidents and*** the exercise of supervisory tasks~~.~~***, as appropriate;*** _____ 1. [insert the full title and OJ publication reference when known]	(f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[1] [Resilience of Critical Entities Directive] for the purposes of information sharing on ***cybersecurity risks, cyber threats and*** incidents ~~and cyber~~***as well as on non-cyber risks,*** threats and ***incidents and*** the exercise of supervisory tasks~~.~~***, as appropriate;*** _____ 1. [insert the full title and OJ publication reference when known]
Article 5(1), point (fa)					

G	167a			***(fa) policy framework for coordination and cooperation between competent authorities under this Directive and competent authorities designated under sector-specific legislation.***	included in 163a	G
Article 5(1), point (fa)						
G	167b		***(fa) an assessment of the general level of cybersecurity awareness among citizens.***		***(fb) a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens***	G
Article 5(2), introductory part						
G	168	2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies:	2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies:	2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies:	2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies: Text Origin: Commission Proposal + Annexes	G
Article 5(2), point (-a)						
G	168a		***(-a) a policy addressing cybersecurity for each sector covered by this Directive;***		deleted	G
Article 5(2), point (a)						

G	169	(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services;	(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services;	(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by ~~essential and important~~ entities for the provision of their services;	(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by ~~essential and important~~ entities for the provision of their services;
	Article 5(2), point (b)				
G	170	(b) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement;	(b) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement***, including encryption requirements and the use of open-source cybersecurity products***;	(b) ~~guidelines~~***a policy*** regarding the inclusion and specification of cybersecurity-related requirements for ICT products and ~~service~~***services*** in public procurement***, including cybersecurity certification***;	(b) ~~guidelines~~***a policy*** regarding the inclusion and specification of cybersecurity-related requirements for ICT products and ~~service~~***services*** in public procurement***, including cybersecurity certification as well as encryption requirements and the use of open-source cybersecurity products***;
	Article 5(2), point (c)				
G	171	(c) a policy to promote and facilitate coordinated vulnerability disclosure within the meaning of Article 6;	(c) a policy to promote and facilitate coordinated vulnerability disclosure within the meaning of Article 6;	(c) a policy ~~to promote and facilitate~~***on management of vulnerabilities, encompassing the promotion and facilitation of voluntary*** coordinated vulnerability disclosure within the meaning of Article ~~6~~***6(1)***;	(c) a policy ~~to promote and facilitate~~***on management of vulnerabilities, encompassing the promotion and facilitation of voluntary*** coordinated vulnerability disclosure within the meaning of Article ~~6~~***6(1)***;
	Article 5(2), point (d)				
G	172				

		(d) a policy related to sustaining the general availability and integrity of the public core of the open internet;	(d) a policy related to sustaining the general availability and integrity of the public core of the open internet***, including cybersecurity of undersea communications cables***;	(d) a policy related to sustaining the general availability***, integrity and confidentiality*** ~~*and integrity*~~ of the public core of the open internet;	(d) a policy related to sustaining the general availability***, integrity and confidentiality*** ~~*and integrity*~~ of the public core of the open internet***, including, where relevant, the (cyber-)security of undersea communication cables***;
	Article 5(2), point (da)				
G	172a		***(da) a policy to promote and support the development and integration of emerging technologies, such as artificial intelligence, in cybersecurity-enhancing tools and applications;***		***(da) a policy to promote the development and integration of relevant advanced technologies aiming to implement of state-of-the-art cybersecurity measures;***
	Article 5(2), point (db)				
G	172b		***(db) a policy to promote the integration of open-source tools and applications;***		deleted
	Article 5(2), point (e)				
G	173	(e) a policy on promoting and developing cybersecurity skills, awareness raising and research and development initiatives;	(e) a policy on promoting and developing cybersecurity skills, awareness raising and research and development initiatives;	(e) a policy on promoting and developing cybersecurity ***education and training,*** skills, awareness raising and research and development initiatives;	(e) a policy on promoting and developing cybersecurity ***education and training,*** skills, awareness raising and research and development initiatives***, as well as guidance on good cyber hygiene prevention practices and controls,***

					aimed at citizens, stakeholders and businesses;
Article 5(2), point (f)					
G	174	(f) a policy on supporting academic and research institutions to develop cybersecurity tools and secure network infrastructure;	(f) a policy on supporting academic and research institutions to develop***, enhance and deploy*** cybersecurity tools and secure network infrastructure;	(f) a policy on supporting academic and research institutions to develop cybersecurity tools and secure network infrastructure;	(f) a policy on supporting academic and research institutions to develop***, enhance and promote the deployment of*** cybersecurity tools and secure network infrastructure;
Article 5(2), point (g)					
G	175	(g) a policy, relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between companies in compliance with Union law;	(g) a policy, relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between companies in compliance with Union law;	(g) a policy, relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between companies in compliance with Union law;	(g) a policy, relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between companies in compliance with Union law; Text Origin: Commission Proposal + Annexes
Article 5(2), point (h)					
G	176	(h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats.	(h) a policy ~~*addressing specific needs of*~~***promoting cybersecurity for*** SMEs, ~~*in particular*~~***including*** those excluded from the scope of this Directive, ~~*in relation to*~~***addressing their specific needs***	(h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to ~~*cybersecurity*~~***cyber***	(h) ***a policy to strengthen the cyber resilience and cyber hygiene baseline of SMEs, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and support***

			and providing easily accessed guidance and support***, including guidelines addressing supply chain challenges faced;*** ~~*in improving their resilience to cybersecurity threats.*~~	threats.	***for their specific needs.*** ~~*a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats.*~~
	Article 5(2), point (ha)				
G	176a		***(ha) a policy to promote cyber hygiene comprising a baseline set of practices and controls and raising the general cybersecurity awareness among citizens of cybersecurity threats and best practices;***		deleted, inserted in 176
	Article 5(2), point (hb)				
Y	176b		***(hb) a policy on promoting active cyber defence;***		***(hb) a policy on promoting active cyber protection;*** Council to check Text Origin: EP Mandate
	Article 5(2), point (hc)				
G	176c		***(hc) a policy to help authorities develop competences and understanding of the security***		deleted, move to a recital (EP to draft)

			considerations needed to design, build and manage connected places;		
Article 5(2), point (hd)					
G	176d		***(hd) a policy specifically addressing the ransomware threat and disrupting the ransomware business model;***		deleted, move to recital (EP to draft) G
Article 5(2), point (he)					
G	176e		***(he) a policy, including relevant procedures and governance frameworks, to support and promote the establishment of cybersecurity PPPs.***		deleted, move to recital G
Article 5(2), point (hf)					
	176f				***(hf) a policy to develop cybersecurity requirements across public administration entities at regional with an equivalent effect to the obligations laid down in this Directive;*** PR proposal in relation to public administrations
Article 5(3)					

G	177	3. Member States shall notify their national cybersecurity strategies to the Commission within three months from their adoption. Member States may exclude specific information from the notification where and to the extent that it is strictly necessary to preserve national security.	3. Member States shall notify their national cybersecurity strategies to the Commission within three months from their adoption. Member States may exclude specific information from the notification where and to the extent that it is ~~*strictly*~~ necessary to preserve national security.	3. Member States shall notify their national cybersecurity strategies to the Commission within three months from their adoption. ***In doing so,*** Member States may exclude ~~*specific information from the notification where and to the extent that it is strictly necessary to preserve*~~ ***elements of the strategy which relate to*** national security.	3. Member States shall notify their national cybersecurity strategies to the Commission within three months from their adoption. ***In doing so,*** Member States may exclude ~~*specific*~~***certain*** information ~~*from the notification where and to the extent that it is strictly necessary to preserve*~~ ***of the strategy which relate to*** national security.	G
Article 5(4)						
G	178	4. Member States shall assess their national cybersecurity strategies at least every four years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon request, in the development of a national strategy and of key performance indicators for the assessment of the strategy.	4. Member States shall assess their national cybersecurity strategies at least every four years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon request, in the development of a national strategy and of key performance indicators for the assessment of the strategy. ***ENISA shall provide guidance to Member States in order to align their already formulated national cybersecurity strategies with the requirements and obligations set out in this Directive.***	4. Member States shall assess their national cybersecurity strategies ***on a regular basis and*** at least every ~~*four*~~***five*** years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon ***their*** request, in the development of a national strategy and of key performance indicators for the assessment of the strategy.	4. Member States shall assess their national cybersecurity strategies ***on a regular basis and*** at least every ~~*four*~~***five*** years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon ***their*** request, in the development ***or the update*** of a national strategy and of key performance indicators for the assessment of the strategy***, in order to align it with the requirements and obligations set out in this Directive***.	G

	Article 6				
G	179	Article 6 Coordinated vulnerability disclosure and a European vulnerability registry	Article 6 Coordinated vulnerability disclosure and a European vulnerability ~~registry~~***database***	Article 6 Coordinated vulnerability disclosure and a European vulnerability registry	Article 6 Coordinated vulnerability disclosure and a European vulnerability ~~registry~~***database*** Text Origin: EP Mandate
	Article 6(1)				
G	180	1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of coordinated vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity and the manufacturer or provider of ICT products or ICT services. Where the reported vulnerability concerns multiple manufacturers or providers of ICT products or ICT services across the Union, the designated CSIRT of each Member State concerned shall cooperate with the CSIRT network.	1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of coordinated vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, ~~where necessary~~***upon the request of the reporting entity***, the interaction between the reporting entity and the manufacturer or provider of ICT products or ICT services. Where the reported vulnerability concerns multiple manufacturers or providers of ICT products or ICT services across the Union, the designated CSIRT of each Member State concerned shall cooperate with the CSIRT network.	1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of coordinated vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity***, the potential vulnerability owner*** and the manufacturer or provider of ICT products or ICT services. ~~Where the reported vulnerability concerns multiple manufacturers or providers of ICT products or ICT services across the Union~~***Any natural or legal person may report, possibly anonymously, a vulnerability referred to in Article 4(8) to the designated CSIRT. The designated CSIRT shall ensure a diligent follow-up of the report***	1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of coordinated vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity and the manufacturer or provider of ***the potentially vulnerable*** ICT products or ICT services ***upon request of either party.*** ***Any natural or legal person may report, possibly anonymously, a vulnerability referred to in Article 4(8) to the designated CSIRT. The designated CSIRT shall ensure a diligent follow-up of the report and the confidentiality of the identity of the person who reports the vulnerability***. Where the

				and the confidentiality of the identity of the person who reports the vulnerability. Where the reported vulnerability could potentially have significant impact on entities in more than one Member State, the designated CSIRT of each Member State concerned shall***, where appropriate,*** cooperate with ***other designated CSIRTs within the CSIRTs*** ~~*the CSIRT*~~ network.	reported vulnerability ~~*concerns multiple manufacturers or providers of ICT products or ICT services across the Union*~~***could potentially have significant impact on entities in more than one Member State***, the designated CSIRT of each Member State concerned shall***, where appropriate,*** cooperate with ***other designated CSIRTs within the CSIRTsnetwork*** ~~*the CSIRT network*~~.
Article 6(2)					
G	181	2. ENISA shall develop and maintain a European vulnerability registry. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties. The registry shall, in particular, include information describing the	2. ENISA shall develop and maintain a European vulnerability ~~*registry*~~***database leveraging the global Common Vulnerabilities and Exposures (CVE)***. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures***, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the database,*** with a view in particular to enabling important and essential entities and their suppliers of network and information systems***, as well as entities which do not fall within the scope of this***	2. ENISA shall develop and maintain a European vulnerability registry***, in consultation with the Cooperation Group***. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register***, on a voluntary basis, publicly known*** vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the	2. ENISA shall develop and maintain***, in consultation with the Cooperation Group,*** a European vulnerability ~~*registry*~~***database***. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures***, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the database,*** with a view in particular to enabling important and essential entities and their suppliers of network and information systems***, as well as entities which do not fall within the scope of this Directive, and their suppliers,*** to	G

	vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.	***Directive, and their suppliers,*** to disclose and register vulnerabilities present in ICT products or ICT services~~, as well as to provide~~***. All interested parties shall be provided*** access to the information on ***the*** vulnerabilities contained in the ~~registry to all interested parties. The registry~~***database that have patches or mitigation measures available. The database*** shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches~~ and, in the~~***. In*** absence of available patches, guidance addressed to users of vulnerable ***ICT*** products and ***ICT*** services as to how the risks resulting from disclosed vulnerabilities may be mitigated ***shall be included in the database***.	registry to all interested parties. The registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance ***issued by national competent authorities or CSIRTs*** addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated. ***ENISA shall ensure that the European vulnerability registry uses secure and resilient communication and information infrastructure.***	disclose and register***, on a voluntary basis, publicly known*** vulnerabilities present in ICT products or ICT services~~, as well as to provide~~***. All interested parties shall be provided*** access to the information on ***the*** vulnerabilities contained in the ~~registry to all interested parties~~***database***~~. The registry~~ ***The database*** shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance ***issued by national competent authorities or CSIRTs*** addressed to users of vulnerable ***ICT*** products and ***ICT*** services as to how the risks resulting from disclosed vulnerabilities may be mitigated.
Article 7					
G 182	Article 7 National cybersecurity crisis management frameworks	Article 7 National cybersecurity crisis management frameworks	Article 7 National cybersecurity crisis management frameworks	Article 7 National cybersecurity crisis management frameworks Text Origin: Commission	G

				Proposal + Annexes	
Article 7(1)					
G	183	1. Each Member State shall designate one or more competent authorities responsible for the management of large-scale incidents and crises. Member States shall ensure that competent authorities have adequate resources to perform, in an effective and efficient manner, the tasks assigned to them.	1. Each Member State shall designate one or more competent authorities responsible for the management of large-scale incidents and crises. Member States shall ensure that competent authorities have adequate resources to perform, in an effective and efficient manner, the tasks assigned to them.	1. Each Member State shall designate one or more competent authorities responsible for the management of large-scale ***cybersecurity*** incidents and crises. Member States shall ensure that competent authorities have adequate resources to perform, in an effective and efficient manner, the tasks assigned to them. ***Member States shall ensure coherence with the existing frameworks for general crisis management.***	1. Each Member State shall designate one or more competent authorities responsible for the management of large-scale ***cybersecurity*** incidents and crises. Member States shall ensure that competent authorities have adequate resources to perform, in an effective and efficient manner, the tasks assigned to them. ***Member States shall ensure coherence with the existing frameworks for general crisis management.***
Article 7(1a)					
G	183a		***1a. Where a Member State designates more than one competent authority referred to in paragraph 1, it shall clearly indicate which of those competent authorities is to serve as the coordinator for the management of large-scale incidents and crises.***	***1a. Where a Member State designates more than one competent authority referred to in paragraph 1, it shall clearly indicate which of those competent authorities is to serve as the coordinator for the management of large-scale incidents and crises.*** Text Origin: EP Mandate	
Article 7(2)					

G	184	2. Each Member State shall identify capabilities, assets and procedures that can be deployed in case of a crisis for the purposes of this Directive.	2. Each Member State shall identify capabilities, assets and procedures that can be deployed in ***the*** case of a crisis for the purposes of this Directive.	2. Each Member State shall identify capabilities, assets and procedures that can be deployed in case of a crisis for the purposes of this Directive.	2. Each Member State shall identify capabilities, assets and procedures that can be deployed in ***the*** case of a crisis for the purposes of this Directive.
	Article 7(3), introductory part				
G	185	3. Each Member State shall adopt a national cybersecurity incident and crisis response plan where objectives and modalities in the management of large-scale cybersecurity incidents and crises are set out. The plan shall lay down, in particular, the following:	3. Each Member State shall adopt a national cybersecurity incident and crisis response plan where objectives and modalities in the management of large-scale cybersecurity incidents and crises are set out. The plan shall lay down, in particular, the following:	3. Each Member State shall adopt a national cybersecurity incident and crisis response plan where objectives and modalities in the management of large-scale cybersecurity incidents and crises are set out. The plan shall lay down, in particular, the following:	3. Each Member State shall adopt a national cybersecurity incident and crisis response plan where objectives and modalities in the management of large-scale cybersecurity incidents and crises are set out. The plan shall lay down, in particular, the following: Text Origin: Commission Proposal + Annexes
	Article 7(3), point (a)				
G	186	(a) objectives of national preparedness measures and activities;	(a) objectives of national preparedness measures and activities;	(a) objectives of national preparedness measures and activities;	(a) objectives of national preparedness measures and activities; Text Origin: Commission Proposal + Annexes
	Article 7(3), point (b)				
G	187	(b) tasks and responsibilities of	(b) tasks and responsibilities of the	(b) tasks and responsibilities of the	(b) tasks and responsibilities of the

		the national competent authorities;	national competent authorities;	national competent authorities;	national competent authorities; Text Origin: Commission Proposal + Annexes
Article 7(3), point (c)					
G	188	(c) crisis management procedures and information exchange channels;	(c) crisis management procedures and information exchange channels;	(c) ***cybersecurity*** crisis management procedures, ***including their integration into the general national crisis management framework*** and information exchange channels;	(c) ***cybersecurity*** crisis management procedures, ***including their integration into the general national crisis management framework*** and information exchange channels;
Article 7(3), point (d)					
G	189	(d) preparedness measures, including exercises and training activities;	(d) preparedness measures, including exercises and training activities;	(d) preparedness measures, including exercises and training activities;	(d) preparedness measures, including exercises and training activities; Text Origin: Commission Proposal + Annexes
Article 7(3), point (e)					
G	190	(e) relevant public and private interested parties and infrastructure involved;	(e) relevant public and private interested parties and infrastructure involved;	(e) relevant public and private ~~interested~~ parties and infrastructure involved;	(e) relevant public and private ~~interested~~ parties and infrastructure involved;
Article 7(3), point (f)					
G	191	(f) national procedures and	(f) national procedures and	(f) national procedures and	

		arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.	arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.	arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.	
Article 7(4)					
R	192	4. Member States shall communicate to the Commission the designation of their competent authorities referred to in paragraph 1 and submit their national cybersecurity incident and crisis response plans as referred to in paragraph 3 within three months from that designation and the adoption of those plans. Member States may exclude specific information from the plan where and to the extent that it is strictly necessary for their national security.	4. Member States shall communicate to the Commission the designation of their competent authorities referred to in paragraph 1 and submit ***to the EU-CyCLONe*** their national cybersecurity incident and crisis response plans as referred to in paragraph 3 within three months from that designation and the adoption of those plans. Member States may exclude specific information from the plan where and to the extent that it is strictly necessary for their national security.	4. Member States shall ~~*communicate to*~~ ***inform*** the Commission ***about*** the designation of their competent authorities referred to in paragraph 1 and submit ***relevant information relating to the requirements of paragraph 3 of this Article about*** their national cybersecurity incident and crisis response plans ~~*as referred to in paragraph 3*~~ within three months from that designation and the adoption of those plans. Member States may exclude specific information ~~*from the plan*~~ where and to the extent that it is ~~*strictly*~~ necessary for their national security***, public security or defence***.	4. Member States shall ~~*communicate to*~~ ***inform*** the Commission ***about*** the designation of their competent authorities referred to in paragraph 1***. They shall submit to the Commission and EU-CyCLONe relevant information relating to the requirements of paragraph 3 of this Article about*** ~~*and submit*~~ their national cybersecurity incident and crisis response plans ~~*as referred to in paragraph 3*~~ within three months from that designation and the adoption of those plans. Member States may exclude specific information ~~*from the plan*~~ where and to the extent that it is ~~*strictly*~~ necessary for their national security. PR compromise text Linked to Art 14

					Text Origin: Council Mandate
Article 8					
G	193	Article 8 National competent authorities and single points of contact	Article 8 National competent authorities and single points of contact	Article 8 National competent authorities and single points of contact	Article 8 National competent authorities and single points of contact Text Origin: Commission Proposal + Annexes
Article 8(1)					
G	194	1. Each Member State shall designate one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VI of this Directive. Member States may designate to that effect an existing authority or existing authorities.	1. Each Member State shall designate one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VI of this Directive. Member States may designate to that effect an existing authority or existing authorities.	1. Each Member State shall designate one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VI of this Directive. Member States may designate to that effect an existing authority or existing authorities.	1. Each Member State shall designate one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VI of this Directive. Member States may designate to that effect an existing authority or existing authorities. Text Origin: Commission Proposal + Annexes
Article 8(2)					
G	195	2. The competent authorities referred to paragraph 1 shall monitor the application of this Directive at national level.	2. The competent authorities referred to paragraph 1 shall monitor the application of this Directive at national level.	2. The competent authorities referred to paragraph 1 shall monitor the application of this Directive at national level.	2. The competent authorities referred to paragraph 1 shall monitor the application of this Directive at national level.

					Text Origin: Commission Proposal + Annexes
Article 8(3)					
G	196	3. Each Member State shall designate one national single point of contact on cybersecurity ('single point of contact'). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact for that Member State.	3. Each Member State shall designate one ***of the competent authorities referred to in paragraph 1 as a*** national single point of contact on cybersecurity ('single point of contact'). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact for that Member State.	3. Each Member State shall designate one national single point of contact on cybersecurity ('single point of contact'). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact for that Member State.	3. Each Member State shall designate one national single point of contact on cybersecurity ('single point of contact'). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact for that Member State. Text Origin: Council Mandate
Article 8(4)					
G	197	4. Each single point of contact shall exercise a liaison function to ensure cross–border cooperation of its Member State's authorities with the relevant authorities in other Member States, as well as to ensure cross-sectorial cooperation with other national competent authorities within its Member State.	4. Each single point of contact shall exercise a liaison function to ensure cross–border cooperation of its Member State's authorities with the relevant authorities in other Member States, ***the Commission and ENISA,*** as well as to ensure cross-sectorial cooperation with other national competent authorities within its Member State.	4. Each single point of contact shall exercise a liaison function to ensure cross–border cooperation of its Member State's authorities with the relevant authorities in other Member States, as well as to ensure cross-sectorial cooperation with other national competent authorities within its Member State.	4. Each single point of contact shall exercise a liaison function to ensure cross–border cooperation of its Member State's authorities with the relevant authorities in other Member States, ***and, where appropriate, the Commission and ENISA,*** as well as to ensure cross-sectorial cooperation with other national competent authorities within its Member State.
Article 8(5)					

G	198	5. Member States shall ensure that the competent authorities referred to in paragraph 1 and the single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group referred to in Article 12.	5. Member States shall ensure that the competent authorities referred to in paragraph 1 and the single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group referred to in Article 12.	5. Member States shall ensure that the competent authorities referred to in paragraph 1 and the single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group referred to in Article 12.	5. Member States shall ensure that the competent authorities referred to in paragraph 1 and the single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group referred to in Article 12. `Text Origin: Commission Proposal + Annexes`	G
	Article 8(6)					
G	199	6. Each Member State shall notify to the Commission, without undue delay, the designation of the competent authority referred to in paragraph 1 and single point of contact referred to in paragraph 3, their tasks, and any subsequent change thereto. Each Member State shall make public their designation. The Commission shall publish the list of the designated single points of contacts.	6. Each Member State shall notify to the Commission, without undue delay, the designation of the competent authority referred to in paragraph 1 and single point of contact referred to in paragraph 3, their tasks, and any subsequent change thereto. Each Member State shall make public their designation. The Commission shall publish the list of the designated single points of contacts.	6. Each Member State shall notify to the Commission, without undue delay, the designation of the competent authority referred to in paragraph 1 and single point of contact referred to in paragraph 3, their tasks, and any subsequent change thereto. Each Member State shall make public their designation. The Commission shall publish the list of the designated single points of contacts.	6. Each Member State shall notify to the Commission, without undue delay, the designation of the competent authority referred to in paragraph 1 and single point of contact referred to in paragraph 3, their tasks, and any subsequent change thereto. Each Member State shall make public their designation. The Commission shall publish the list of the designated single points of contacts. `Text Origin: Commission`	G

					Proposal + Annexes	
	Article 9					
G	200	Article 9 Computer security incident response teams (CSIRTs)	Article 9 Computer security incident response teams (CSIRTs)	Article 9 Computer security incident response teams (CSIRTs)	Article 9 Computer security incident response teams (CSIRTs) Text Origin: Commission Proposal + Annexes	G
	Article 9(1)					
G	201	1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in Article 10(1), covering at least the sectors, subsectors or entities referred to in Annexes I and II, and be responsible for incident handling in accordance with a well–defined process. A CSIRT may be established within a competent authority referred to in Article 8.	1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in Article 10(1), covering at least the sectors, subsectors or entities referred to in Annexes I and II, and be responsible for incident handling in accordance with a well–defined process. A CSIRT may be established within a competent authority referred to in Article 8.	1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in Article 10(1), covering at least the sectors, subsectors or entities referred to in Annexes I and II, and be responsible for incident handling in accordance with a well–defined process. A CSIRT may be established within a competent authority referred to in Article 8.	1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in Article 10(1), covering at least the sectors, subsectors or entities referred to in Annexes I and II, and be responsible for incident handling in accordance with a well–defined process. A CSIRT may be established within a competent authority referred to in Article 8. Text Origin: Commission Proposal + Annexes	G
	Article 9(2)					
G	202	2. Member States shall ensure that each CSIRT has adequate	2. Member States shall ensure that each CSIRT has adequate	2. Member States shall ensure that each CSIRT has adequate	2. Member States shall ensure that each CSIRT has adequate	G

		resources to carry out effectively their tasks as set out in Article 10(2).	resources ***and the technical capabilities necessary*** to carry out effectively their tasks as set out in Article 10(2).	resources to carry out effectively their tasks as set out in Article 10(2). ***When carrying out these tasks, CSIRTs may prioritise the provision of particular services to entities based on a risk-based approach.***	resources ***and the technical capabilities necessary*** to carry out effectively their tasks as set out in Article 10(2). Council text to be added to article 10(2) `Text Origin: EP Mandate`	
Article 9(3)						
G	203	3. Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure to exchange information with essential and important entities and other relevant interested parties. To this end, Member States shall ensure that the CSIRTs contribute to the deployment of secure information sharing tools.	3. Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure to exchange information with essential and important entities and other relevant interested parties. To this end, Member States shall ensure that the CSIRTs contribute to the deployment of secure information sharing tools.	3. Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure to exchange information with essential and important entities and other relevant interested parties. To this end, Member States shall ensure that the CSIRTs contribute to the deployment of secure information sharing tools.	3. Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure to exchange information with essential and important entities and other relevant interested parties. To this end, Member States shall ensure that the CSIRTs contribute to the deployment of secure information sharing tools. `Text Origin: Commission Proposal + Annexes`	G
Article 9(4)						
G	204	4. CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 26 with trusted	4. CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 26 with trusted	4. CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 26 with trusted	4. CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 26 with trusted	G

		sectorial or cross-sectorial communities of essential and important entities.	sectorial or cross-sectorial communities of essential and important entities.	sectorial or cross-sectorial communities of essential and important entities.	sectorial or cross-sectorial communities of essential and important entities. Text Origin: Commission Proposal + Annexes
	Article 9(5)				
G	205	5. CSIRTs shall participate in peer reviews organised in accordance with Article 16.	5. CSIRTs shall participate in peer reviews organised in accordance with Article 16.	5. CSIRTs shall participate in peer***- learnings*** ~~*reviews*~~ organised in accordance with Article 16.	5. CSIRTs shall participate in peer reviews organised in accordance with Article 16. Text Origin: Commission Proposal + Annexes
	Article 9(6)				
G	206	6. Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 13.	6. Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 13.	6. Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 13.	
	Article 9(6a)				
G	206a		***6a. Member States shall ensure the possibility of effective, efficient and secure information exchange on all classification levels between their own CSIRTs and CSIRTs from third countries on the same classification level.***		***6a. CSIRTs may establish cooperation relationships with national CSIRTs of third countries. As part of such cooperation relationships, Member States shall facilitate effective, efficient and secure***

				PUBLIC	***information exchange with CSIRTs of third countries, using relevant information sharing protocols, including the Traffic Light Protocol. CSIRTs may exchange relevant information with CSIRTs of third countries, including personal data in accordance with Union law on data protection.***
Article 9(6b)					
G	206b		***6b. CSIRTs shall, without prejudice to Union law, in particular Regulation (EU) 2016/679, cooperate with CSIRTs or equivalent bodies in candidate countries and in other third countries in the Western Balkans and the Eastern Partnership and, where possible, provide them with cybersecurity assistance.***		***6b. CSIRTs may cooperate with CSIRTs or equivalent bodies in third countries, in particular with an aim to provide them with cybersecurity assistance.***
Article 9(7)					
G	207	7. Member States shall communicate to the Commission without undue delay the CSIRTs designated in accordance with paragraph 1, the CSIRT coordinator designated in accordance with Article 6(1) and	7. Member States shall communicate to the Commission without undue delay the CSIRTs designated in accordance with paragraph 1~~,~~ ***and*** the CSIRT coordinator designated in accordance with Article 6(1)***,***	7. Member States shall communicate to the Commission without undue delay the CSIRTs designated in accordance with paragraph 1, the CSIRT coordinator designated in accordance with Article 6(1) and	7. Member States shall communicate to the Commission without undue delay the CSIRTs designated in accordance with paragraph 1~~,~~ ***and*** the CSIRT coordinator designated in accordance with Article 6(1)***,***

		their respective tasks provided in relation to the entities referred to in Annexes I and II.	***including*** ~~*and*~~ their respective tasks provided in relation to the ~~*entities referred to in Annexes I and II*~~***essential and important entities***.	their respective tasks provided in relation to the entities referred to in Annexes I and II.	***including*** ~~*and*~~ their respective tasks provided in relation to the ~~*entities referred to in Annexes I and II*~~***essential and important entities***. Text Origin: EP Mandate
Article 9(8)					
G	208	8. Member States may request the assistance of ENISA in developing national CSIRTs.	8. Member States may request the assistance of ENISA in developing national CSIRTs.	8. Member States may request the assistance of ENISA in developing national CSIRTs.	8. Member States may request the assistance of ENISA in developing national CSIRTs. Text Origin: Commission Proposal + Annexes
Article 10					
G	209	Article 10 Requirements and tasks of CSIRTs	Article 10 Requirements***, technical capabilities*** and tasks of CSIRTs	Article 10 Requirements and tasks of CSIRTs	Article 10 Requirements***, capabilities*** and tasks of CSIRTs
Article 10(1), introductory part					
G	210	1. CSIRTs shall comply with the following requirements:	1. CSIRTs shall comply with the following requirements:	1. CSIRTs shall comply with the following requirements:	1. CSIRTs shall comply with the following requirements: Text Origin: Commission Proposal + Annexes
Article 10(1), point (a)					

G	211	(a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. CSIRTs shall clearly specify the communication channels and make them known to constituency and cooperative partners;	(a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. CSIRTs shall clearly specify the communication channels and make them known to constituency and cooperative partners;	(a) CSIRTs shall ensure a high level of availability of their communications ~~*services*~~***channels*** by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. CSIRTs shall clearly specify the communication channels and make them known to constituency and cooperative partners;	(a) ***CSIRTs shall ensure a high level of availability of their communication channels by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. CSIRTs shall clearly specify the communication channels and make them known to constituency and cooperative partners;*** ~~*CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. CSIRTs shall clearly specify the communication channels and make them known to constituency and cooperative partners;*~~	G
Article 10(1), point (b)						
G	212	(b) CSIRTs' premises and the supporting information systems shall be located in secure sites;	(b) CSIRTs' premises and the supporting information systems shall be located in secure sites;	(b) CSIRTs' premises and the supporting information systems shall be located in secure sites;	(b) CSIRTs' premises and the supporting information systems shall be located in secure sites; Text Origin: Commission Proposal + Annexes	G
Article 10(1), point (c)						

G	213	(c) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular, to facilitate effective and efficient handovers;	(c) CSIRTs shall be equipped with an appropriate system for ~~*managing and routing*~~***classifying, routing and tracking*** requests, in particular, to facilitate effective and efficient handovers;	(c) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular, to facilitate effective and efficient handovers;	(c) ***CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular, to facilitate effective and efficient handovers;*** ~~*CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular, to facilitate effective and efficient handovers;*~~ Text Origin: Commission Proposal + Annexes	G
Article 10(1), point (ca)					
G	213a		***(ca) CSIRTs shall have appropriate codes of conduct in place to ensure the confidentiality and trustworthiness of their operations;***		***(ca) CSIRTs shall ensure the confidentiality and trustworthiness of their operations;*** recital to be added (EP to draft)	G
Article 10(1), point (d)					
G	214	(d) CSIRTs shall be adequately staffed to ensure availability at all times;	(d) CSIRTs shall be adequately staffed to ensure availability at all times ***and ensure appropriate training frameworks of their staff***;	(d) CSIRTs shall be adequately staffed to ensure availability at all times;	(d) CSIRTs shall be adequately staffed to ensure availability at all times ***and shall ensure that their staff is trained appropriately***;	G
Article 10(1), point (e)					

G	215	(e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services;	(e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services***, including broad connectivity across networks, information systems, services and devices***;	(e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services;	(e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services; Text Origin: Commission Proposal + Annexes
	Article 10(1), point (f)				
G	216	(f) CSIRTs shall have the possibility to participate in international cooperation networks.	(f) CSIRTs shall have the possibility to participate in international cooperation networks.	(f) CSIRTs shall have the possibility to participate in international cooperation networks.	(f) CSIRTs shall have the possibility to participate in international cooperation networks. Text Origin: Commission Proposal + Annexes
	Article 10(1a)				
G	216a		***1a. CSIRTs shall develop at least the following technical capabilities:*** ***(a) the ability to conduct real-time or near-real-time monitoring of networks and information systems, and anomaly detection;*** ***(b) the ability to support intrusion prevention and detection;*** ***(c) the ability to collect and conduct complex forensic data analysis, and to reverse engineer***		***1a. Member States shall ensure that their CSIRTs jointly have the technical capabilities necessary to perform the tasks referred to in paragraph 2. Member States shall ensure that sufficient resources are allocated to CSIRTs to ensure adequate staffing levels to enable CSIRTs to develop their technical capabilities***

			cyber threats; ***(d) the ability to filter malign traffic;*** ***(e) the ability to enforce strong authentication and access privileges and controls; and*** ***(f) the ability to analyse cyber threats.***		
Article 10(2), introductory part					
G	217	2. CSIRTs shall have the following tasks:	2. CSIRTs shall have the following tasks:	2. CSIRTs shall have the following tasks:	2. CSIRTs shall have the following tasks: Text Origin: Commission Proposal + Annexes
Article 10(2), point (a)					
G	218	(a) monitoring cyber threats, vulnerabilities and incidents at national level;	(a) monitoring cyber threats, vulnerabilities and incidents at national level ***and acquiring real-time threat intelligence***;	(a) monitoring cyber threats, vulnerabilities and incidents at national level;	(a) ***monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing support to entities regarding real-time or near real-time monitoring of their networks and information systems;*** ~~*monitoring cyber threats, vulnerabilities and incidents at national level;*~~
Article 10(2), point (b)					
G	219				

		(b) providing early warning, alerts, announcements and dissemination of information to essential and important entities as well as to other relevant interested parties on cyber threats, vulnerabilities and incidents;	(b) providing early warning, alerts, announcements and dissemination of information to essential and important entities as well as to other relevant interested parties on cyber threats, vulnerabilities and incidents***, if possible near-real-time***;	(b) providing early warning, alerts, announcements and dissemination of information to essential and important entities as well as to ***competent authorities and*** other relevant interested parties on cyber threats, vulnerabilities and incidents;	(b) ***providing early warnings, alerts, announcements and dissemination of information to essential and important entities as well as to competent authorities and other relevant interested parties on cyber threats, vulnerabilities and incidents, if possible in near-real-time****providing early warning, alerts, announcements and dissemination of information to essential and important entities as well as to other relevant interested parties on cyber threats, vulnerabilities and incidents;*
Article 10(2), point (c)					
G	220	(c) responding to incidents;	(c) responding to incidents ***and providing assistance to the entities involved***;	(c) responding to incidents;	(c) ***responding to incidents and providing assistance to the entities concerned, where applicable;****responding to incidents;*
Article 10(2), point (d)					
G	221	(d) providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;	(d) providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;	(d) ***collecting and analysing forensic data and*** providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;	(d) ***collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;****providing dynamic*

					~~*risk and incident analysis and situational awareness regarding cybersecurity;*~~
Article 10(2), point (e)					
G	222	(e) providing, upon request of an entity, a proactive scanning of the network and information systems used for the provision of their services;	(e) providing, upon request of an entity ***or in the case of a serious threat to national security***, a proactive scanning of the network and information systems used for the provision of their services;	(e) providing, ~~*upon request of an entity, a proactive scanning of*~~***a proactive scanning of the network and information systems to detect vulnerabilities with potential significant impact provided that, where there is no consent of that entity,*** the network and information systems ~~*used for the provision of*~~***are not intruded or*** their ~~*services*~~***functioning negatively impacted***;	(e) providing, upon ***the*** request of an entity, a proactive scanning of the network and information systems ~~*used for the provision*~~***of the entity concerned to detect vulnerabilities with a potential significant impact. CSIRTs may carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential or important entities. Such scanning shall be carried out to detect vulnerable or insecurely configured network and information systems and inform the entities concerned. Such scanning shall not have any negative impact on the functioning*** of their services;
Article 10(2), point (f)					
G	223	(f) participating in the CSIRTs network and providing mutual assistance to other members of the network upon their request.	(f) participating in the CSIRTs network and providing mutual assistance to other members of the network upon their request.	(f) participating in the CSIRTs network and providing mutual assistance ***according to their capacities and competencies*** to other members of the network	(f) participating in the CSIRTs network and providing mutual assistance ***according to their capacities and competencies*** to other members of the network

				upon their request.	upon their request. Text Origin: Council Mandate
Article 10(2), point (fa)					
G	223a			***(fa) where applicable, acting as a coordinator for the purpose of the coordinated vulnerability disclosure process pursuant to Article 6 (1) that shall include in particular facilitating the interaction between the reporting entities, the potential vulnerability owner and the manufacturer or provider of ICT products or ICT services in cases where this is necessary, identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure time lines and managing vulnerabilities that affect multiple organisations (multi-party coordinated vulnerability disclosure).***	***(fa) where applicable, acting as a coordinator for the purpose of the coordinated vulnerability disclosure process pursuant to Article 6 (1) that shall include in particular facilitating the interaction between the reporting entities, the potential vulnerability owner and the manufacturer or provider of ICT products or ICT services in cases where this is necessary, identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure time lines and managing vulnerabilities that affect multiple organisations (multi-party coordinated vulnerability disclosure).***
Article 10(2), point (fa)					
G	223b		***(fa) providing, upon request of an entity, enabling and configuration of network logging to protect data, including personal data from unauthorised exfiltration;***		EP proposal to include in relevant recitals (27a, 45a)

Article 10(2), point (fb)					
G	223c		***(fb) contributing to the deployment of secure information sharing tools pursuant to Article 9(3).***		***(fb) contributing to the deployment of secure information sharing tools pursuant to Article 9(3).*** Text Origin: EP Mandate
Article 10(2), point (fd)					
G	223d				***When carrying out these tasks, CSIRTs may prioritise particular tasks based on a risk-based approach.***
Article 10(3)					
G	224	3. CSIRTs shall establish cooperation relationships with relevant actors in the private sector, with a view to better achieving the objectives of the Directive.	3. CSIRTs shall establish cooperation relationships with relevant actors in the private sector, with a view to better achieving the objectives of the Directive.	3. CSIRTs shall establish cooperation relationships with relevant actors in the private sector, with a view to better achieving the objectives of the Directive.	3. CSIRTs shall establish cooperation relationships with relevant actors in the private sector, with a view to better achieving the objectives of the Directive. Text Origin: Commission Proposal + Annexes
Article 10(3a)					
G	224a			***3a. CSIRTs may establish***	

				cooperation relationships with national CSIRTs of third countries. As part of this cooperation, they may exchange relevant information, including personal data in accordance with Union law on data protection.	included in Art 9
Article 10(4), introductory part					
G	225	4. In order to facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to the following:	4. In order to facilitate cooperation, CSIRTs shall promote ***automation of information exchange,*** the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to the following:	4. In order to facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to the following:	4. In order to facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to the following: Text Origin: Commission Proposal + Annexes
Article 10(4), point (a)					
G	226	(a) incident handling procedures;	(a) incident handling procedures;	(a) incident handling procedures;	(a) incident handling procedures; Text Origin: Commission Proposal + Annexes
Article 10(4), point (b)					
G	227	(b) cybersecurity crisis management;	(b) cybersecurity crisis management;	(b) cybersecurity crisis management;	(b) cybersecurity crisis management;

					Text Origin: Commission Proposal + Annexes
Article 10(4), point (c)					
G	228	(c) coordinated vulnerability disclosure.	(c) coordinated vulnerability disclosure.	(c) coordinated vulnerability disclosure.	(c) coordinated vulnerability disclosure. Text Origin: Commission Proposal + Annexes
Article 11					
G	229	Article 11 Cooperation at national level	Article 11 Cooperation at national level	Article 11 Cooperation at national level	Article 11 Cooperation at national level Text Origin: Commission Proposal + Annexes
Article 11(1)					
G	230	1. Where they are separate, the competent authorities referred to in Article 8, the single point of contact and the CSIRT(s) of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive.	1. Where they are separate, the competent authorities referred to in Article 8, the single point of contact and the CSIRT(s) of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive.	1. Where they are separate, the competent authorities referred to in Article 8, the single point of contact and the CSIRT(s) of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive.	1. Where they are separate, the competent authorities referred to in Article 8, the single point of contact and the CSIRT(s) of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive. Text Origin: Commission Proposal + Annexes
Article 11(2)					

Y	231	2. Member States shall ensure that either their competent authorities or their CSIRTs receive notifications on incidents, and significant cyber threats and near misses submitted pursuant to this Directive. Where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to carry out their tasks, be granted access to data on incidents notified by the essential or important entities, pursuant to Article 20.	2. Member States shall ensure that ~~either their competent authorities or~~ their CSIRTs receive notifications on ***significant*** incidents~~, and significant~~ ***pursuant to Article 20 and*** cyber threats and near misses ~~submitted~~ pursuant to ~~this Directive. Where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to carry out their tasks, be granted access to data on incidents notified by the essential or important entities, pursuant to~~***Article 27 through the single entry point referred to in*** Article 20***(4a)***.	2. Member States shall ensure that either their competent authorities or their CSIRTs receive notifications on incidents, and significant cyber threats and near misses submitted pursuant to this Directive. Where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to carry out their tasks, be granted access to data on incidents notified by the essential or important entities, pursuant to Article 20.	2. Member States shall ensure that ~~either~~ their ~~competent authorities or their CSIRTs~~***CSIRTs or, where relevant, the competent authority,*** receive notifications on ***significant*** incidents~~, and significant~~ ***pursuant to Article 20 and*** cyber threats and near misses ~~submitted~~ pursuant to ~~this Directive. Where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to carry out their tasks, be granted access to data on incidents notified by the essential or important entities, pursuant to~~***Article 27 through the single entry point referred to in*** Article 20***(4a)***. linked to discussion single point of entry Art 20 Text Origin: EP Mandate	Y
	Article 11(3)					
G	232	3. Each Member State shall ensure that its competent authorities or CSIRTs inform its single point of contact of notifications on incidents, significant cyber threats and near misses submitted	3. Each Member State shall ensure that its competent authorities or CSIRTs inform its single point of contact of notifications on incidents, significant cyber threats and near misses submitted pursuant	3. Each Member State shall ensure that its competent authorities or CSIRTs inform its single point of contact of notifications on incidents, significant cyber threats and near misses submitted pursuant	3. Each Member State shall ensure that its competent authorities or CSIRTs inform its single point of contact of notifications on incidents, significant cyber threats and near misses submitted pursuant	G

		pursuant to this Directive.	to this Directive.	to this Directive.	to this Directive. Text Origin: Commission Proposal + Annexes
Article 11(4)					
G	233	4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[1] [the DORA Regulation] within that Member State. _____ 1. [insert the full title and OJ publication reference when known]	4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities ~~and~~, single points of contact, ***CSIRTs,*** ~~and~~ law enforcement authorities, ***national regulatory authorities or other competent authorities responsible for public electronic communications networks or for publicly available electronic communications services pursuant to Directive (EU) 2018/1972,*** data protection authorities, ~~and~~ the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[1] [the DORA Regulation] within that Member State ***in line***	4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities, ***CSIRTs,*** ~~and~~ single points of contact ~~and~~***as well as*** law enforcement authorities, data protection authorities, and the ***competent*** authorities ~~responsible for critical infrastructure~~***designated*** pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]***, the competent authorities under Commission Implementing Regulation 2019/1583, the national regulatory authorities designated in accordance with Directive (EU) 2018/1972, the national authorities designated pursuant to Article 17 of Regulation (EU) No 910/2014,*** ~~and~~ the national financial authorities designated in accordance with Regulation (EU)	4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities ~~and~~, single points of contact ~~and law enforcement authorities, data protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[1] [the DORA Regulation] within that Member State.~~***, CSIRTs and other relevant authorities within that Member State, in line with their respective competences.*** _____ ~~1. [insert the full title and OJ publication reference when known]~~ Add list, including DORA, from both	G

			with their respective competences. _____ 1. [insert the full title and OJ publication reference when known]	XXXX/XXXX of the European Parliament and of the Council[1] [the DORA Regulation]***, as well as competent authorities designated by other sector-specific Union legal acts,*** within that Member State. _____ ~~1. [insert the full title and OJ publication reference when known]~~	AMs to recital + "relevant authorities" issue. COM to prepare recitals
Article 11(5)					
G	234	5. Member States shall ensure that their competent authorities regularly provide information to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] on cybersecurity risks, cyber threats and incidents affecting essential entities identified as critical, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken by competent authorities in response to those risks and incidents.	5. Member States shall ensure that their competent authorities regularly provide ***timely*** information to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] on cybersecurity risks, cyber threats and incidents affecting essential entities identified as critical, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken by competent authorities in response to those risks and incidents.	5. Member States shall ensure that their competent authorities ~~regularly provide information to~~***under this Directive and the*** competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] ***regularly exchange information on the identification of critical entities,*** ~~on~~ cybersecurity risks, cyber threats and incidents ***as well as on non-cyber risks, threats and incidents*** affecting essential entities identified as critical, ***[***or as entities equivalent to critical entities,***]*** pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken ~~by~~***in response to those risks and***	5. Member States shall ensure that their competent authorities ***designated*** regularly provide information to ***under this Directive and their*** competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] ***regularly exchange information with regard to the identification of critical entities,*** on cybersecurity risks, cyber threats and incidents ***as well as on non-cyber risks, threats and incidents*** affecting essential entities identified as critical, ***[***or as entities equivalent to critical entities,***]*** pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken ~~by~~***by in response to such risks and***	G

			incidents. Member States shall also ensure that competent authorities under this Directive and the competent authorities designated under Regulation XXXX/XXXX [DORA Regulation], Directive 2018/1972 and Regulation (EU) 910/2014 regularly exchange relevant information. ***With regard to trust service providers and in particular in cases where that supervisory role under this Directive is assigned to a different body than the supervisory bodies designated pursuant to Regulation (EU) 910/2014, the national*** competent authorities ***under this Directive shall cooperate closely, in a timely manner, by exchanging the relevant information in order to ensure effective supervision and compliance of trust service providers with the requirements set out in this Directive and Regulation [XXXX/XXXX] and, where applicable, the national competent authority under this Directive shall, without undue delay, inform the eIDAS supervisory body about any notified significant cyber threat or incident with impact on trust***	***incidents. Member States shall also ensure that their competent authorities designated under this Directive and their*** competent authorities ~~*in response to those risks and incidents*~~***designated under Regulation XXXX/XXXX [DORA Regulation] and Directive 2018/1972 and Regulation (EU) 910/2014 regularly exchange relevant information, including with regard to relevant incidents and cyber threats***. To be aligned with CER later. EP proposal

				services*~~in response to those risks and incidents~~*.		
	Article 11(5a)					
G	234a			***5a. For the purpose of simplifying the reporting of incidents, Member States may establish a single-entry point for all notifications required under this Directive, as well as under Regulation (EU) 2016/679 and Directive 2002/58/EC, where appropriate. Member States may use the single entry point for notifications required under other sector-specific Union legal acts. This single-entry point shall not affect the application of the provisions of Regulation (EU) 2016/679 and Directive 2002/58/EC, in particular those relating to independent supervisory authorities.***	***5a. The competent authorities designated under this Directive and the supervisory bodies designated under Regulation (EU) 910/2014 shall cooperate closely and shall assist each other with a view to ensuring effective supervision and compliance of trust service providers with this Directive and with Regulation (EU) 910/2014. Where applicable, the competent authorities designated under this Directive shall inform the supervisory bodies designated under Regulation (EU) 910/2014, without undue delay, of relevant incidents and cyber threats.***	G
	Article 11(5b)					
Y	234b				***5b.*** COM to draft new text on single entry point	Y
	CHAPTER III					

G	235	CHAPTER III Cooperation	CHAPTER III Cooperation	CHAPTER III ***EU*** Cooperation	CHAPTER III Cooperation ***at Union and international level***
	Article 12				
G	236	Article 12 Cooperation Group	Article 12 Cooperation Group	Article 12 Cooperation Group	Article 12 Cooperation Group Text Origin: Commission Proposal + Annexes
	Article 12(1)				
G	237	1. In order to support and to facilitate strategic cooperation and the exchange of information among Member States in the field of application of the Directive, a Cooperation Group is established.	1. In order to support and to facilitate strategic cooperation and the exchange of information among Member States in the field of application of the Directive, a Cooperation Group is established.	1. In order to support and to facilitate strategic cooperation and the exchange of information among Member States ~~*in the field of application of the Directive*~~***as well as to strengthen trust and confidence*** , a Cooperation Group is established.	1. In order to support and to facilitate strategic cooperation and the exchange of information among Member States ~~*in the field of application of the Directive*~~***as well as to strengthen trust and confidence*** , a Cooperation Group is established. Text Origin: Council Mandate
	Article 12(2)				
G	238	2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 6.	2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 6.	2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 6.	2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 6.

					Text Origin: Commission Proposal + Annexes
Article 12(3), introductory part					
G	239	3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group.	3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European ***Parliament and the European*** External Action Service shall participate in the activities of the Cooperation Group as ~~*an observer*~~***observers***. The European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group.	3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) ~~*in accordance with Article 17(5)(c) of*~~***and the competent authorities designated under*** Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group ***in accordance with Article 42(1) of Regulation (EU) XXXX/XXXX [the DORA Regulation]***.	3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) ~~*in accordance with Article 17(5)(c) of*~~***and the competent authorities designated under*** Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group ***in accordance with Article 42(1) of Regulation (EU) XXXX/XXXX [the DORA Regulation]***. Text Origin: Council Mandate	G
Article 12(3), first paragraph					
G	240	Where appropriate, the Cooperation Group may invite representatives of relevant stakeholders to participate in its work.	Where appropriate, the Cooperation Group may invite representatives of relevant stakeholders***, such as the European Data Protection Board***	Where appropriate, the Cooperation Group may invite representatives of relevant stakeholders to participate in its work.	Where appropriate, the Cooperation Group may invite ***the European Parliament and*** representatives of relevant stakeholders to participate in its	G

			and representatives of industry, to participate in its work.		work. EP proposal: (34) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It should organise regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Cooperation Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Cooperation Group should consider inviting relevant Union institutions, bodies and agencies involved in cybersecurity policy, such as the European Parliament, Europol, the European Data Protection Board, the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work. Text Origin: Commission Proposal + Annexes
Article 12(3), second paragraph					
G	241	The Commission shall provide the secretariat.	The Commission shall provide the secretariat.	The Commission shall provide the secretariat.	The Commission shall provide the secretariat. Text Origin: Commission Proposal + Annexes

Article 12(4), introductory part					
G	242	4. The Cooperation Group shall have the following tasks:	4. The Cooperation Group shall have the following tasks:	4. The Cooperation Group shall have the following tasks:	4. The Cooperation Group shall have the following tasks: tasks on report to EP to be added Text Origin: Commission Proposal + Annexes	G
Article 12(4), point (a)					
G	243	(a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive;	(a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive;	(a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive;	(a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive; Text Origin: Commission Proposal + Annexes	G
Article 12(4), point (aa)					
G	243a			***(aa) providing guidance in relation to the development and implementation of policies on coordinated vulnerability disclosure as referred to in Article 5(2) (c) and Article 6(1);***	***(aa) providing guidance in relation to the development and implementation of policies on coordinated vulnerability disclosure as referred to in Article 5(2) (c) and Article 6(1);*** Text Origin: Council Mandate	G
Article 12(4), point (b)					

G	244	(b) exchanging best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, trainings, exercises and skills, building capacity as well as standards and technical specifications;	(b) exchanging best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, trainings, exercises and skills, ***capacity*** building***, standards and technical specifications*** ~~capacity~~ as well as ~~standards and technical specifications~~***the identification of essential and important entities***;	(b) exchanging best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, trainings, exercises and skills, building capacity as well as standards and technical specifications;	(b) exchanging best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, trainings, exercises and skills, ***capacity*** building***, standards and technical specifications*** ~~capacity~~ as well as ~~standards and technical specifications~~***the designation of essential and important entities pursuant to Art. 2(2) point (b)-(f)***; COM to reflect on "identification"	G
Article 12(4), point (ba)					
G	244a		***(ba) mapping the national solutions in order to promote compatibility of cybersecurity solutions applied to each specific sector across the Union;***		G
Article 12(4), point (c)					
G	245	(c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives;	(c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives ***and the overall consistency of sector-specific***	(c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives;	(c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives ***and the overall consistency of sector-specific***	G

			cybersecurity requirements;		***cybersecurity requirements***; Text Origin: EP Mandate
Article 12(4), point (d)					
Y	246	(d) exchanging advice and cooperating with the Commission on draft Commission implementing or delegated acts adopted pursuant to this Directive;	(d) exchanging advice and cooperating with the Commission on draft Commission implementing or delegated acts adopted pursuant to this Directive;	(d) exchanging advice and cooperating with the Commission on draft Commission implementing ~~*or delegated*~~ acts adopted pursuant to this Directive;	Y
Article 12(4), point (e)					
G	247	(e) exchanging best practices and information with relevant Union institutions, bodies, offices and agencies;	(e) exchanging best practices and information with relevant Union institutions, bodies, offices and agencies;	(e) exchanging best practices and information with relevant Union institutions, bodies, offices and agencies;	(e) exchanging best practices and information with relevant Union institutions, bodies, offices and agencies; Text Origin: Commission Proposal + Annexes	G
Article 12(4), point (ea)					
G	247a			***(ea) exchanging views on the implementation of sectorial legislation with cybersecurity aspects;***	***(ea) exchanging views on the implementation of sectorial legislation with cybersecurity aspects;*** Text Origin: Council Mandate	G
Article 12(4), point (f)					

Y	248	(f) discussing reports on the peer review referred to in Article 16(7);	(f) discussing reports on the peer review referred to in Article 16(7)***, and drawing up conclusions and recommendations***;	(f) discussing reports on the peer ~~review~~***learnings*** referred to in Article 16(7);	(f) discussing reports on the peer review referred to in Article 16(7); connected to art. 16 Text Origin: Commission Proposal + Annexes	Y
	Article 12(4), point (fa)					
G	248a		***(fa) carrying out coordinated security risk assessments that may be initiated pursuant to Article 19(1), in cooperation with the Commission and ENISA;***		***(fa) carrying out coordinated security risk assessments in accordance with Article 19(1);***	G
	Article 12(4), point (g)					
G	249	(g) discussing results from joint-supervisory activities in cross-border cases as referred to in Article 34;	(g) discussing results from joint-supervisory activities in cross-border cases as referred to in Article 34;	(g) discussing ~~*results*~~ ***experiences*** from joint-supervisory activities in cross-border cases as referred to in Article 34;	(g) discussing ***cases of mutual assistance, including experiences and*** results from ***cross-border*** joint-supervisory activities ~~*in cross-border cases*~~ as referred to in Article 34;	G
	Article 12(4), point (ga)					
G	249a				***(ga) upon request of one or more Member States concerned, discussing particular requests for mutual assistance referred to in***	G

					Article 34;
Article 12(4), point (h)					
G	250	(h) providing strategic guidance to the CSIRTs network on specific emerging issues;	(h) providing strategic guidance to the CSIRTs network on specific emerging issues;	(h) providing strategic guidance to the CSIRTs network ***and EU–CyCLONe*** on specific emerging issues;	(h) providing strategic guidance to the CSIRTs network ***and EU–CyCLONe*** on specific emerging issues; Text Origin: Council Mandate
Article 12(4), point (ha)					
G	250a			***(ha) exchanging views on policy follow-up of large-scale cybersecurity incidents on the basis of lessons learned of the CSIRTs network and EU–CyCLONe;***	***(ha) exchanging views on policy follow-up of large-scale cybersecurity incidents and crises on the basis of lessons learned of the CSIRTs network and EU–CyCLONe;***
Article 12(4), point (i)					
G	251	(i) contributing to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the Member States' competent authorities or CSIRTs;	(i) contributing to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the Member States' competent authorities or CSIRTs;	(i) contributing to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the Member States' competent authorities or CSIRTs;	(i) contributing to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the Member States' competent authorities or CSIRTs; Text Origin: Commission Proposal + Annexes

Article 12(4), point (j)					
G	252	(j) organising regular joint meetings with relevant private interested parties from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges;	(j) organising regular joint meetings with relevant private interested parties from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges;	(j) organising regular joint meetings with relevant private interested parties from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges;	(j) organising regular joint meetings with relevant private interested parties from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges; Text Origin: Commission Proposal + Annexes
Article 12(4), point (k)					
G	253	(k) discussing the work undertaken in relation to cybersecurity exercises, including the work done by ENISA.	(k) discussing the work undertaken in relation to cybersecurity exercises, including the work done by ENISA.	(k) discussing the work undertaken in relation to cybersecurity exercises, including the work done by ENISA.	(k) discussing the work undertaken in relation to cybersecurity exercises, including the work done by ENISA. Text Origin: Commission Proposal + Annexes
Article 12(4), point (ka)					
Y	253a			***(ka) establish the peer-learning mechanism in accordance with Article 16 of this Directive.***	To be aligned with art. 16
Article 12(4), point (ka)					
G	253b		***(ka) submitting to the***		***(ka) preparing reports for the***

			Commission for the purpose of the review referred to in Article 35 reports on the experience gained at a strategic and operational level;		***purpose of the review referred to in Article 35 on the experience gained at a strategic level and from peer reviews;*** ***The reports shall be submitted to the Commission, the European Parliament and the Council.*** potential overlap to be checked
Article 12(4), point (kb)					
G	253c		***(kb) providing a yearly assessment in cooperation with ENISA, Europol and national law enforcement institutions on which third countries are harbouring ransomware criminals.***		***(kc) discussing and carrying out on a regular basis an assessment of the state of play of current cyber threats or incidents, such as ransomware.*** recital to be added
Article 12(5)					
G	254	5. The Cooperation Group may request from the CSIRT network a technical report on selected topics.	5. The Cooperation Group may request from the CSIRT network a technical report on selected topics.	5. The Cooperation Group may request from the CSIRT network a technical report on selected topics.	5. The Cooperation Group may request from the CSIRT network a technical report on selected topics. Text Origin: Commission Proposal + Annexes
Article 12(6)					
G	255				

		6. By … [] 24 months after the date of entry into force of this Directive[] and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive shall be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148.	6. By … [] 24 months after the date of entry into force of this Directive[] and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive shall be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148.	6. By … [~~]/24 months after the date of entry into force of this Directive[~~]/ and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive shall be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148.	6. By … [~~]/24 months after the date of entry into force of this Directive[~~]/ and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive shall be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148. Text Origin: Council Mandate
Article 12(7)					
G	256	7. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).	7. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).	7. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).	7. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2). Text Origin: Commission Proposal + Annexes
Article 12(8)					
G	257	8. The Cooperation Group shall	8. The Cooperation Group shall	8. The Cooperation Group shall	8. The Cooperation Group shall

		meet regularly and at least once a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to promote strategic cooperation and exchange of information.	meet regularly and at least ~~once~~***twice*** a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to ~~promote~~***facilitate*** strategic cooperation and ~~exchange of information~~***information exchange***.	meet regularly and at least once a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to promote strategic cooperation and ***facilitate*** exchange of information.	meet regularly and at least once a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to promote ***and facilitate*** strategic cooperation and ~~exchange of information~~***information exchange***.
Article 13					
G	258	Article 13 CSIRTs network	Article 13 CSIRTs network	Article 13 CSIRTs network	Article 13 CSIRTs network Text Origin: Commission Proposal + Annexes
Article 13(1)					
G	259	1. In order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of the national CSIRTs is established.	1. In order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of the national CSIRTs is established.	1. In order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of the national CSIRTs is established.	1. In order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of the national CSIRTs is established. Text Origin: Commission Proposal + Annexes
Article 13(2)					
G	260				

		2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT–EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support cooperation among the CSIRTs.	2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT–EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support cooperation among the CSIRTs.	2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs ***designated in accordance with Article 9*** and CERT–EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support cooperation among the CSIRTs.	2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs ***designated in accordance with Article 9*** and CERT–EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support cooperation among the CSIRTs. Text Origin: Council Mandate
Article 13(3), introductory part					
G	261	3. The CSIRTs network shall have the following tasks:	3. The CSIRTs network shall have the following tasks:	3. The CSIRTs network shall have the following tasks:	3. The CSIRTs network shall have the following tasks: Text Origin: Commission Proposal + Annexes
Article 13(3), point (a)					
G	262	(a) exchanging information on CSIRTs' capabilities;	(a) exchanging information on CSIRTs' capabilities;	(a) exchanging information on CSIRTs' capabilities;	(a) exchanging information on CSIRTs' capabilities; Text Origin: Commission Proposal + Annexes
Article 13(3), point (aa)					
G	262a		***(aa) facilitating the sharing and transferring of technology and***		***(aa) facilitating the sharing, transferring and exchanging of***

			relevant measures, policies, best practices and frameworks among the CSIRTs;		***technology and relevant measures, policies, tools, processes, best practices and frameworks among the CSIRTs;***
Article 13(3), point (b)					
G	263	(b) exchanging relevant information on incidents, near misses, cyber threats, risks and vulnerabilities;	(b) exchanging relevant information on incidents, near misses, cyber threats, risks and vulnerabilities;	(b) exchanging relevant information on incidents, near misses, cyber threats, risks and vulnerabilities;	(b) exchanging relevant information on incidents, near misses, cyber threats, risks and vulnerabilities; Text Origin: Commission Proposal + Annexes
Article 13(3), point (ba)					
G	263a			***(ba) exchanging information in regard to cybersecurity publications and recommendations;***	***(ba) exchanging information in regard to cybersecurity publications and recommendations;***
Article 13(3), point (ba)					
G	263b		***(ba) ensuring interoperability with regard to information sharing standards;***		***(bb) ensuring interoperability with regard to information sharing specifications and protocols;***
Article 13(3), point (bb)					
G	263c				

				(bb) sharing of technical solutions facilitating the technical handling of incidents;	Deleted.
Article 13(3), point (bc)					
G	263d			***(bc) exchanging best practices, tools and processes in regards to the tasks of the CSIRTs;***	Deleted. G
Article 13(3), point (c)					
G	264	(c) at the request of a representative of the CSIRT network potentially affected by an incident, exchanging and discussing information in relation to that incident and associated cyber threats, risks and vulnerabilities;	(c) at the request of a representative of the CSIRT network potentially affected by an incident, exchanging and discussing information in relation to that incident and associated cyber threats, risks and vulnerabilities;	(c) at the request of a ~~representative~~***member*** of the ~~CSIRT~~***CSIRTs*** network potentially affected by an incident, exchanging and discussing information in relation to that incident and associated cyber threats, risks and vulnerabilities~~;~~	(c) at the request of a ~~representative~~***member*** of the ~~CSIRT~~***CSIRTs*** network potentially affected by an incident, exchanging and discussing information in relation to that incident and associated cyber threats, risks and vulnerabilities~~;~~ Text Origin: Council Mandate G
Article 13(3), point (d)					
G	265	(d) at the request of a representative of the CSIRT network, discussing and, where possible, implementing a coordinated response to an incident that has been identified within the jurisdiction of that Member State;	(d) at the request of a representative of the CSIRT network, discussing and, where possible, implementing a coordinated response to an incident that has been identified within the jurisdiction of that Member State;	(d) at the request of a ~~representative of the CSIRT~~***member of the CSIRTs*** network, discussing and, where possible, implementing a coordinated response to an incident that has been identified within the	(d) at the request of a ~~representative of the CSIRT~~***member of the CSIRTs*** network, discussing and, where possible, implementing a coordinated response to an incident that has been identified within the G

				jurisdiction of that Member State;	jurisdiction of that Member State; Text Origin: Council Mandate
Article 13(3), point (e)					
G	266	(e) providing Member States with support in addressing cross–border incidents pursuant to this Directive;	(e) providing Member States with support in addressing cross–border incidents pursuant to this Directive;	(e) providing Member States with support in addressing cross–border incidents pursuant to this Directive;	(e) providing Member States with support in addressing cross–border incidents pursuant to this Directive; Text Origin: Commission Proposal + Annexes
Article 13(3), point (f)					
G	267	(f) cooperating and providing assistance to designated CSIRTs referred to in Article 6 with regard to the management of multiparty coordinated disclosure of vulnerabilities affecting multiple manufacturers or providers of ICT products, ICT services and ICT processes established in different Member States;	(f) cooperating and providing assistance to designated CSIRTs referred to in Article 6 with regard to the management of multiparty coordinated disclosure of vulnerabilities affecting multiple manufacturers or providers of ICT products, ICT services and ICT processes established in different Member States;	(f) cooperating***, exchanging best practices*** and providing assistance to designated CSIRTs referred to in Article 6 with– regard to the management of ~~*multiparty*~~ coordinated disclosure of vulnerabilities affecting multiple manufacturers or providers of ICT products, ICT services and ICT processes established in different Member States;	(f) cooperating***, exchanging best practices*** and providing assistance to designated CSIRTs referred to in Article 6 with– regard to the management of ~~*multiparty*~~ coordinated disclosure of vulnerabilities affecting multiple manufacturers or providers of ICT products, ICT services and ICT processes established in different Member States; Text Origin: Council Mandate
Article 13(3), point (g), introductory part					
G	268	(g) discussing and identifying	(g) discussing and identifying	(g) discussing and identifying	(g) discussing and identifying

		further forms of operational cooperation, including in relation to:	further forms of operational cooperation, including in relation to:	further forms of operational cooperation, including in relation to:	further forms of operational cooperation, including in relation to: Text Origin: Commission Proposal + Annexes
	Article 13(3), point (g)(i)				
G	269	(i) categories of cyber threats and incidents;	(i) categories of cyber threats and incidents;	(i) categories of cyber threats and incidents;	(i) categories of cyber threats and incidents; Text Origin: Commission Proposal + Annexes
	Article 13(3), point (g)(ii)				
G	270	(ii) early warnings;	(ii) early warnings;	(ii) early warnings;	(ii) early warnings; Text Origin: Commission Proposal + Annexes
	Article 13(3), point (g)(iii)				
G	271	(iii) mutual assistance;	(iii) mutual assistance;	(iii) mutual assistance;	(iii) mutual assistance; Text Origin: Commission Proposal + Annexes
	Article 13(3), point (g)(iv)				
G	272	(iv) principles and modalities for coordination in response to cross–	(iv) principles and modalities for coordination in response to cross–	(iv) principles and modalities for coordination in response to cross–	(iv) principles and modalities for coordination in response to cross–

		border risks and incidents;	border risks and incidents;	border risks and incidents;	border risks and incidents; Text Origin: Commission Proposal + Annexes
Article 13(3), point (g)(v)					
G	273	(v) contribution to the national cybersecurity incident and crisis response plan referred to in Article 7 (3);	(v) contribution to the national cybersecurity incident and crisis response plan referred to in Article 7 (3);	(v) contribution to the national cybersecurity incident and crisis response plan referred to in Article 7 (3) ***at the request of a Member State***;	(v) contribution to the national cybersecurity incident and crisis response plan referred to in Article 7 (3) ***at the request of a Member State***; Text Origin: Council Mandate
Article 13(3), point (h)					
G	274	(h) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (g), where necessary, requesting guidance in that regard;	(h) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (g), where necessary, requesting guidance in that regard;	(h) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (g), ***and,*** where necessary, requesting guidance in that regard;	(h) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (g), ***and,*** where necessary, requesting guidance in that regard; Text Origin: Council Mandate
Article 13(3), point (i)					
G	275	(i) taking stock from cybersecurity exercises, including from those organised by ENISA;	(i) taking stock from cybersecurity exercises, including from those organised by ENISA;	(i) taking stock from cybersecurity exercises, including from those organised by ENISA;	(i) taking stock from cybersecurity exercises, including from those organised by ENISA; Text Origin: Commission Proposal + Annexes

Article 13(3), point (j)					
G	276	(j) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT;	(j) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT;	(j) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT;	(j) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT; Text Origin: Commission Proposal + Annexes
Article 13(3), point (k)					
G	277	(k) cooperating and exchanging information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and threats across the Union;	(k) cooperating and exchanging information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and threats across the Union;	(k) cooperating and exchanging information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and threats across the Union;	(k) cooperating and exchanging information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and threats across the Union; Text Origin: Commission Proposal + Annexes
Article 13(3), point (l)					
Y	278	(l) discussing the peer-review reports referred to in Article 16(7);	(l) discussing the peer-review reports referred to in Article 16(7);	(l) discussing the ~~*peer-review*~~***peer-learning*** reports referred to in Article 16(7);	(l) discussing the peer-review reports referred to in Article 16(7); To be aligned with Art 16 Text Origin: Commission Proposal + Annexes

Article 13(3), point (m)					
G	279	(m) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.	(m) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.	(m) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.	(m) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation. Text Origin: Commission Proposal + Annexes
Article 13(4)					
Y	280	4. For the purpose of the review referred to in Article 35 and by □24 months after the date of entry into force of this Directive□, and every two years thereafter, the CSIRTs network shall assess the progress made with the operational cooperation and produce a report. The report shall, in particular, draw conclusions on the outcomes of the peer reviews referred to in Article 16 carried out in relation to national CSIRTs, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group.	4. For the purpose of the review referred to in Article 35 and by □24 months after the date of entry into force of this Directive□, and every two years thereafter, the CSIRTs network shall assess the progress made with the operational cooperation and produce a report. The report shall, in particular, draw conclusions on the outcomes of the peer reviews referred to in Article 16 carried out in relation to national CSIRTs, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group.	4. For the purpose of the review referred to in Article 35 and by ~~□~~*[*24 months after the date of entry into force of this Directive~~□~~*]*, and every two years thereafter, the CSIRTs network shall assess the progress made with the operational cooperation and produce a report. The report shall, in particular, draw conclusions on the outcomes of the ~~*peer reviews*~~*peer-learning* referred to in Article 16 carried out in relation to national CSIRTs, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group.	4. For the purpose of the review referred to in Article 35 and by □24 months after the date of entry into force of this Directive□, and every two years thereafter, the CSIRTs network shall assess the progress made with the operational cooperation and produce a report. The report shall, in particular, draw conclusions on the outcomes of the peer reviews referred to in Article 16 carried out in relation to national CSIRTs, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group. To be aligned with article 16. Text Origin: Commission

					Proposal + Annexes
Article 13(5)					
G	281	5. The CSIRTs network shall adopt its own rules of procedure.	5. The CSIRTs network shall adopt its own rules of procedure.	5. The CSIRTs network shall adopt its own rules of procedure.	5. The CSIRTs network shall adopt its own rules of procedure. Text Origin: Commission Proposal + Annexes
Article 13(6)					
G	281a			***6. The CSIRT network shall cooperate with the EU-CyCLONe on the basis of agreed procedural arrangements.***	***6. The CSIRT network and the EU-CyCLONe shall agree on procedural arrangements and cooperate on the basis thereof.***
Article 14					
G	282	Article 14 The European cyber crises liaison organisation network (EU - CyCLONe)	Article 14 The European cyber crises liaison organisation network (EU - CyCLONe)	Article 14 The European cyber crises liaison organisation network (EU - CyCLONe)	Article 14 The European cyber crises liaison organisation network (EU - CyCLONe) Text Origin: Commission Proposal + Annexes
Article 14(1)					
G	283	1. In order to support the coordinated management of large-scale cybersecurity incidents and	1. In order to support the coordinated management of large-scale cybersecurity incidents and	1. In order to support the coordinated management of large-scale cybersecurity incidents and	1. In order to support the coordinated management of large-scale cybersecurity incidents and

		crises at operational level and to ensure the regular exchange of information among Member States and Union institutions, bodies and agencies, the European Cyber Crises Liaison Organisation Network (EU - CyCLONe) is hereby established.	crises at operational level and to ensure the regular exchange of ***relevant*** information among Member States and Union institutions, bodies and agencies, the European Cyber Crises Liaison Organisation Network (EU - CyCLONe) is hereby established.	crises at operational level and to ensure the regular exchange of information among Member States and Union institutions, bodies and agencies, the European Cyber Crises Liaison Organisation Network (EU - CyCLONe) is hereby established.	crises at operational level and to ensure the regular exchange of ***relevant*** information among Member States and Union institutions, bodies and agencies, the European Cyber Crises Liaison Organisation Network (EU - CyCLONe) is hereby established. Text Origin: EP Mandate
	Article 14(2)				
R	284	2. EU-CyCLONe shall be composed of the representatives of Member States' crisis management authorities designated in accordance with Article 7, the Commission and ENISA. ENISA shall provide the secretariat of the network and support the secure exchange of information.	2. EU-CyCLONe shall be composed of the representatives of Member States' crisis management authorities designated in accordance with Article 7, the Commission and ENISA. ENISA shall provide the secretariat of the ~~network~~***EU-CyCLONe*** and support the secure exchange of information.	2. EU-CyCLONe shall be composed of the representatives of Member States' ***cyber*** crisis management authorities designated in accordance with Article 7. The Commission ~~and ENISA~~***shall participate in the activities of the network as an observer***. ENISA shall provide the secretariat of the network and support the secure exchange of information ***as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information.*** ***Where appropriate, EU-CyCLONe may invite representatives of relevant stakeholders to participate in its work***.	membership of COM and ENISA - red line (to be discussed at political level) agreement on the other changes made in the EP and Council text

Article 14(2a)				
284a				
Article 14(3), introductory part				
285	3. EU-CyCLONe shall have the following tasks:	3. EU-CyCLONe shall have the following tasks:	3. EU-CyCLONe shall have the following tasks:	3. EU-CyCLONe shall have the following tasks: Text Origin: Commission Proposal + Annexes
Article 14(3), point (a)				
286	(a) increasing the level of preparedness of the management of large scale incidents and crises;	(a) increasing the level of preparedness of the management of large scale incidents and crises;	(a) increasing the level of preparedness of the management of large scale ***cybersecurity*** incidents and crises;	(a) increasing the level of preparedness of the management of ~~*large scale*~~***large-scale cybersecurity*** incidents and crises;
Article 14(3), point (b)				
287	(b) developing a shared situational awareness of relevant cybersecurity events;	(b) developing a shared situational awareness of relevant cybersecurity events;	(b) developing a shared situational awareness ~~*of relevant*~~***for large scale*** cybersecurity ~~*events*~~***incidents and crisis***;	(b) developing a shared situational awareness ~~*of relevant*~~***for large-scale*** cybersecurity ~~*events*~~***incidents and crises***;
Article 14(3), point (ba)				
287a			***(ba) assessing the consequences and impact of relevant large scale cybersecurity incidents and***	***(ba) assessing the consequences and impact of relevant large-scale cybersecurity incidents and crises***

				proposing possible mitigation measures;	***and proposing possible mitigation measures;***
Article 14(3), point (c)					
G	288	(c) coordinating large scale incidents and crisis management and supporting decision-making at political level in relation to such incidents and crisis;	(c) coordinating large scale incidents and crisis management and supporting decision-making at political level in relation to such incidents and crisis;	(c) coordinating ***the management of*** large scale ***cybersecurity*** incidents and crisis ~~*management*~~ and supporting decision-making at political level in relation to such incidents and crisis;	(c) coordinating ~~*large scale*~~***the management of large-scale cybersecurity*** incidents and ~~*crisis management*~~***crises*** and supporting decision-making at political level in relation to such incidents and ~~*crisis*~~***crises***;
Article 14(3), point (d)					
G	289	(d) discussing national cybersecurity incident and response plans referred to in Article 7(2).	(d) discussing national cybersecurity incident and response plans referred to in Article 7(2).	(d) ***at a request of a Member State,*** discussing ***its*** national cybersecurity incident and ***crisis*** response plans referred to in Article ~~*7(2).*~~***7(3);***	(d) discussing national cybersecurity incident and ***crisis*** response plans referred to in Article ~~*7(2)*~~***7(3). A national cybersecurity incident and crisis response plan of a Member State shall be discussed only at its request;***
Article 14(4)					
G	290	4. EU-CyCLONe shall adopt its rules of procedure.	4. EU-CyCLONe shall adopt its rules of procedure.	4. EU-CyCLONe shall adopt its rules of procedure.	4. EU-CyCLONe shall adopt its rules of procedure. Text Origin: Commission Proposal + Annexes

Article 14(5)					
G	291	5. EU-CyCLONe shall regularly report to the Cooperation Group on cyber threats, incidents and trends, focusing in particular on their impact on essential and important entities.	5. EU-CyCLONe shall regularly report to the Cooperation Group on ~~cyber threats,~~***large-scale*** incidents and ***crises, as well as*** trends, focusing in particular on their impact on essential and important entities.	5. EU-CyCLONe shall regularly report to the Cooperation Group on ~~cyber threats,~~***the management of large scale cybersecurity*** incidents and ~~trends~~***crisis management***, focusing in particular on their impact on essential and important entities.	5. EU-CyCLONe shall regularly report to the Cooperation Group on ~~cyber threats,~~***the management of large-scale cybersecurity*** incidents and ***crises, as well as*** trends, focusing in particular on their impact on essential and important entities.
Article 14(6)					
G	292	6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements.	6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements.	6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements.	6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements ***provided for in Article 13(6)***.
Article 14(6a)					
G	292a			***7. EU-CyCLONe shall submit to the European Parliament and the Council a report assessing its work by [24 months after the date of entering into force of this Directive].***	***7. EU-CyCLONe shall submit to the European Parliament and the Council a report assessing its work by [18 months after the date of entering into force of this Directive] and every 18 months thereafter.*** Text Origin: Council Mandate
Article 14a					

G	292b			***Article 14a International cooperation***	***Article 14a International cooperation*** Text Origin: Council Mandate	G
Article 14a, first paragraph						
G	292c			***The Union may, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe, in accordance with Union law on data protection.***	***The Union may, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe, in accordance with Union law on data protection.*** Text Origin: Council Mandate	G
Article 15						
G	293	Article 15 Report on the state of cybersecurity in the Union	Article 15 Report on the state of cybersecurity in the Union	Article 15 Report on the state of cybersecurity in the Union	Article 15 Report on the state of cybersecurity in the Union Text Origin: Commission Proposal + Annexes	G
Article 15(1), introductory part						

G	294	1. ENISA shall issue, in cooperation with the Commission, a biennial report on the state of cybersecurity in the Union. The report shall in particular include an assessment of the following:	1. ENISA shall issue, in cooperation with the Commission, a biennial report on the state of cybersecurity in the Union ***and shall submit and present it to the European Parliament***. The report shall ***be delivered in machine-readable format and shall*** in particular include an assessment of the following:	1. ENISA shall issue, in cooperation with the Commission ***and the Cooperation Group***, a biennial report on the state of cybersecurity in the Union. ***In particular,*** the report shall ~~*in particular*~~ include ~~*an assessment of*~~ the following:	1. ENISA shall issue, in cooperation with the Commission ***and the Cooperation Group***, a biennial report on the state of cybersecurity in the Union ***and shall submit and present it to the European Parliament***. The report shall***, inter alia, be made available in machine-readable data and include*** ~~*in particular include an assessment of*~~ the following:
	Article 15(1), point (aa)				
G	294a			***(aa) a Union-level cybersecurity risk assessment, taking account of the threat landscape;***	***(aa) a Union-level cybersecurity risk assessment, taking account of the threat landscape;*** Text Origin: Council Mandate
	Article 15(1), point (a)				
G	295	(a) the development of cybersecurity capabilities across the Union;	(a) the development of cybersecurity capabilities across the Union;	(a) ***an assessment of*** the development of cybersecurity capabilities ***in the public and private sectors*** across the Union;	(a) ***an assessment of*** the development of cybersecurity capabilities ***in the public and private sectors*** across the Union; Text Origin: Council Mandate
	Article 15(1), point (aa)				
G	295a		***(aa) the general level of***		***(aa) an assessment of the general***

		cybersecurity awareness and hygiene among citizens and entities, including SMEs, as well as the general level of security of connected devices;		***level of cybersecurity awareness and hygiene among citizens and entities, including SMEs;*** NEW PCY proposal: .... EP proposal for recital: Cybersecurity is influenced by many factors, including user awareness and level of security of consumer connected devices play an important role. Consumer-connected devices can be elements used in attacks therefore the level of preparedness of the citizens and the attributes of devices commonly put on the market are an important indicator of risks and tools for reducing those risks. Data driven policymaking, requires an assessment of the general level of cybersecurity awareness among citizens as well as on the general level of security of consumer-connected devices to establish baselines and direction for improvements. Such assessments need to be tailored to the needs and capacities of each Members State, and should also ensure a common understanding of risks at the Union level. To that regard, the Commission can provide guidance.
Article 15(1), point (b)				

G	296	(b) the technical, financial and human resources available to competent authorities and cybersecurity policies, and the implementation of supervisory measures and enforcement actions in light of the outcomes of peer reviews referred to in Article 16;	(b) the technical, financial and human resources available to competent authorities and cybersecurity policies, and the implementation of supervisory measures and enforcement actions in light of the outcomes of peer reviews referred to in Article 16;	(b) ~~the technical, financial and human resources available to competent authorities and cybersecurity policies, and the implementation of supervisory measures and enforcement actions in light of the outcomes of peer reviews referred to in Article 16;~~	(b) ~~the technical, financial and human resources available to competent authorities and cybersecurity policies, and the implementation of supervisory measures and enforcement actions in light of~~***an aggregated assessment on*** the outcomes of peer reviews referred to in Article 16; Text Origin: EP Mandate	G
	Article 15(1), point (c)				
G	297	(c) a cybersecurity index providing for an aggregated assessment of the maturity level of cybersecurity capabilities.	(c) a cybersecurity index providing for an aggregated assessment of the maturity level of cybersecurity capabilities ***across the Union, including the alignment of Member States national cybersecurity strategies***.	(c) ~~a~~***an aggregated assessment based on*** cybersecurity ~~index~~***quantitative and qualitative indicators,*** providing for an ~~aggregated assessment~~ ***overview*** of the maturity level of cybersecurity ***capabilities, including sector-specific*** capabilities.	(c) ~~a cybersecurity index providing for~~ an aggregated assessment of the maturity level of cybersecurity capabilities ***and resources across the Union, including sector-specific, including the alignment of Member States national cybersecurity strategies***.	G
	Article 15(2)				
G	298	2. The report shall include particular policy recommendations for increasing the level of cybersecurity across the Union and a summary of the findings for the	2. The report shall include particular ***identification of obstacles and*** policy recommendations for increasing the level of cybersecurity across	2. The report shall include particular policy recommendations for increasing the level of cybersecurity across the Union and a summary of the findings for the	2. The report shall include particular policy recommendations***, in view of addressing shortcomings and*** ~~for~~ increasing the level of cybersecurity across	G

		particular period from the Agency's EU Cybersecurity Technical Situation Reports issued by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.	the Union and a summary of the findings for the particular period from the Agency's EU Cybersecurity Technical Situation Reports issued by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.	particular period from the Agency's EU Cybersecurity Technical Situation Reports issued by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.	the Union, and a summary of the findings for the particular period from the Agency's EU Cybersecurity Technical Situation Reports issued by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.
Article 15(2a)					
G	298a		***2a. ENISA, in cooperation with the Commission and with guidance from the Cooperation Group and the CSIRTs network, shall prepare the methodology including the relevant variables of the cybersecurity index referred to in paragraph 1, point (c).***		***2a. ENISA, in cooperation with the Commission, the Cooperation Group and the CSIRTs network, shall develop the methodology, including the relevant variables, such as quantitative and qualitative indicators of the aggregated assessment referred to in paragraph 1, point (c).***
Article 16					
G	299	Article 16 Peer-reviews	Article 16 Peer-reviews	Article 16 ~~*Peer-reviews*~~***Peer-learnings***	Article 16 Peer-reviews Text of article 16 in 4th column reflects a former Presidency proposal. Text Origin: Commission Proposal + Annexes
Article 16(1), introductory part					

Y	300	1. The Commission shall establish, after consulting the Cooperation Group and ENISA, and at the latest by 18 months following the entry into force of this Directive, the methodology and content of a peer-review system for assessing the effectiveness of the Member States' cybersecurity policies. The reviews shall be conducted by cybersecurity technical experts drawn from Member States different than the one reviewed and shall cover at least the following:	1. The Commission shall establish, after consulting the Cooperation Group and ENISA, and at the latest by **… [**18 months following the entry into force of this Directive**]**, the methodology and content of a peer-review system for assessing the effectiveness of the Member States' cybersecurity policies. The ~~reviews~~**peer-reviews** shall be conducted **in consultation with ENISA** by cybersecurity technical experts drawn from **at least two** Member States different than the one reviewed and shall cover at least the following:	1. **With a view to strengthening mutual trust, achieving a high common level of cybersecurity, as well as strengthening the Member States' cybersecurity capabilities and policies necessary for effectively implementing this Directive, the Cooperation Group** ~~The Commission~~ shall establish, **with the support of the Commission and** after consulting **ENISA, and, where relevant, the CSIRTs network** ~~the Cooperation Group and ENISA~~, and at the latest by ~~18~~**24** months following the entry into force of this Directive, the methodology ~~and content of a peer-review~~**for an objective, non-discriminatory and fair peer-learning** system ~~for assessing the effectiveness of the Member States' cybersecurity policies. The reviews~~**concerning the Member States' implementation of this Directive. Participation in the peer-learning is voluntary. The system** shall ~~be~~**consist of assessment rounds** conducted by cybersecurity ~~technical~~ experts drawn from Member States ~~different than the one reviewed~~ and shall cover **one or several of** ~~at least~~ the following **aspects**:	1. The ~~Commission~~ **Cooperation Group** shall establish, ~~after consulting the Cooperation Group~~**with the support of the Commission** and ENISA **, and where relevant the CSIRT network** ~~, and~~ at the latest **[by 24**~~by 18~~ months following the entry into force of this Directive**]**, the methodology and ~~content~~**organisational aspects** of a peer-review ~~system for assessing the effectiveness of the~~**with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing** Member States' cybersecurity **capabilities and** policies **necessary to implement this Directive. Participation in the peer-reviews is voluntary. The peer-reviews**~~. The reviews~~ shall be conducted by cybersecurity ~~technical experts drawn from~~**experts assigned by at least two** Member States**,** different ~~than the one~~**from the Member State being** reviewed and shall cover at least **one of** the following: **]** EP: If peer-reviews are voluntary, all MS shall carry out a self-assessment.	Y

					PCY suggests a recital encouraging MS to carry out self-assessments.
Article 16(1)(i)					
G	301	(i) the effectiveness of the implementation of the cybersecurity risk management requirements and reporting obligations referred to in Articles 18 and 20;	(i) the effectiveness of the implementation of the cybersecurity risk management requirements and reporting obligations referred to in Articles 18 and 20;	(i) ~~*the effectiveness of*~~ the implementation of the cybersecurity risk management requirements and reporting obligations referred to in Articles 18 and 20;	(i) the ~~*effectiveness of the*~~***level of*** implementation of the cybersecurity risk management requirements and reporting obligations referred to in Articles 18 and 20;
Article 16(1)(ii)					
Y	302	(ii) the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the national competent authorities;	(ii) the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the national competent authorities;	(ii) the ~~*level of*~~ capabilities, including the available ~~*financial, technical and human*~~ resources, and the ~~*effectiveness of the*~~ exercise of the tasks of the national competent authorities ***referred to in Article 8 and CSIRTs referred to in Article 9***;	(ii) the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the national competent authorities; Council check
Article 16(1)(iii)					
G	303	(iii) the operational capabilities and effectiveness of CSIRTs;	(iii) the operational capabilities and effectiveness of CSIRTs ***in executing their tasks***;	(iii) ~~*the operational capabilities and effectiveness of CSIRTs;*~~	(iii) the operational capabilities ~~*and effectiveness*~~ of CSIRTs;
Article 16(1)(iii)					
G	304				

		(iv) the effectiveness of mutual assistance referred to in Article 34;	(iv) the effectiveness of mutual assistance referred to in Article 34;	(~~iv~~***iii***) the ~~effectiveness~~***implementation*** of mutual assistance referred to in Article 34;	(iv) the ~~effectiveness~~***level of implementation*** of mutual assistance referred to in Article 34;
	Article 16(1)(iv)				
G	305	(v) the effectiveness of the information-sharing framework, referred to in Article 26 of this Directive.	(v) the effectiveness of the information-sharing framework, referred to in Article 26 of this Directive.	~~(v)~~***(iv) the implementation*** ~~the effectiveness~~ of the information-sharing framework, referred to in Article 26 ~~of this Directive~~.	(v) the ~~effectiveness~~***level of implementation*** of the information-sharing framework, referred to in Article 26 ~~of this Directive.~~***;***
	Article 16(1)(Va)				
G	305a				***(vi) specific issues of cross-border or cross-sector nature.***
	Article 16(2)				
G	306	2. The methodology shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States shall designate experts eligible to carry out the peer reviews. ENISA and the Commission shall designate experts to participate as observers in the peer-reviews. The Commission, supported by ENISA, shall establish within the methodology as referred to in	2. The methodology shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States shall designate experts eligible to carry out the peer reviews. ENISA and the Commission shall designate experts to participate as observers in the peer-reviews. The Commission, supported by ENISA, shall establish within the methodology as referred to in	2. The ~~methodology shall include objective, non-discriminatory, fair and transparent criteria on the basis of~~ ***criteria based on*** which ~~the~~ Member States ~~shall~~***are to*** designate experts eligible to ~~carry out the peer reviews. ENISA and the Commission~~***participate in the peer-learning rounds*** shall ~~designate experts to participate as observers in the peer-reviews. The Commission, supported by~~	2. The methodology shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States ~~shall~~ designate experts eligible to carry out the peer reviews. ENISA and the Commission shall ~~designate experts to~~ participate as observers in the peer-reviews. ~~The Commission, supported by ENISA, shall establish within the methodology as referred to in~~

	paragraph 1 an objective, non-discriminatory, fair and transparent system for the selection and the random allocation of experts for each peer review.	paragraph 1 an objective, non-discriminatory, fair and transparent system for the selection and the random allocation of experts for each peer review.	~~ENISA,~~**~~be objective, non-discriminatory, fair and transparent and~~** shall ~~establish within~~**~~be included in~~** the methodology ~~as~~ referred to in paragraph 1 ~~an objective, non-discriminatory, fair and transparent system for the selection and the random allocation of experts for each peer review~~**. ENISA and the Commission may designate experts to participate as observers in the peer-learning rounds**.	~~paragraph 1 an objective, non-discriminatory, fair and transparent system for the selection and the random allocation of experts for each peer review.~~
Article 16(2a)				
306a				
Article 16(3)				
307	3. The organisational aspects of the peer reviews shall be decided by the Commission, supported by ENISA, and, following consultation of the Cooperation Group, be based on criteria defined in the methodology referred to in paragraph 1. Peer reviews shall assess the aspects referred to in paragraph 1 for all Member States and sectors, including targeted issues specific to one or several	3. The organisational aspects of the peer reviews shall be decided by the Commission, supported by ENISA, and, following consultation of the Cooperation Group, be based on criteria defined in the methodology referred to in paragraph 1. Peer reviews shall assess the aspects referred to in paragraph 1 for all Member States and sectors, including targeted issues specific to one or several	3. ~~The organisational aspects of the peer reviews shall be decided by the Commission, supported by ENISA, and, following consultation of the Cooperation Group, be based on criteria defined in the methodology referred to in paragraph 1. Peer reviews shall assess the aspects referred to in paragraph 1 for all Member States and sectors, including targeted issues specific to one or several~~	3. ~~The organisational aspects of the peer reviews shall be decided by the Commission, supported by ENISA, and, following consultation~~**Member States may identify specific issues mentioned in paragraph 1 (vi) to be reviewed. The scope** of the ~~Cooperation Group, be based on criteria defined in the methodology referred to in paragraph 1. Peer reviews shall assess the aspects~~

		Member States or one or several sectors.	Member States or one or several sectors. ***The designated experts carrying out the review shall communicate these targeted issues to the Member State under peer-review, prior to its commencement.***	~~*Member States or one or several sectors.*~~	~~*referred to in paragraph 1 for all*~~***review, including identified issues, shall be communicated to the participating*** Member States ~~*and sectors, including targeted issues specific to one or several Member States or one or several sectors*~~***prior to the commencement of the peer review***.
	Article 16(3a)				
Y	307a			***3a. Prior to the commencement of the peer-learning rounds, Member States may carry out a self-assessment of the aspects covered by that particular peer learning round and provide that self-assessment to the designated experts referred to in paragraph 2.***	***3a. Prior to the commencement of the peer-review, Member State may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated experts. The methodology for the self-assessment shall be defined by the Cooperation Group, with the support of the Commission and ENISA.*** To be looked at together with §1.
	Article 16(3a)				
Y	307b		***3a. Prior to the commencement of the peer-review process, the Member State under to the peer-review shall carry out a self-assessment of the reviewed aspects***		To be looked at together with §1.

			and provide that self-assessment to the designated experts.		
Article 16(4)					
G	308	4. Peer reviews shall entail actual or virtual on-site visits and off-site exchanges. In view of the principle of good cooperation, the Member States being reviewed shall provide the designated experts with the requested information necessary for the assessment of the reviewed aspects. Any information obtained through the peer review process shall be used solely for that purpose. The experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of that review to any third parties.	4. Peer reviews shall entail actual or virtual on-site visits and off-site exchanges. In view of the principle of good cooperation, the Member States being reviewed shall provide the designated experts with the requested information necessary for the assessment of the reviewed aspects. ***The Commission, in cooperation with ENISA, shall develop appropriate codes of conduct underpinning the working methods of designated experts.*** Any information obtained through the peer review process shall be used solely for that purpose. The experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of that review to any third parties.	4. ~~*Peer reviews shall*~~***Peer-learnings may*** entail ~~*actual*~~***physical*** or virtual on-site visits and off-site exchanges. In view of the principle of good cooperation, the Member States ~~*being reviewed*~~***taking part in the peer-learning*** shall provide the designated experts with the ~~*requested*~~ information necessary for the assessment***, without prejudice to national or Union laws concerning protection of confidential or classified information or to safeguarding essential State functions, such as national security*** ~~*of the reviewed aspects*~~. Any information obtained through the ~~*peer review*~~***peer-learning*** process shall be used solely for that purpose. The experts participating in the ~~*peer review*~~***peer-learning*** shall not disclose any sensitive or confidential information obtained in ***that context to any third parties. The Member State participating in the peer-learning may object to the designation of particular***	4. Peer reviews shall entail ~~*actual*~~***physical*** or virtual on-site visits and off-site exchanges. ~~-~~ In view of the principle of good cooperation, the Member ~~*States being reviewed*~~***State subject to the peer review*** shall provide the designated experts with the ~~*requested*~~ information necessary for the assessment***, without prejudice to national or Union laws concerning protection of confidential or classified information or to safeguard essential State functions, such as national security. The Cooperation Group, in cooperation with the Commission and ENISA, shall develop appropriate codes of conduct underpinning the working methods of designated experts*** ~~*of the reviewed aspects*~~. Any information obtained through the peer review process shall be used solely for that purpose. The experts participating in the peer review shall not disclose any sensitive or confidential information obtained

				experts on duly justified grounds communicated to the Cooperation Group ~~*the course of that review to any third parties*~~.	in the course of that review to any third parties.
Article 16(5)					
G	309	5. Once reviewed in a Member State, the same aspects shall not be subject to further peer review within that Member State during the two years following the conclusion of a peer review, unless otherwise decided by the Commission, upon consultation with ENISA and the Cooperation Group.	5. Once reviewed in a Member State, the same aspects shall not be subject to further peer review within that Member State during the two years following the conclusion of a peer review, unless otherwise decided by the Commission, upon consultation with ENISA and the Cooperation Group.	5. Once ~~*reviewed in a Member State*~~***subject to a peer-learning round***, the same aspects shall not be subject to further ~~*peer review within that*~~***peer-learning rounds for the participating*** Member ~~*State*~~***States*** during the ~~*two*~~***four*** years following the conclusion of ~~*a peer review*~~***that peer- learning round***, unless ~~*otherwise decided by the Commission, upon consultation with ENISA and*~~***the Member State concerned requests it or agrees upon proposal by*** the Cooperation Group.	5. Once ~~*reviewed in a Member State*~~***subject to a peer-review***, the same aspects ***reviewed in a Member State,*** shall not be subject to further ~~*peer*~~ review ~~*within*~~***in*** that Member State ~~*during*~~***for*** the two years following the conclusion of ~~*a*~~***the*** peer review, unless otherwise ~~*decided*~~***requested*** by the ~~*Commission, upon consultation with ENISA and*~~***Member State or agreed upon after a proposal by*** the Cooperation Group.
Article 16(6)					
G	310	6. Member State shall ensure that any risk of conflict of interests concerning the designated experts are revealed to the other Member States, the Commission and ENISA without undue delay.	6. Member State shall ensure that any risk of conflict of interests concerning the designated experts are revealed to the other Member States, the Commission and ENISA, ***before the commencement of the peer-review process*** ~~*without undue delay*~~.	6. ~~*Member State shall ensure that any risk of conflict of interests concerning the designated experts are revealed to the other Member States, the Commission and ENISA without undue delay.*~~	6. Member ~~*State*~~***States*** shall ensure that any risk of conflict of interests concerning the designated experts are revealed to the other Member States, the ***Cooperation Group, the*** Commission and ENISA, ***before the commencement of the peer-***

					review. The Member State subject to the peer-review may object to the designation of particular experts on duly justified grounds communicated to the designating Member State ~~*without undue delay*~~.
Article 16(7)					
G	311	7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews. The reports shall be submitted to the Commission, the Cooperation Group, the CSIRTs network and ENISA. The reports shall be discussed in the Cooperation Group and the CSIRTs network. The reports may be published on the dedicated website of the Cooperation Group.	7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews. The reports ***include recommendations to enable improvement on the aspects covered by the peer-review process. The reports*** shall be submitted to the Commission, the Cooperation Group, the CSIRTs network and ENISA. The reports shall be discussed in the Cooperation Group and the CSIRTs network. The reports may be published on the dedicated website of the Cooperation Group***, excluding sensitive and confidential information***.	7. Experts participating in ~~*peer reviews*~~***peer-leaning rounds*** shall draft reports on the findings and conclusions of the ~~*reviews. The reports*~~***assessments. Member States*** shall be ~~*submitted to the Commission, the Cooperation Group, the CSIRTs network and ENISA. The*~~ ***allowed to provide comments on their respective draft reports, which shall be attached to the report. The final*** reports shall be ~~*discussed in*~~***submitted to*** the Cooperation ~~*Group and the CSIRTs network. The reports may be published on the dedicated website of the Cooperation Group*~~***GroupMember States may decide to make their respective reports publicly available***.	7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews. ~~*The*~~***Member States shall be allowed to provide comments on their respective draft*** reports***, which*** shall be ~~*submitted*~~***attached*** to the ~~*Commission, the Cooperation Group, the CSIRTs network and ENISA*~~***reports. The reports shall include recommendations to enable improvement on the aspects covered by the peer-review***. The reports shall be ~~*discussed in*~~***presented to*** the Cooperation Group and the CSIRTs network ***when relevant. The Member State under review may decide to make its report, or a redacted version of its report, publicly available***~~*. The reports may be published on the dedicated website of the Cooperation Group*~~.	G

CHAPTER IV					
G	312	CHAPTER IV Cybersecurity risk management and reporting obligations	CHAPTER IV Cybersecurity risk management and reporting obligations	CHAPTER IV Cybersecurity risk management and reporting obligations	CHAPTER IV Cybersecurity risk management and reporting obligations Text Origin: Commission Proposal + Annexes	G
SECTION I					
G	313	SECTION I Cybersecurity risk management and reporting	SECTION I Cybersecurity risk management and reporting	SECTION I Cybersecurity risk management and reporting	SECTION I Cybersecurity risk management and reporting Text Origin: Commission Proposal + Annexes	G
Article 17					
G	314	Article 17 Governance	Article 17 Governance	Article 17 Governance	Article 17 Governance Text Origin: Commission Proposal + Annexes	G
Article 17(1)					
G	315	1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by	1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in	1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in	1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in	G

		those entities in order to comply with Article 18, supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.	order to comply with Article 18, supervise its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.	order to comply with Article 18, ~~supervise~~***oversee*** its implementation and ***can be held*** ~~be~~ accountable for the non-compliance by the entities with the obligations under this Article. ***The application of this paragraph shall be without prejudice to the Member State's national laws as regards the liability rules in public institutions, as well as the liability of public servants and elected and appointed officials.***	order to comply with Article 18, ~~supervise~~***oversee*** its implementation and ***can be held liable*** ~~be accountable~~ for the non-compliance by the entities with the obligations under this Article. ***The application of this paragraph shall be without prejudice to the Member State's national laws as regards the liability rules in public institutions, as well as the liability of public servants and elected and appointed officials.*** Text Origin: Council Mandate
Article 17(2)					
G	316	2. Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity.	2. Member States shall ensure that members of the management body ***of essential and important entities*** follow specific ~~trainings,~~ ***training, and shall encourage essential and important entities to offer similar training to all employees*** on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the ~~operations of~~***services provided by*** the entity.	2. Member States shall ensure that ***the*** members of the management body ~~follow specific~~***are required to follow*** trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity.	2. Member States shall ensure that ***the*** members of the management body ~~follow specific trainings,~~ ***of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to all employees*** on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the ~~operations of~~***services provided by*** the entity.
Article 18					

G	317	Article 18 Cybersecurity risk management measures	Article 18 Cybersecurity risk management measures	Article 18 Cybersecurity risk management measures	Article 18 Cybersecurity risk management measures Text Origin: Commission Proposal + Annexes	G
	Article 18(1a)					
G	317a			***1a. This Directive applies an "all-hazard" approach that includes the protection of network and information systems and their physical environment from any event that could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of services offered by, or accessible via, network and information systems.***	Moved to §2	G
	Article 18(1)					
Y	318	1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the	1. Member States shall ensure that essential and important entities ~~*shall*~~ take appropriate and proportionate technical, ***operational*** and organisational measures to manage the risks posed to the security of network and information systems which	1. Member States shall ensure that essential and important entities ~~*shall*~~ take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network~~-~~, and information systems which those entities use in the	1. Member States shall ensure that essential and important entities ~~*shall*~~ take appropriate and proportionate technical, ***operational*** and organisational measures to manage the risks posed to the security of network and information systems which	Y

		provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.	those entities use ~~in~~***for their operations or for*** the provision of their services ***and prevent or minimise the impact of incidents on recipients of their services and on other services***. Having regard to the state of the art ***and to European or international standards***, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.	provision of their services. Having regard to the state of the art ***and the cost of implementation***, those measures shall ensure a level of security of network and information systems appropriate to the risk presented. ***When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, its size, the likelihood of occurrence of incidents and their severity. Having regard of the level and type of the risk posed to society in the event of incidents affecting essential or important entities, cybersecurity risk management measures imposed on important entities may be less stringent than those imposed on essential entities.***	those entities use ~~in~~***for their operations or for*** the provision of their services~~.~~***, and to prevent or minimise the impact of incidents on recipients of their services and on other services.*** Having regard to the state of the art ***and, where applicable, relevant European and international standards, as well as the cost of implementation***, those measures shall ensure a level of security of network and information systems appropriate to the risk presented. ***When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, its size, the likelihood of occurrence of incidents and their severity, including their societal and economic impact.*** EP and Council to check
Article 18(2), introductory part					
G	319	2. The measures referred to in paragraph 1 shall include at least the following:	2. The measures referred to in paragraph 1 shall include at least the following:	2. The measures referred to in paragraph 1 shall include at least the following:	2. The measures referred to in paragraph 1 shall ***be based on an all-hazards approach aiming to protect network and information systems and their physical environment from incidents, and*** G

					shall include at least the following: Text Origin: Commission Proposal + Annexes
Article 18(2), point (a)					
G	320	(a) risk analysis and information system security policies;	(a) risk analysis and information system security policies;	(a) risk analysis and information system security policies;	(a) risk analysis and information system security policies; Text Origin: Commission Proposal + Annexes
Article 18(2), point (b)					
G	321	(b) incident handling (prevention, detection, and response to incidents);	(b) incident handling ~~*(prevention, detection, and response to incidents)*~~;	(b) incident handling (prevention, detection, ***response and recovery from*** ~~*and response to*~~ incidents);	(b) incident handling ~~*(prevention, detection, and response to incidents)*~~; Text Origin: EP Mandate
Article 18(2), point (c)					
G	322	(c) business continuity and crisis management;	(c) business continuity***, such as backup management and disaster recovery,*** and crisis management;	(c) business continuity and crisis management;	(c) business continuity***, such as backup management and disaster recovery,*** and crisis management; Text Origin: EP Mandate
Article 18(2), point (d)					
G	323	(d) supply chain security including security-related aspects concerning	(d) supply chain security including security-related aspects concerning	(d) supply chain security including security-related aspects concerning	(d) supply chain security including security-related aspects concerning

		the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;	the relationships between each entity and its suppliers or service providers ~~such as providers of data storage and processing services or managed security services~~;	the relationships between each entity and its ***direct*** suppliers or service providers such as providers of data storage and processing services or managed security services;	the relationships between each entity and its ***direct*** suppliers or service providers ~~such as providers of data storage and processing services or managed security services~~; Deletion moved to recital 43 Text Origin: Council Mandate
	Article 18(2), point (e)				
G	324	(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure; Text Origin: Commission Proposal + Annexes
	Article 18(2), point (f)				
G	325	(f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;	(f) policies and procedures (***training,*** testing and auditing) to assess the effectiveness of cybersecurity risk management measures;	(f) policies and procedures ~~(testing and auditing)~~ to assess the effectiveness of cybersecurity risk management measures;	(f) policies and procedures ~~(testing and auditing)~~ to assess the effectiveness of cybersecurity risk management measures; Consider a recital to cover the elements Text Origin: Council Mandate

	Article 18(2), point (fa)				
G	325a		***(fa) basic computer hygiene practices and cybersecurity training;***		***(fa) basic computer hygiene practices and cybersecurity training;*** recital 45a Text Origin: EP Mandate
	Article 18(2), point (g)				
G	326	(g) the use of cryptography and encryption.	(g) the use of cryptography***, such as*** ~~*and*~~ encryption~~.~~***, where appropriate;***	(g) ~~*the use of*~~***policy on the useof*** cryptography and encryption~~.~~***;***	(g) ***policies and procedures regarding*** the use of cryptography and***, where appropriate,*** encryption~~.~~***;*** Text Origin: EP Mandate
	Article 18(2), point (ga)				
G	326a			***(ga) human resources security, access control policies and asset management.***	***(ga) human resources security, access control policies and asset management.*** Text Origin: Council Mandate
	Article 18(2), point (ga)				
G	326b		***(ga) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text***		***(ga) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text***

			communications and secured emergency communications systems within the entity, where appropriate.		***communications and secured emergency communications systems within the entity, where appropriate.*** Text Origin: EP Mandate
Article 18(3)					
G	327	3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities ~~*shall*~~***are required to*** take into account the vulnerabilities specific to each ***direct*** supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. ***Member States shall also ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities are required to take into account the results of the coordinated risk assessments carried out in accordance with Article 19 (1).***	3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities ~~*shall*~~ take into account the vulnerabilities specific to each ***direct*** supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. ***Member States shall also ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities are required to take into account the results of the coordinated risk assessments carried out in accordance with Article 19 (1).*** Text Origin: Council Mandate	G
Article 18(4)					

G	328	4. Member States shall ensure that where an entity finds that respectively its services or tasks are not in compliance with the requirements laid down in paragraph 2, it shall, without undue delay, take all necessary corrective measures to bring the service concerned into compliance.	4. Member States shall ensure that where an entity finds that respectively its services or tasks are not in compliance with the requirements laid down in paragraph 2, it shall, without undue delay, take all necessary, ***appropriate and proportionate*** corrective measures to bring the service concerned into compliance.	4. Member States shall ensure that where an entity finds that respectively its services or tasks are not in compliance with the requirements laid down in paragraph 2, it shall, without undue delay, take all necessary corrective measures to bring the service concerned into compliance.	4. Member States shall ensure that where an entity finds that respectively its services or tasks are not in compliance with the requirements laid down in paragraph 2, it shall, without undue delay, take all necessary, ***appropriate and proportionate*** corrective measures to bring the service concerned into compliance. Text Origin: EP Mandate	G
	Article 18(5)					
R	329	5. The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.	~~*5. The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.*~~	5. The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications***, as well as sectoral specificities, as necessary,*** of the elements referred to in paragraph 2 ***of this Article. The Commission shall adopt by [18 months after the entry into force of this Directive] implementing acts in order to lay down the technical and the methodological specifications for entities referred to in Article 24(1) and trust service providers referred to in point 8 of Annex I. Those implementing acts***~~*. Where preparing those acts, the*~~	Should be discussed in relation to the political discussion on DA/IA	R

				~~Commission~~ shall ~~proceed~~***be adopted*** in accordance with the examination procedure referred to in Article 37(2). ***When preparing such implementing acts, the Commission shall*** ~~and follow~~, to the greatest extent possible, ***follow*** international and European standards, as well as relevant technical specifications ***and exchange advice with the Cooperation Group and ENISA on the draft implementing act in accordance with Article 12(4)(d)***.	
Article 18(6)					
R	330	6. The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities.	6. The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 ***of this Article*** to take account of new cyber threats, technological developments or sectorial specificities ***as well as to supplement this Directive by laying down the technical and the methodological specifications of the measures referred to in paragraph 2 of this Article***.	6. ~~The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities.~~	Same as the previous one	R
Article 19					
G	331				G

		Article 19 EU coordinated risk assessments of critical supply chains	Article 19 EU coordinated risk assessments of critical supply chains	Article 19 EU coordinated risk assessments of critical supply chains	Article 19 EU coordinated risk assessments of critical supply chains Text Origin: Commission Proposal + Annexes
	Article 19(1)				
G	332	1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.	1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT ***and information and communication system (ICS)*** services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.	1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.	1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors. Text Origin: Commission Proposal + Annexes
	Article 19(2)				
G	333	2. The Commission, after consulting with the Cooperation Group and ENISA, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.	2. The Commission, after consulting ~~with~~ the Cooperation Group and ENISA, ***and, where applicable, relevant stakeholders,*** shall identify the specific critical ICT ***and ICS*** services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.	2. The Commission, after consulting with the Cooperation Group and ENISA, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.	2. The Commission, after consulting ~~with~~ the Cooperation Group and ENISA***, and, where necessary, relevant stakeholders***, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.

Article 20					
G	334	Article 20 Reporting obligations	Article 20 Reporting obligations	Article 20 Reporting obligations	Article 20 Reporting obligations Text Origin: Commission Proposal + Annexes
Article 20(1)					
G	335	1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.	1. Member States shall ensure that essential and important entities notify, without undue delay, the ~~competent authorities or the~~ CSIRT in accordance with paragraphs 3 and 4 of any ~~incident having a~~ significant ~~impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service~~***incident***. Member States shall ensure that those entities report, among others, any information enabling ~~the competent authorities or~~ the CSIRT to determine any cross-border impact of the incident.	1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of ***these*** incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident. ***The act of the notification in itself shall not make the notifying entity subject to increased liability.***	1. Member States shall ensure that essential and important entities notify, without undue delay~~, the competent authorities or the CSIRT~~ ***the CSIRT or, where relevant, the competent authority*** in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of ***those*** incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, ~~among others~~***inter alia***, any information enabling the ~~competent authorities or the CSIRT~~***CSIRT and the competent authority*** to determine any cross-border impact of the incident. ***The mere act of notification shall not subject the notifying entity to***

					increased liability. ***Where the entities concerned do not notify the CSIRT in accordance with paragraph 4, Member States shall ensure that the competent authority forward the notification to the CSIRT upon receipt.*** ***In the case of a cross-border or cross-sectorial incident, Member States shall ensure that the single point of contact is provided in due time with relevant information notified in accordance with paragraph 4.*** (Recital to be added on encouraging automated system).
Article 20(2)					
G	336	2. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident.	2. ~~*Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident.*~~	2. ~~*Member States shall ensure that*~~***Where applicable, the*** essential and important entities ***shall*** notify, without undue delay, the ~~*competent authorities or the CSIRT of any*~~***recipients of their services that are potentially affected by a*** significant cyber threat ***of any measures or remedies*** that those ***recipients can take in response to that threat. Where appropriate,***	2. ~~*Member States shall ensure that*~~***Where applicable,*** essential and important- entities ~~*notify*~~***shall communicate***, without undue delay, the ~~*competent authorities or the CSIRT of any*~~***recipients of their services that are potentially affected by a*** significant cyber threat ***any measures or remedies*** that those ~~*entities identify that could have potentially resulted in a*~~

				the entities ~~*identify that could have potentially resulted in a significant incident*~~***shall also notify those recipients of the threat itself. The act of the notification in itself shall not make the notifying entity subject to increased liability***.	~~*significant incident*~~***recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the threat itself***.
Article 20(2), first paragraph					
G	337	Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.	Where applicable, ~~*those entities*~~***Member States*** shall ~~*notify, without undue delay,*~~***ensure that essential and important entities inform*** the recipients of their services***, without undue delay, of protective measures or remedies to particular incidents and known risks, which can be taken by the recipients*** ~~*that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat*~~. Where appropriate, the entities shall ~~*also notify those recipients*~~***inform the recipients of their services*** of the ~~*threat*~~***incident or known risk*** itself. ~~*The notification*~~***Informing of recipients shall take place on a 'best efforts' basis and*** shall not ~~*make*~~***subject*** the notifying entity ~~*subject to increased*~~***to an increase in*** liability.	~~*Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.*~~	Deleted, covered by line 337. COM to draft recital including 'best efforts'.	G

Article 20(3)				
338	3. An incident shall be considered significant if:	3. ~~An~~***In order to determine the significance of the*** incident***, where available, the following parameters*** shall be ~~considered significant if~~***taken into account***:	3. An incident shall be considered significant if:	3. An incident shall be considered significant if: Text Origin: Commission Proposal + Annexes
Article 20(3), point (a)				
339	(a) the incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned;	(a) the ~~incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned~~***number of recipients of the services affected by the incident***;	(a) the incident has caused or has the potential to cause ~~substantial~~ ***severe*** operational disruption ***of the service*** or financial losses for the entity concerned;	(a) the incident has caused or ~~has the potential to cause substantial~~***is capable of causing severe*** operational disruption ***of the service*** or financial losses for the entity concerned;
Article 20(3), point (b)				
340	(b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.	(b) the ~~incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses~~ ***duration of the incident;***	(b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.	(b) the incident has affected or ~~has the potential to affect~~***is capable of affecting*** other natural or legal persons by causing considerable material or non-material losses. Text Origin: Commission Proposal + Annexes
Article 20(3), point (ba)				

G	340a		***(ba) the geographical spread of the area affected by the incident;***		deleted	G
	Article 20(3), point (bb)					
G	340b		***(bb) the extent to which the functioning and continuity of the service is affected by the incident;***		deleted	G
	Article 20(3), point (bc)					
G	340c		***(bc) the extent of the impact of the incident on economic and societal activities.***		deleted	G
	Article 20(4), introductory part					
G	341	4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities or the CSIRT:	4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the ~~*competent authorities or the*~~ CSIRT:	4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities or the CSIRT:	4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the ~~*competent authorities or the CSIRT*~~***CSIRT or, where relevant, the competent authority***:	G
	Article 20(4), point (a)					
Y	342	(a) without undue delay and in any event within 24 hours after having become aware of the incident, an	(a) ~~*without undue delay and in any event within 24 hours after having become aware*~~***an initial***	(a) without undue delay and in any event within 24 hours after having become aware of the incident, an	(a) ~~*without undue delay and in any event within 24 hours after having become aware*~~***an initial***	Y

		initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;	***notification*** of the ***significant*** incident, ~~*an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;*~~ ***shall contain information available to the notifying entity on a best efforts basis as follows:***	initial notification ***as an early warning***, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;	***notification*** of the ***significant*** incident, ~~*an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;*~~***containing information available to the notifying entity on a best efforts basis as follows:***
	Article 20(4), point (a)(i)				
˅	342a		***(i) with regard to incidents that significantly disrupt the availability of the services provided by the entity, the CSIRT shall be notified without undue delay and in any event within 24 hours of becoming aware of the incident;***		***(i) with regard to incidents that significantly disrupt the availability of the services provided by the entity concerned or in the case of a ransomware attack, the CSIRT or the competent authority shall be notified without undue delay and in any event within 24 hours of the entity concerned becoming aware of the incident;***
	Article 20(4), point (a)(ii)				
˅	342b		***(ii) with regard to incidents that have a significant impact on the entity other than on the availability of the services provided by that entity, the CSIRT shall be notified without undue delay and in any event within 72***		***(ii) with regard to incidents that have a significant impact on the entity other than on the availability of the services provided by that entity without undue delay and in any event within 72 hours of the entity***

			hours of becoming aware of the incident;		***concerned becoming aware of the incident;*** EP to provide new text
Article 20(4), point (a)(iii)					
Y	342c		***(iii) with regard to incidents that have a significant impact on the services of a trust services provider as defined in Article 3, point (19) of Regulation (EU) No 910/2014 or on the personal data maintained by that trust service provider, the CSIRT shall be notified without undue delay and in any event within 24 hours of becoming aware of the incident;***		***(iii) with regard to incidents that have a significant impact on the services of a trust service provider as defined in Article 3, point (19) of Regulation (EU) No 910/2014 or on the personal data maintained by that trust service provider, the CSIRT shall be notified without undue delay and in any event within 24 hours of becoming aware of the incident;***
Article 20(4), point (b)					
G	343	(b) upon the request of a competent authority or a CSIRT, an intermediate report on relevant status updates;	(b) ~~*upon the request of a competent authority or a CSIRT,*~~ an intermediate report on relevant status updates***, upon the request of a CSIRT***;	(b) upon the request of a competent authority or a CSIRT, an intermediate report on relevant status updates;	(b) upon the request of a ~~*competent authority or a CSIRT*~~***CSIRT or the competent authority***, an intermediate report ***including indicators of compromise*** on relevant status updates;
Article 20(4), point (c), introductory part					
G	344	(c) a final report not later than one	(c) a ~~*final*~~***comprehensive*** report	(c) a final report not later than one	(c) a final report not later than one

		month after the submission of the report under point (a), including at least the following:	not later than one month after the submission of the ~~report under point (a)~~***initial notification***, including at least the following:	month after the submission of the ~~report~~***initial notification*** under point (a), including at least the following:	month after the submission of the ~~report~~***initial notification*** under point (a), including at least the following: Text Origin: Council Mandate
	Article 20(4), point (c)(i)				
G	345	(i) a detailed description of the incident, its severity and impact;	(i) a detailed description of the incident, its severity and impact;	(i) a detailed description of the incident, its severity and impact;	(i) a detailed description of the incident, its severity and impact; Text Origin: Commission Proposal + Annexes
	Article 20(4), point (c)(ii)				
G	346	(ii) the type of threat or root cause that likely triggered the incident;	(ii) the type of threat or root cause that likely triggered the incident;	(ii) the type of threat or root cause that likely triggered the incident;	(ii) the type of threat or root cause that likely triggered the incident; Text Origin: Commission Proposal + Annexes
	Article 20(4), point (c)(iii)				
G	347	(iii) applied and ongoing mitigation measures.	(iii) applied and ongoing mitigation measures.	(iii) applied and ongoing mitigation measures.	(iii) applied and ongoing mitigation measures. Text Origin: Commission Proposal + Annexes
	Article 20(4), point (ca)				
G	347a				

			(ca) in the case of an ongoing incident at time of the submission of the comprehensive report referred to in point (c), a final report shall be provided one month after the incident has been resolved.		***In cases of ongoing incidents at the time of the submission of the final report referred to in point (c), Member States shall ensure that entities provide a comprehensive report at that time and a final report within one month after the incident has been handled.*** EP proposal to include paragraph 4a Member States shall establish a single entry point (EP) line 348a ("shall/may") + recital on the intent of the single entry point
Article 20(4), first paragraph					
G	348	Member States shall provide that in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines laid down in points (a) and (c).	Member States shall provide that in duly justified cases and in agreement with the ~~*competent authorities or the*~~ CSIRT, the entity concerned can deviate from the deadlines laid down in points ~~*(a) and (c).*~~ ***(a)(i) and (ii) and point (c). Member States shall ensure the confidentiality and appropriate protection of sensitive information about incidents shared with CSIRTs, and shall adopt measures and procedures for sharing and reuse of incident information.***	Member States shall provide that in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines laid down in points (a) and (c). ***In particular, a deviation from the deadline referred to in point (c) can be justified in cases where the incident is still ongoing.***	Deleted.

	Article 20(4a)				
Y	348a		***4a. Member States shall establish a single entry point for all notifications required under this Directive and other relevant Union law. ENISA, in cooperation with the Cooperation Group, shall develop and continuously improve common notification templates by means of guidelines to simplify and streamline the reporting information required under Union law and decrease the burden on reporting entities.***		Y
	Article 20(4b)				
G	348b		***4b. Essential and important entities referred to in Article 24(1) may meet the requirements of paragraph 1 of this Article by notifying the CSIRT of the Member State in which the entities have the main establishment within in the Union, and by notifying the essential and important entities they provide services to of any significant incident that is known to impact the recipient of the services.***	Deleted.	G

Article 20(5)				
349	5. The competent national authorities or the CSIRT shall provide, within 24 hours after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures. Where the CSIRT did not receive the notification referred to in paragraph 1 , the guidance shall be provided by the competent authority in collaboration with the CSIRT. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.	5. ~~*The competent national authorities or*~~ The CSIRT shall provide, within 24 hours after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity, including initial feedback on the incident and, upon ***the*** request of the entity, guidance ***and actionable advice*** on the implementation of possible mitigation measures. ~~*Where the CSIRT did not receive the notification referred to in paragraph 1 , the guidance shall be provided by the competent authority in collaboration with the CSIRT. The*~~ CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the ~~*competent national authorities or the*~~ CSIRT shall also provide guidance on reporting the incident to law enforcement authorities. ***The CSIRT may share information on the incident with other important and essential entities, while ensuring the confidentiality of the information provided by the reporting entity.***	5. The competent national authorities or the CSIRT shall provide, ***without undue delay*** ~~*within 24 hours*~~ after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures. Where the CSIRT did not receive the notification referred to in paragraph 1-, the guidance shall be provided by the competent authority in collaboration with the CSIRT. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.	5. The ~~*competent national authorities*~~***CSIRT*** or the ~~*CSIRT*~~***competent national authority*** shall provide, ***without undue delay and where possible*** within 24 hours after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance ***or other operational advice*** on the implementation of possible mitigation measures. Where the CSIRT ~~*did not receive*~~***is not the initial recipient of*** the notification referred to in paragraph 1-, the guidance shall be provided by the competent authority in collaboration with the CSIRT. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the ~~*competent national authorities*~~***CSIRT*** or the ~~*CSIRT*~~***competent authority*** shall also provide guidance on reporting the incident to law enforcement authorities.

Article 20(6)				
350	6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States and ENISA of the incident. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.	6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the ~~competent authority or the~~ CSIRT shall inform the other affected Member States and ENISA of the incident ***and provide relevant information***. In so doing, the ~~competent authorities,~~ CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.	6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority***, the CSIRT*** or the ~~CSIRT~~***Single Point of Contact*** shall inform the other affected Member States and ENISA of the incident***. Such information shall include at least the elements provided for in paragraph (4) of this Article***. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.	6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the ***CSIRT, the*** competent authority***,*** or the ~~CSIRT~~***Single Point of Contact*** shall inform***, without undue delay,*** the other affected Member States and ENISA of the incident. ***Such information shall include at least the type of information received in accordance with paragraph 4.*** In so doing, the ~~competent authorities, CSIRTs~~ ***CSIRTs, competent authority,*** and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.
Article 20(7)				
351	7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident,	7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident,	7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident,	7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident,

		or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned may, after consulting the entity concerned, inform the public about the incident or require the entity to do so.	or where disclosure of the incident is otherwise in the public interest, the ~~competent authority or the~~ CSIRT, and where appropriate ~~the authorities or~~ the CSIRTs of other Member States concerned may, after consulting the entity concerned, inform the public about the incident or require the entity to do so.	or where disclosure of the incident is otherwise in the public interest, the competent authority or the CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned may, after consulting the entity concerned, inform the public about the incident or require the entity to do so.	or where disclosure of the incident is otherwise in the public interest, the ~~competent authority~~***CSIRT*** or the ~~CSIRT~~***competent authority***, and where appropriate the ~~authorities~~***CSIRTs*** or the ~~CSIRTs~~ ***competent authorities*** of other Member States concerned**,** may, after consulting the entity concerned, inform the public about the incident or require the entity to do so.
	Article 20(7a)				
G	351a		***7a. CSIRTs shall, without undue delay, provide the single point of contact and where relevant, the competent authorities, with the information on significant incidents notified in accordance with paragraph 1.***		Deleted.
	Article 20(8)				
Y	352	8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to paragraphs 1 and 2 to the single points of contact of other affected Member States.	8. At the request of the ~~competent authority or the~~ CSIRT, the single point of contact shall forward notifications received pursuant to ~~paragraphs 1 and 2~~ ***paragraph 1*** to the single points of contact of other affected Member States**,** ***while ensuring confidentiality and***	8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to ~~paragraphs 1 and 2~~***paragraph 1*** to the single points of contact of other affected Member States.	8. At the request of the ~~competent authority~~***CSIRT*** or the ~~CSIRT~~***competent authority*** , the single point of contact shall forward notifications received pursuant to ~~paragraphs 1 and 2~~ ***paragraph 1*** to the single points of contact of other affected

			appropriate protection of the information provided by the reporting entity.		Member States. ***In so doing, the CSIRTs, competent authority and the single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.*** Council check
Article 20(9)					
G	353	9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraphs 1 and 2 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.	9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with ~~*paragraphs 1 and 2 and in accordance with*~~***paragraph 1 of this Article and*** Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.	9. The single point of contact shall submit to ENISA ~~*on a monthly basis*~~ ***every six months*** a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with ~~*paragraphs*~~***paragraph*** 1 and ~~*2 and*~~ in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report. ***ENISA shall inform every six months the Cooperation Group and the CSIRTs network about its findings on the notifications received.***	9. The single point of contact shall submit to ENISA ~~*on a monthly basis*~~***every three months*** a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraphs 1 and 2 ***of this Article*** and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report. ***ENISA shall inform every six months the Cooperation Group and the CSIRTs network about its findings on notifications received.***

					Text Origin: Council Mandate
Article 20(10)					
G	354	10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with paragraphs 1 and 2 by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].	10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with ~~paragraphs 1 and 2~~***paragraph 1 of this Article and Article 27*** by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].	10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with paragraphs 1 and 2 by essential entities identified as critical entities, ***[***or as entities equivalent to critical entities,***]*** pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].	10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with ~~paragraphs~~***paragraph*** 1 and ~~2 by essential~~***Article 27 by*** entities identified as critical entities, ***[***or as entities equivalent to critical entities,***]*** pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]. Text Origin: EP Mandate	G
Article 20(11)					
R	355	11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing acts to further	11. The Commission, may adopt implementing acts further specifying the ~~type of information, the format and the~~ procedure of a notification submitted pursuant to ~~paragraphs 1 and 2. The Commission may also adopt implementing acts to further~~	11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing acts to further	11. The Commission, may adopt implementing acts further specifying the ~~type of information, the format and the~~ procedure of a notification submitted pursuant to ~~paragraphs~~***paragraph*** 1 and 2 ***of this Article and Article 27. With regard to entities referred to in***	R

		specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).	~~specify the cases in which an incident shall be considered significant as referred to in paragraph 3~~***paragraph 1 of this Article and Article 27***. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).	specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).	***Article 24 (1)b,*** ~~–~~the Commission ~~*may also adopt*~~ ***shall adopt by […months after the date of entry into force of this Directive (deadline for transposition)]*** implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3 ***and may also adopt such implementing acts with regards to other entities***. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2). D/IA political issue
Article 20(11a)					
R	355a		***11a. The Commission is empowered to adopt delegated acts, in accordance with Article 36, to supplement this Directive by specifying the type of information to be submitted pursuant to paragraph 1 of this Article and by further specifying the parameters which are to be taken into account when determining the significance of an incident as referred to in paragraph 3 of this Article.***		***11a. The Commission is empowered to adopt delegated acts, in accordance with Article 36, to supplement this Directive by specifying the type of information to be submitted pursuant to paragraph 1 of this Article and by further specifying the parameters which are to be taken into account when determining the significance of an incident as referred to in paragraph 3 of this Article.*** R

					D/IA political issue
Article 21					
G	356	Article 21 Use of European cybersecurity certification schemes	Article 21 Use of European cybersecurity certification schemes	Article 21 Use of European cybersecurity certification schemes	Article 21 Use of European cybersecurity certification schemes Text Origin: Commission Proposal + Annexes
Article 21(1)					
G	357	1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.	1. ~~*In order to demonstrate compliance with certain requirements of Article 18, Member States may require*~~***Member States shall, following guidance from ENISA, the Commission and the Cooperation Group, encourage*** essential and important entities to certify certain ICT products, ICT services and ICT processes***, either developed by the essential or important entity or procured from third parties, under*** ~~*under specific*~~ European cybersecurity ~~*certification*~~ schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881~~*. The products, services and processes*~~	1. In order to demonstrate compliance with certain requirements of Article 18~~,~~ Member States may require ~~*essential and important*~~ entities to ~~*certify certain*~~***use particular*** ICT products,~~*, ICT*~~ services and ~~*ICT processes*~~***processes certified*** under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The ***ICT*** products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.	1. ~~*In order to demonstrate compliance with certain requirements of Article 18, Member States may require*~~***Member States may require, entities to use particular ICT products, services and processes, either developed by the*** essential ~~*and*~~***or*** important ~~*entities to certify certain ICT products, ICT services and ICT processes*~~***entity or procured from third parties, that are certified*** under ~~*specific*~~ European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. ~~*The products, services and processes subject to certification may be*~~

		~~subject to~~ ***or, if not yet available, under similar internationally recognised*** certification ~~may be developed by an~~***schemes. Furthermore, Member States shall encourage*** essential ~~or~~***and*** important ~~entity or procured from third parties~~***entities to use qualified trust services pursuant to Regulation (EU) No 910/2014***.		~~developed by an essential or important entity or procured from third parties~~***Furthermore, Member States shall encourage essential and important entities to use qualified trust services pursuant to Regulation (EU) No 910/2014***. PCY recital proposal: For the purposes of demonstrating compliance with cybersecurity risk management measures and in the absence of appropriate European cybersecurity certification schemes adopted in accordance with Regulation (EU) 2019/881, Member States should promote, in consultation with the Cooperation Group and the European Cybersecurity Certification Group, the use of appropriate European or international standards by the essential and important entities (or may require entities to use certified ICT products, services and processes or obtain a certificate under available national cybersecurity schemes). Furthermore, Member States should encourage entities to use qualified trust services pursuant to Regulation (EU) No 910/2014. Text in parentheses to be discussed again.

Article 21(2)					
R	358	2. The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.	2. The Commission ~~shall be~~***is*** empowered to adopt delegated acts***, in accordance with Article 36, to supplement this Directive by*** specifying which categories of essential ***and important*** entities ~~shall be~~***are*** required to obtain a certificate ~~and~~ under ~~which~~ specific European cybersecurity ~~certification~~ schemes pursuant to ~~paragraph 1. The~~***Article 49 of Regulation (EU) 2019/881. Such*** delegated acts shall be ~~adopted in accordance with Article 36~~***considered where insufficient levels of cybersecurity have been identified, shall be preceded by an impact assessment and shall provide for an implementation period***.	2. The Commission ~~shall be empowered to~~ ***may*** adopt ~~delegated~~***implementing*** acts specifying which categories of essential ***or important*** entities shall be required to ***use certain certified ICT products, services and processes or*** obtain a certificate ~~and~~ under which ~~specific~~ European cybersecurity certification schemes ***adopted*** pursuant to ~~paragraph 1~~***Article 49 of Regulation (EU) 2019/881***.***Those implementing*** ~~The delegated~~ acts shall be adopted in accordance with ***the examination procedure referred to in*** Article ~~36~~***37(2)***. ***When preparing such implementing acts, the Commission shall, in accordance with Article 56 of Regulation (EU) 2019/881:***	2. The Commission ~~shall be~~ ***is*** empowered to adopt delegated acts***, in accordance with Article 36*** specifying which categories of essential ***or important*** entities shall be required to ***use certain certified ICT products, services and processes or*** obtain a certificate ~~and~~ under which ~~specific~~ European cybersecurity certification schemes ***adopted*** pursuant to ~~paragraph 1. The~~ ***Article 49 of Regulation (EU) 2019/881. Those delegated acts shall be adopted where insufficient levels of cybersecurity have been identified and shall provide for an implementation period. The adoption of such*** delegated acts shall be ~~adopted~~***preceded by an impact assessment and stakeholder consultation*** in accordance with article ~~36~~***56 of Regulation EU 2019/881***. D/IA political issue. COM to draft recital on transition.	R
Article 21(i)					
G	358a				G

				(i) take into account the impact of the measures on the manufacturers or providers of such ICT products, services or processes and on the users in terms of the cost of those measures and the societal or economic benefits stemming from the anticipated enhanced level of security for the targeted ICT products, services or processes as well as their alternative availability on the market;	Delete.
Article 21(ii)					
G	358b			***(ii) carry out an open, transparent and inclusive consultation process with all relevant stakeholders and Member States;***	Delete. G
Article 21(iii)					
G	358c			***(iii) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measures on the manufacturers, or providers of ICT products, services or processes, or users thereof, particularly SMEs;***	Delete. G

Article 21(iv)					
G	358d			***(iv) take into account the existence and implementation of relevant Member State laws.***	Delete.
Article 21(3)					
G	359	3. The Commission may request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available.	3. The Commission may***, after consulting the Cooperation Group and the European Cybersecurity Certification Group,*** request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available.	3. The Commission may request ENISA to prepare a candidate scheme ***or to review an existing European cybersecurity certification scheme*** pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 ***of this Article*** is available.	3. The Commission may***, after consulting the Cooperation Group and the European Cybersecurity Certification Group,*** request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 is available. Text Origin: Council Mandate
Article 22					
G	360	Article 22 Standardisation	Article 22 Standardisation	Article 22 Standardisation	Article 22 Standardisation Text Origin: Commission Proposal + Annexes
Article 22(1)					

G	361	1. In order to promote the convergent implementation of Article 18(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.	1. In order to promote the convergent implementation of Article 18(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.	1. In order to promote the convergent implementation of Article 18(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.	1. In order to promote the convergent implementation of Article 18(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems. Text Origin: Commission Proposal + Annexes	G
Article 22(2)					
G	362	2. ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.	2. ENISA, in collaboration with Member States, ***and, where appropriate, after consulting relevant stakeholders,*** shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.	2. ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.	2. ENISA, in collaboration with Member States, ***and, where appropriate, after consulting relevant stakeholders,*** shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered. Text Origin: EP Mandate	G
Article 22(2a)					

G	362a		***2a. The Commission, in collaboration with ENISA, shall support and promote the development and implementation of standards set by relevant Union and international standardisation bodies for the convergent implementation of Article 18 (1) and (2). The Commission shall support the update of the standards in the light of technological developments.***			G
	Article 23					
G	363	Article 23 Databases of domain names and registration data	Article 23 ~~*Databases*~~***Database structure*** of domain names and registration data	Article 23 Databases of domain names and registration data	Article 23 ~~*Databases*~~***Database*** of domain names and registration data	G
	Article 23(1)					
Y	364	1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data	1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ~~*ensure that*~~***require*** TLD registries and the entities providing domain name registration services ~~*for the TLD shall*~~***to*** collect and maintain accurate***, verified*** and complete domain name registration data in a ~~*dedicated*~~ database ~~*facility with*~~	1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD ***name*** registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate***,*** and complete domain name registration data in a dedicated database facility with due diligence ~~*subject to Union*~~***in***	1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ~~*ensure*~~***require*** that TLD ***name*** registries and the entities providing domain name registration services ~~*for the TLD shall*~~ collect and maintain accurate and complete domain name registration data in a dedicated database ~~*facility*~~ with due diligence	Y

		protection law as regards data which are personal data.	~~due diligence subject to Union data protection law as regards data which are personal data~~***structure operated for that purpose***.	***accordance withUnion*** data protection law as regards data which are personal data.	~~subject to~~***in accordance with*** Union data protection law as regards data which are personal data. EP to check verification. Other wording of paragraph is fine for EP
	Article 23(2)				
G	365	2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.	2. Member States shall ensure that the ~~databases~~***database structure*** of domain name registration data referred to in paragraph 1 ~~contain~~***contains*** relevant information***, which shall include at least the registrants' name, their physical and email address as well as their telephone number,*** to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.	2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs~~.~~***, including at least the following data:***	2. ***For the purpose referred to in paragraph 1,*** Member States shall ~~ensure~~***require*** that the ~~databases~~***database*** of domain name registration data referred to in paragraph 1 contain ~~relevant~~***necessary*** information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. ***Such information shall include:***
	Article 23(a)				
G	365a			***a. domain name***	***2a. the domain name,***
	Article 23(b)				
G	365b			***b. date of registration***	***2b. the date of registration,***

	Article 23(2c)					
G	365c			***c. registrant data, including:***	***2c. the registrants' [full] name,***	G
	Article 23(2ci)					
G	365d			***(i) for individuals - name, surname and e-mail address;***	***2d. the registrant's contact email address,***	G
	Article 23(2cii)					
G	365e			***(ii) for legal persons - name and e-mail address.***	***2e. the registrant's contact telephone number.***	G
	Article 23(2f)					
G	365f				***2f. the contact email address and telephone number of the point of contact administering the domain name in case it is different from the registrant's.***	G
	Article 23(3)					
Y	366	3. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases include accurate and complete	3. Member States shall ensure that the TLD registries and ~~the~~ entities providing domain name registration services ~~for the TLD~~ have policies and procedures in place to ensure that the ~~databases include~~***database structure includes***	3. Member States shall ensure that the TLD ***name*** registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases include accurate and complete	3. Member States shall ~~ensure~~***require*** that the TLD ***name*** registries and the entities providing domain name registration services ~~for the TLD~~ have policies and procedures in place to ensure that the databases include accurate and	Y

		information. Member States shall ensure that such policies and procedures are made publicly available.	accurate***, verified*** and complete information. Member States shall ensure that such policies and procedures are made publicly available.	information. Member States shall ensure that such policies and procedures are made publicly available.	complete information***, including verification procedures where there is a suspicion of domain name abuse***. Member States shall ~~ensure~~***require*** that such policies and procedures are made publicly available. EP to check Text Origin: EP Mandate
	Article 23(4)				
G	367	4. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.	4. Member States shall ensure that the TLD registries and ~~the~~ entities providing domain name registration services ~~for the TLD publish~~***make publicly available***, without undue delay after the registration of a domain name, domain registration data which are not personal data. ***For legal persons as registrants, the domain registration data publicly available shall include at least the registrants' name, their physical and email address as well as their telephone number.***	4. Member States shall ensure that the TLD ***name*** registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.	4. Member States shall ~~ensure~~***require*** that the TLD ***name*** registries and the entities providing domain name registration services ~~for the TLD publish~~***make publicly available***, without undue delay after the registration of a domain name, domain ***name*** registration data which are not personal data. clarification to be checked in recital by the EP/COM
	Article 23(5)				
G	368	5. Member States shall ensure that	5. Member States shall ~~ensure that~~	5. Member States shall ensure that	5. Member States shall

		the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.	~~the~~***require*** TLD registries and ~~the~~ entities providing domain name registration services ~~for the TLD~~***to*** provide access to specific domain name registration data***, including personal data, upon*** ~~upon lawful and~~ duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ~~ensure that the~~***require*** TLD registries and ~~the~~ entities providing domain name registration services ~~for the TLD~~***to*** reply without undue delay ~~to all~~***and in any event within 72 hours upon the receipt of the*** requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.	the TLD ***name*** registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD ***name*** registries and the entities providing domain name registration services for the TLD reply without undue delay ***and in any case within 72 hours*** to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.	~~ensure~~***require*** that the TLD ***name*** registries and the entities providing domain name registration services ~~for the TLD~~ provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ~~ensure~~***require*** that the TLD ***name*** registries and the entities providing domain name registration services ~~for the TLD~~ reply without undue delay ***and in any event within 72 hours*** to all requests for access. Member States shall ~~ensure~~***require*** that policies and procedures to disclose such data are made publicly available. Text Origin: EP Mandate
Section II					
G	369	Section II Jurisdiction and Registration	Section II Jurisdiction and Registration	Section II Jurisdiction and Registration	Section II Jurisdiction and Registration Text Origin: Commission Proposal + Annexes
Article 24					
G	370	Article 24 Jurisdiction and territoriality	Article 24 Jurisdiction and territoriality	Article 24 Jurisdiction and territoriality	Article 24 Jurisdiction and territoriality

					Council new text Art. 24 (1) Text Origin: Commission Proposal + Annexes
Article 24(1a)					
G	370a			***1a. Entities under this Directive shall be deemed to be under the jurisdiction of the Member State where they provide their services. Entities referred to in points 1 to 7 and 10 of Annex I, trust service providers and Internet Exchange Point providers referred to in point 8 of Annex I, and points 1 to 5 of Annex II shall be deemed under the jurisdiction of the Member State on the territory of which they are established.***	deleted, inserted later
Article 24(1)					
G	371	1. DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and content delivery network providers referred to in point 8 of Annex I, as well as digital providers referred to in point 6 of Annex II shall be deemed to be under the jurisdiction	1. DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and content delivery network providers referred to in point 8 of Annex I, as well as digital providers referred to in point 6 of Annex II shall be deemed to be under the jurisdiction	1. DNS service providers, TLD name registries ***and entities providing domain name registration services for the TLD***, cloud computing service providers, data centre service providers ~~*and*~~, content delivery network providers***, managed service providers, and managed security***	1. ~~*DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and content delivery network providers referred to in point 8 of Annex I, as well as digital providers referred to in point 6 of Annex II*~~***Entities under this Directive*** shall be

		of the Member State in which they have their main establishment in the Union.	of the Member State in which they have their main establishment in the Union.	***service providers*** referred to in point 8 ***and point 8a*** of Annex I, as well as digital providers referred to in point 6 of Annex II shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union.	deemed to be under the jurisdiction of the Member State in which they ~~*have their main establishment in the Union.*~~***are established, except:***
	Article 24(1), point (a)				
G	371a				***(a) providers of public electronic communications networks or providers of electronic communications services referred to in point 8 of Annex I which shall be deemed to be under the jurisdiction of the Member State in which they provide their services;***
	Article 24(1), point (b)				
G	371b				***(b) DNS service providers, TLD name registries, and entities providing domain name registration services for the TLD, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, and managed security service providers referred***

					to in point 8 and point 8a of Annex I, as well as digital providers referred to in point 6 of Annex II which shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union;
Article 24(1), point (c)					
G	371c				***(c) public administration entities referred to in point 9 of Annex I which shall be deemed under the jurisdiction of the Member State which established them.***
Article 24(2)					
G	372	2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment with the highest	2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State ***either*** where the entities have the establishment with the highest	2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are ***predominantly*** taken. If ***the place where such decisions are predominantly taken cannot be determined or*** such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to	2. For the purposes of this Directive, entities referred to in paragraph ~~1~~***1b*** shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are ***predominantly*** taken. If ***the place where such decisions are predominantly taken cannot be determined or*** such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to

		number of employees in the Union.	number of employees in the Union ***or the establishment where cybersecurity operations are carried out***.	be in the Member State where the entities have the establishment with the highest number of employees in the Union. ***Where the services are provided by a group of undertakings, the main establishment shall be deemed to be the main establishment of the group of undertakings.***	be in the Member State where ***cybersecurity operations are carried out. If the place where cybersecurity operations are carried out cannot be determined the main establishment shall be deemed to be in the Member State where*** the entities have the establishment with the highest number of employees in the Union. recital to be added clarifying predominantly	
	Article 24(3)					
G	373	3. If an entity referred to in paragraph 1 is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this Article, any Member State in which the entity provides services may take legal actions against the entity for non-	3. If an entity referred to in paragraph 1 is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this Article, any Member State in which the entity provides services may take legal actions against the entity for non-	3. If an entity referred to in paragraph 1 is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this Article, any Member State in which the entity provides services may take legal actions against the entity for non-	3. If an entity referred to in paragraph 1 is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this Article, any Member State in which the entity provides services may take legal actions against the entity for non-	G

		compliance with the obligations under this Directive.	compliance with the obligations under this Directive.	compliance with the obligations under this Directive.	compliance with the obligations under this Directive. Text Origin: Commission Proposal + Annexes
Article 24(4)					
G	374	4. The designation of a representative by an entity referred to in paragraph 1 shall be without prejudice to legal actions, which could be initiated against the entity itself.	4. The designation of a representative by an entity referred to in paragraph 1 shall be without prejudice to legal actions, which could be initiated against the entity itself.	4. The designation of a representative by an entity referred to in paragraph 1 shall be without prejudice to legal actions, which could be initiated against the entity itself.	4. The designation of a representative by an entity referred to in paragraph 1 shall be without prejudice to legal actions, which could be initiated against the entity itself. Text Origin: Commission Proposal + Annexes
Article 24(4a)					
G	374a			***4a. Member States that have received a request for mutual assistance in relation to the entities referred to in paragraph 1, may, within the limits of the request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has the network and information system on their territory.***	***4a. Member States that have received a request for mutual assistance in relation to the entities referred to in paragraph 1b, may, within the limits of the request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has the network and information system on their territory.*** Text Origin: Council Mandate

	Article 25				
G	375	Article 25 Registry for essential and important entities	Article 25 ~~*Registry for essential and important entities*~~***ENISA registry***	Article 25 Registry for essential and important entities	Article 25 Registry ~~*for*~~***of*** essential and important entities name to be checked
	Article 25(1), introductory part				
Y	376	1. ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1). The entities shall submit the following information to ENISA by [12 months after entering into force of the Directive at the latest]:	1. ENISA shall create and maintain a ***secure*** registry ~~*for*~~***of*** essential and important entities referred to in Article 24(1)~~*. The entities*~~***, which*** shall ~~*submit*~~***include*** the following information ~~*to ENISA by [12 months after entering into force of the Directive at the latest]*~~:	1. ~~*ENISA*~~***Member States*** shall ~~*create and maintain a registry for essential and important entities referred to in Article 24(1). The entities shall*~~***ensure that the entities referred to in Article 24(1) having their main establishment on their territory, or, if not established in the Union, having their designated representative in the Union established on their territory are required to*** submit the following information to ~~*ENISA by*~~***the competent authoritiesby*** [12 months after entering into force of the Directive at the latest]:	1. ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1)***, based on the information received from the Member States' single points of contacts according to paragraph 1a, except (d), and 2. Upon request, ENISA shall enable access of competent authorities to the registry, while ensuring the necessary guarantees to protect the confidentiality of*** ~~*. The entities shall submit the following*~~ information ***where applicable.*** ***1a. Member States shall require entities referred to in Article 24(1) to submit the following information to the competent authorities [3 months after the transposition deadline***~~*to ENISA by*~~

					~~[12 months after entering into force of the Directive at the latest~~]:
Article 25(1), point (a)					
Y	377	(a) the name of the entity;	(a) the name of the entity;	(a) the name of the entity;	(a) the name of the entity; Text Origin: Council Mandate
Article 25(1), point (aa)					
Y	377a			***(aa) the type of entity as per Annexes I and II to this Directive;***	***(aa) relevant sector, subsector and type of entity as referred to in Annex I and II***
Article 25(1), point (b)					
Y	378	(b) the address of its main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 24(3);	(b) the address of its main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 24(3);	(b) the address of its main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 24(3);	(b) the address of its main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 24(3); Text Origin: Council Mandate
Article 25(1), point (c)					
Y	379	(c) up-to-date contact details, including email addresses and telephone numbers of the entities.	(c) up-to-date contact details, including email addresses***, IP ranges,*** ~~and~~ telephone numbers ***and relevant sectors and***	(c) up-to-date contact details, including email addresses and telephone numbers of the entities***and of their representatives;***	(c) up-to-date contact details, including email addresses and telephone numbers of the ~~entities~~***entity and where***

			subsectors of the entities ***referred to in Annexes I and II***.		***applicable, its representative designated pursuant to Article 24(3)***.
Article 25(1), point (d)					
Y	379a			***(d) Member States where the entity provides the service.*** ***Where applicable, this information shall be submitted through the national mechanism of self-notification referred to in Article 2a.***	***(ca) Member States where the entity provides services.***
Article 25(1), point (d), point (1)					
	379b				***(d) IP ranges***
Article 25(1a)					
Y	379c		***1a. By ... [12 months after the date of entry into force of this Directive], the essential and important entities shall submit the information referred to in the first subparagraph to ENISA.***		***1a. Where applicable, this information shall be submitted through the national mechanism of self-notification referred to in Article 2a(2). The single point of contact in the Member State concerned shall forward the information to ENISA without undue delay after its receipt.***
Article 25(2)					

Y	380	2. The entities referred to in paragraph 1 shall notify ENISA about any changes to the details they submitted under paragraph 1 without delay, and in any event, within three months from the date on which the change took effect.	2. The entities referred to in paragraph 1 shall notify ENISA about any changes to the details they submitted under paragraph 1 without delay, and in any event, within three months from the date on which the change took effect.	2. ***Member States shall ensure that*** the entities referred to in paragraph 1 ~~*shall*~~***also*** notify ~~*ENISA about*~~ any changes to the details they submitted under paragraph 1 without delay, and in any event, within three months from the date on which the change took effect.	2. ***Member States shall ensure that*** the entities referred to in paragraph 1 ~~*shall*~~ notify ~~*ENISA*~~ ***the competent authority*** about any changes to the details they submitted under paragraph ~~*1*~~***1a*** without delay, and in any event, within three months from the date on which the change took effect. ***Without undue delay after its receipt, this information except the information referred to in paragraph 1a(d) shall be forwarded by the single point of contact of the Member State concerned to ENISA.***	Y
	Article 25(3)					
Y	381	3. Upon receipt of the information under paragraph 1, ENISA shall forward it to the single points of contact depending on the indicated location of each entity's main establishment or, if it is not established in the Union, of its designated representative. Where an entity referred to in paragraph 1 has besides its main establishment in the Union further establishments in other Member States, ENISA shall also inform the single points of contact of those Member States.	3. Upon receipt of the information under paragraph 1, ENISA shall forward it to the single points of contact depending on the indicated location of each entity's main establishment or, if it is not established in the Union, of its designated representative. Where an entity referred to in paragraph 1 has besides its main establishment in the Union further establishments in other Member States, ENISA shall also inform the single points of contact of those Member States.	3. ~~*Upon receipt of the information under paragraph 1, ENISA shall forward it to the*~~***The Member States'*** single points of contact ~~*depending on the indicated location of each entity's main establishment or, if it is not established in the Union, of its designated representative. Where an entity*~~***shall forward the information*** referred to in ~~*paragraph 1 has besides its main establishment in the Union further establishments in other Member*~~	Deleted	Y

				~~States,~~ ***paragraphs 1 and 2 to*** ENISA ~~*shall also inform the single points of contact of those Member States.*~~ ***.***	
Article 25(3a)					
Y	381a			***3a. Based on the information received according to paragraph 3 of this Article, ENISA shall create and maintain a registry for the entities referred to in paragraph 1. Upon request of Member States, ENISA shall enable access of relevant competent authorities to the registry, while ensuring the necessary guarantees to protect confidentiality of information where applicable.***	Deleted
Article 25(4)					
Y	382	4. Where an entity fails to register its activity or to provide the relevant information within the deadline set out in paragraph 1, any Member State where the entity provides services shall be competent to ensure that entity's compliance with the obligations laid down in this Directive.	4. Where an entity fails to register its activity or to provide the relevant information within the deadline set out in paragraph 1, any Member State where the entity provides services shall be competent to ensure that entity's compliance with the obligations laid down in this Directive.	4. ~~*Where an entity fails to register its activity or to provide the relevant information within the deadline set out in paragraph 1, any Member State where the entity provides services shall be competent to ensure that entity's compliance with the obligations laid down in this Directive.*~~	Deleted
CHAPTER V					

G	383	CHAPTER V Information sharing	CHAPTER V Information sharing	CHAPTER V Information sharing	CHAPTER V Information sharing Text Origin: Commission Proposal + Annexes	G
	Article 26					
G	384	Article 26 Cybersecurity information-sharing arrangements	Article 26 Cybersecurity information-sharing arrangements	Article 26 Cybersecurity information-sharing arrangements	Article 26 Cybersecurity information-sharing arrangements Text Origin: Commission Proposal + Annexes	G
	Article 26(1), introductory part					
G	385	1. Without prejudice to Regulation (EU) 2016/679, Member States shall ensure that essential and important entities may exchange relevant cybersecurity information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools, where such information sharing:	1. ~~*Without prejudice to Regulation (EU) 2016/679,*~~ Member States shall ensure that essential and important entities ***and other relevant entities not covered by the scope of this Directive*** may exchange relevant cybersecurity information among themselves including information relating to cyber threats***, near misses***, vulnerabilities, ***techniques and procedures, metadata and content data,*** indicators of compromise, ***adversarial*** tactics, ~~*techniques and procedures*~~***modus operandi, actor specific information***, cybersecurity	1. ~~*Without prejudice to Regulation (EU) 2016/679,*~~ Member States shall ensure that essential and important entities may exchange ***on a voluntary basis*** relevant cybersecurity information among themselves including information relating to cyber threats***, near misses***, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools, where such information sharing:	1. ~~*Without prejudice to Regulation (EU) 2016/679,*~~ Member States shall ensure that essential and important entities ***and, where relevant, other relevant entities not covered by the scope of this Directive*** may exchange ***on a voluntary basis*** relevant cybersecurity information among themselves including information relating to cyber threats***, near misses***, vulnerabilities, ***techniques and procedures,*** indicators of compromise, ***adversarial*** tactics, ~~*techniques and procedures*~~***threat actor specific information***,	G

			alerts***, industrial espionage tactics and recommended security tool configurations*** ~~*and configuration tools*~~, where such information sharing:		cybersecurity alerts and ***recommendations regarding*** configuration ***of cybersecurity*** tools ***to detect cyber attacks***, where such information sharing: Text Origin: EP Mandate
Article 26(1), point (a)					
G	386	(a) aims at preventing, detecting, responding to or mitigating incidents;	(a) aims at preventing, detecting, responding to or mitigating incidents;	(a) aims at preventing, detecting, responding to or mitigating incidents;	G
Article 26(1), point (b)					
G	387	(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection techniques, mitigation strategies, or response and recovery stages.	(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection***, containment and prevention*** techniques, mitigation strategies, or response and recovery stages ***or promoting collaborative cyber threat research between public and private entities***.	(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection techniques, mitigation strategies, or response and recovery stages.	(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection***, containment and prevention*** techniques, mitigation strategies, or response and recovery stages ***or promoting collaborative cyber threat research between public and private entities***. Text Origin: EP Mandate	G

Article 26(2)				
388	2. Member States shall ensure that the exchange of information takes place within trusted communities of essential and important entities. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared and in compliance with the rules of Union law referred to in paragraph 1.	2. Member States shall ~~ensure that~~***facilitate*** the exchange of information ~~takes place within~~***by enabling the establishment of*** trusted communities of essential and important entities ***and their service providers or, where relevant, other suppliers***. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared ~~and in compliance with the rules of Union law referred to in paragraph 1~~.	2. Member States shall ensure that the exchange of information takes place within ~~trusted~~ communities of essential and important entities. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared ~~and in compliance with the rules of Union law referred to in paragraph 1~~.	2. Member States shall ensure that the exchange of information takes place within ~~trusted~~ communities of essential and important entities***, and where relevant, their service providers or other suppliers***. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared ~~and in compliance with the rules of Union law referred to in paragraph 1~~.
Article 26(3)				
389	3. Member States shall set out rules specifying the procedure, operational elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. Such rules shall also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the	3. Member States shall ~~set out rules specifying the procedure,~~***facilitate the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by making*** operational elements (including the use of dedicated ICT platforms~~), content and conditions of the information sharing arrangements referred to in paragraph 2. Such~~	3. Member States ~~shall~~***may*** set out rules specifying the procedure, operational elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. Such rules ~~shall~~***may*** also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the	3. Member States shall ~~set out rules specifying the procedure,~~ ***facilitate the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2. Such arrangements may specify*** operational elements (including the use of dedicated ICT platforms ***and automation tools), content and conditions of the information sharing arrangements. In laying*** ~~),~~

		use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).	~~rules~~ ***and automation tools) and content available. Member States*** shall ~~also~~ lay down the details of the involvement of public authorities in such arrangements~~, as well as operational elements, including the use of dedicated IT platforms~~ ***and may impose certain conditions on the information made available by competent authorities or CSIRTs***. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).	use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).	~~content and conditions of the information sharing arrangements referred to in paragraph 2. Such rules shall also lay~~ down the details of the involvement of public authorities in such arrangements~~, as well as operational elements, including the use of dedicated IT platforms~~ ***Member States may impose certain conditions on the information made available by competent authorities or CSIRTs***. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).
Article 26(4)					
G	390	4. Essential and important entities shall notify the competent authorities of their participation in the information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.	4. Essential and important entities shall notify the competent authorities of their participation in the information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.	4. Essential and important entities shall notify the competent authorities of their participation in the information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.	4. Essential and important entities shall notify the competent authorities of their participation in the information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect. Text Origin: Commission Proposal + Annexes

Article 26(5)				
391	5. In compliance with Union law, ENISA shall support the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by providing best practices and guidance.	5. In compliance with Union law, ENISA shall support the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by providing best practices and guidance.	5. ~~*In compliance with Union law,*~~ ENISA shall support the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by providing best practices and guidance.	5. ~~*In compliance with Union law,*~~ ENISA shall support the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by providing best practices and guidance. Text Origin: Council Mandate
Article 27				
392	Article 27 Voluntary notification of relevant information	Article 27 Voluntary notification of relevant information	Article 27 Voluntary notification of relevant information	Article 27 Voluntary notification of relevant information Text Origin: Commission Proposal + Annexes
Article 27, (1)				
393	Member States shall ensure that, without prejudice to Article 3, entities falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses. When processing notifications, Member States shall act in accordance with	Member States shall ensure that~~, *without prejudice to Article 3, entities falling outside the scope of this Directive may submit notifications*~~ ***notifications may be submitted to the CIRTS***, on a voluntary basis, ~~*of significant incidents, cyber threats or near misses. When processing*~~	***1.*** ~~*Member States shall ensure that,*~~ Without prejudice to Article ~~*3, entities falling outside the scope of this Directive may submit notifications*~~***20, Member States shall ensure that essential and important entities may notify***, on a voluntary basis, ~~*of significant incidents, cyber threats or near*~~	Member States shall ensure that~~, *without prejudice to Article 3, entities falling outside the scope of this Directive may submit notifications*~~ ***notifications may be submitted to the CSIRTs, or where relevant competent authorities***, on a voluntary basis, ~~*of significant incidents, cyber*~~

		the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.	~~notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.~~ ***by:***	~~misses. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification~~***to the competent authorities or the CSIRTs any relevant incidents, cyber threats or near misses***.	~~threats or near misses. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.~~ ***by:*** Text Origin: EP Mandate
Article 27, first paragraph, point (a)					
G	393a		***(a) essential and important entities with regard to cyber threats and near misses;***		***(a) essential and important entities with regard to cyber threats, near misses and relevant incidents which do not meet the criteria pursuant to Article 20(3);*** lawyer linguists to finetune Text Origin: EP Mandate
Article 27, first paragraph, point (b)					
G	393b		***(b) entities falling outside the scope of this Directive, with***		***(b) entities falling outside the scope of this Directive, with***

			regard to significant incidents, cyber threats or near misses.		***regard to significant incidents, cyber threats or near misses.*** Text Origin: EP Mandate
Article 27, (2)					
G	393c			***2. Member States shall ensure that, without prejudice to Article 3, entities falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Without prejudice to the investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.***	***2. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Without prejudice to the investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.*** ***Where necessary, [CSIRTs shall provide the single point of contact and, where relevant, the competent authorities], with the information on notifications received pursuant this Article, while ensuring confidentiality and appropriate protections of the information provided by the reporting entity. Voluntary***

					notification shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.
	Article 27, (3)				
G	393d			***3. Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on the Member State concerned.***	deleted
	Article 27 (1), subparagraph 1a				
G	393e		***When processing such notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Where necessary, CSIRTs shall provide the single point of contact and, where relevant, the competent authorities, with the information on notifications received pursuant this Article, while ensuring confidentiality and appropriate protections of the information***		deleted, inserted in c

			provided by the reporting entity. Voluntary notification shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.		
CHAPTER VI					
G	394	CHAPTER VI Supervision and enforcement	CHAPTER VI Supervision and enforcement	CHAPTER VI Supervision and enforcement	CHAPTER VI Supervision and enforcement Text Origin: Commission Proposal + Annexes
Article 28					
G	395	Article 28 General aspects concerning supervision and enforcement	Article 28 General aspects concerning supervision and enforcement	Article 28 General aspects concerning supervision and enforcement	Article 28 General aspects concerning supervision and enforcement Text Origin: Commission Proposal + Annexes
Article 28(1)					
G	396	1. Member States shall ensure that competent authorities effectively monitor and take the measures necessary to ensure compliance with this Directive, in particular the obligations laid down in	1. Member States shall ensure that competent authorities effectively monitor and take the measures necessary to ensure compliance with this Directive, in particular the obligations laid down in	1. Member States shall ensure that competent authorities effectively monitor and take the measures necessary to ensure compliance with this Directive, in particular the obligations laid down in	1. Member States shall ensure that competent authorities effectively monitor and take the measures necessary to ensure compliance with ***the obligations under*** this Directive.

		Articles 18 and 20.	Articles 18 and 20.	Articles 18, ***20 and 23. Member States may allow competent authorities to prioritise supervision, which shall be based on a risk-based approach*** ~~*and 20*~~.	***1a. Member States may allow competent authorities to prioritise supervision, which shall be based on a risk-based approach. For this purpose, where exercising their supervisory tasks provided for in Article 29 and Article 30, competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.*** ~~*- in particular the obligations laid down in Articles 18 and 20.*~~ Text Origin: Council Mandate
Article 28(2)					
G	397	2. Competent authorities shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.	2. Competent authorities shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches. ***This shall be done in accordance with their competence and tasks pursuant to Regulation (EU) 2016/679.***	2. Competent authorities shall work in close cooperation with data protection authorities, ***competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], supervisory bodies designated pursuant to Regulation (EU) 910/2014 and other competent authorities designated under sector-specific Union legal acts when addressing cybersecurity incidents*** ~~*when addressing*~~	2. Competent authorities shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches. ***This shall be done in accordance with their competence and tasks pursuant to Regulation (EU) 2016/679.*** COM objects to EP AM. Text Origin: EP Mandate

				~~*incidents resulting in personal data breaches*~~.	
Article 28(3)					
G	397a			***3. Without prejudice to national legislative and institutional frameworks, Member States shall ensure that, in the supervision of compliance of public administration entities with this Directive and the enforcement of potential sanctions for non-compliance, the competent authorities have the appropriate powers to conduct such tasks with operational independence vis-à-vis the entities supervised. Member States may decide on the imposition of appropriate, proportionate and effective measures of supervision and enforcement in relation to these entities in accordance with the national frameworks and legal order.***	***3. Without prejudice to national legislative and institutional frameworks, Member States shall ensure that, in the supervision of compliance of public administration entities with this Directive and the enforcement of potential sanctions for non-compliance, the competent authorities have the appropriate powers to conduct such tasks with operational independence vis-à-vis the entities supervised. Member States may decide on the imposition of appropriate, proportionate and effective measures of supervision and enforcement in relation to these entities in accordance with the national frameworks and legal order.*** Text Origin: Council Mandate	G
Article 29					
G	398	Article 29 Supervision and enforcement for	Article 29 Supervision and enforcement for	Article 29 Supervision and enforcement for	Article 29 Supervision and enforcement for	G

		essential entities	essential entities	essential entities	essential entities Text Origin: Commission Proposal + Annexes
	Article 29(1)				
G	399	1. Member States shall ensure that the measures of supervision or enforcement imposed on essential entities in respect of the obligations set out in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.	1. Member States shall ensure that the measures of supervision or enforcement imposed on essential entities in respect of the obligations set out in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.	1. Member States shall ensure that the measures of supervision or enforcement imposed on essential entities in respect of the obligations set out in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.	1. Member States shall ensure that the measures of supervision or enforcement imposed on essential entities in respect of the obligations set out in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case. Text Origin: Commission Proposal + Annexes
	Article 29(2)				
G	400	2. Member States shall ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, have the power to subject those entities to:	2. Member States shall ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, have the power to subject those entities to:	2. Member States shall ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, ***follow a risk-based approach and*** have the power to subject those entities ***at least*** to:	2. Member States shall ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, have the power to subject those entities ***at least*** to: Text Origin: Council Mandate
	Article 29(2), point (a)				
G	401				

	(a) on-site inspections and off-site supervision, including random checks;	(a) on-site inspections and off-site supervision, including random checks ***conducted by trained professionals***;	(a) on-site inspections and off-site supervision, including random checks;	(a) on-site inspections and off-site supervision, including random checks ***conducted by trained professionals***; EP proposal for recital: When exercising their supervisory tasks in relation to essential and important entities, competent authorities should ensure that the person conducting inspections are trained professionals. Trained professionals should be independent and have the necessary skills to exercise the tasks designated by this Directive when conducting on-site and off-site inspections, including the identification of any weaknesses in databases, hardware, firewalls, encryption and networks. Trained professionals should ensuring that inspections are consistent and of the highest quality; Text Origin: Commission Proposal + Annexes
Article 29(2), point (aa)				
G 401a		***(aa) investigation of cases of non-compliance and the effects thereof on the security of the services;***		G
Article 29(2), point (b)				

	402	(b) regular audits;	(b) ~~regular~~***annual and targeted security*** audits ***carried out by a qualified independent body or a competent authority***;	(b) regular ***security*** audits;	(b) regular ***and targeted security*** audits ***carried out by an independent body or a competent authority***; Text Origin: EP Mandate
	Article 29(2), point (c)				
	403	(c) targeted security audits based on risk assessments or risk-related available information;	(c) ~~targeted security~~***ad hoc*** audits ~~based on risk assessments or risk-related available information~~***in cases justified on the ground of a significant incident or non-compliance by the essential entity***;	(c) targeted security audits based on risk assessments or risk-related available information;	(c) ~~targeted security~~***ad hoc*** audits***, including in cases justified on the ground of a significant incident or non-compliance by the essential entity*** ~~based on risk assessments or risk-related available information~~; Text Origin: EP Mandate
	Article 29(2), point (d)				
	404	(d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria;	(d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria;	(d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria***, where necessary for technical reasons, with the cooperation of the entity concerned***;	(d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria***, where necessary, with the cooperation of the entity concerned***;
	Article 29(2), point (e)				
	405	(e) requests of information necessary to assess the	(e) requests of information necessary to assess the	(e) requests of information necessary to assess the	(e) requests of information necessary to assess the

		cybersecurity measures adopted by the entity, including documented cybersecurity policies, as well as compliance with the obligation to notify the ENISA pursuant to Article 25 (1) and (2);	cybersecurity measures adopted by the entity, including documented cybersecurity policies, as well as compliance with the obligation to notify the ENISA pursuant to Article 25 (1) and (2);	cybersecurity measures adopted by the entity, including documented cybersecurity policies~~, as well as compliance with the obligation to notify the ENISA pursuant to Article 25 (1) and (2)~~;	cybersecurity measures adopted by the entity, including documented cybersecurity policies, as well as compliance with the obligation to notify the ~~ENISA~~**competent authorities** pursuant to Article 25 ~~(1) and (2)~~; Text Origin: Commission Proposal + Annexes
Article 29(2), point (f)					
G	406	(f) requests to access data, documents or any information necessary for the performance of their supervisory tasks;	(f) requests to access data, documents or any information necessary for the performance of their supervisory tasks;	(f) requests to access data, documents or any information necessary for the performance of their supervisory tasks;	(f) requests to access data, documents or any information necessary for the performance of their supervisory tasks; Text Origin: Commission Proposal + Annexes
Article 29(2), point (g)					
G	407	(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.	(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.	(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.	(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence. Text Origin: Commission Proposal + Annexes
Article 29(2a)					

G	407a			*(2a) Where exercising their supervisory tasks provided for in paragraph 2 of this Article, competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.*	Deleted Text Origin: Council Mandate	G
Article 29(2), subparagraph 1a & 1b						
G	407b		*The targeted security audits, referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.* *The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by a qualified independent body shall be paid by the entity concerned.*		*The targeted security audits, referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.* *The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the entity concerned, except in duly justified cases when the competent authority decides otherwise.*	G
Article 29(2a)						

G	407c		***2a. Where exercising their powers under paragraph 2, points (a) to (d), the competent authorities shall minimise the impact on the business processes of the entity.***		move to a recital
	Article 29(3)				
G	408	3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.	3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.	3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.	3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested. Text Origin: Commission Proposal + Annexes
	Article 29(4), introductory part				
G	409	4. Member States shall ensure that competent authorities, where exercising their enforcement powers in relation to essential entities, have the power to:	4. Member States shall ensure that competent authorities, where exercising their enforcement powers in relation to essential entities, have the power to:	4. Member States shall ensure that competent authorities, where exercising their enforcement powers in relation to essential entities, have the power ***at least*** to:	4. Member States shall ensure that competent authorities, where exercising their enforcement powers in relation to essential entities, have the power ***at least*** to: Text Origin: Council Mandate
	Article 29(4), point (a)				
G	410	(a) issue warnings on the entities' non-compliance with the	(a) issue warnings on the entities' non-compliance with the	(a) issue warnings on the entities' non-compliance with the	(a) issue warnings on the entities' non-compliance with the

		obligations laid down in this Directive;	obligations laid down in this Directive;	obligations laid down in this Directive;	obligations laid down in this Directive; Text Origin: Commission Proposal + Annexes
Article 29(4), point (b)					
G	411	(b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive;	(b) issue binding instructions, ***including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation,*** or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive;	(b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive;	(b) issue binding instructions, ***including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation,*** or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive; Text Origin: EP Mandate
Article 29(4), point (c)					
G	412	(c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;	(c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;	(c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;	(c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Directive and desist from repeating that conduct; Text Origin: Commission Proposal + Annexes
Article 29(4), point (d)					

G	413	(d) order those entities to bring their risk management measures and/or reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;	(d) order those entities to bring their risk management measures and/or reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;	(d) order those entities to bring their risk management measures and/or reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;	(d) order those entities to bring their risk management measures and/or reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period; Text Origin: Commission Proposal + Annexes
	Article 29(4), point (e)				
G	414	(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;	(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;	(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of ***the nature of the threat, as well as*** any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;	(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of ***the nature of the threat, as well as*** any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat; Text Origin: Council Mandate
	Article 29(4), point (f)				
G	415	(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;	(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;	(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;	(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;

					Text Origin: Commission Proposal + Annexes
Article 29(4), point (g)					
G	416	(g) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with their obligations provided for by Articles 18 and 20;	(g) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with their obligations provided for by Articles 18 and 20;	(g) ~~*designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with their obligations provided for by Articles 18 and 20;*~~	(g) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with their obligations provided for by Articles 18 and 20; Text Origin: Commission Proposal + Annexes
Article 29(4), point (h)					
G	417	(h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner;	(h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner;	(h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner***, when such public disclosure does not lead to a harmful exposure of the respective entity***;	(h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner; Text Origin: Commission Proposal + Annexes
Article 29(4), point (i)					
G	418	(i) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the	~~*(i) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the*~~	(i) ~~*make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the*~~	deleted

		nature of that infringement;	~~nature of that infringement;~~	~~nature of that infringement;~~		
Article 29(4), point (j)						
G	419	(j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (i) of this paragraph, depending on the circumstances of each individual case.	(j) impose or request the imposition by the relevant bodies or courts ~~according to~~***in accordance with*** national ~~laws~~***law*** of an administrative fine pursuant to Article 31 in addition to~~, or instead of,~~ the measures referred to in points (a) to (i) of this paragraph, depending on the circumstances of each individual case~~.~~	(j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (i) of this paragraph, depending on the circumstances of each individual case.	(j) impose or request the imposition by the relevant bodies or courts ~~according to~~***in accordance with*** national ~~laws~~***law*** of an administrative fine pursuant to Article 31 in addition to~~, or instead of,~~ ***any of*** the measures referred to in points (a) to (i) of this paragraph, depending on the circumstances of each individual case~~.~~	G
Article 29(5), introductory part						
G	420	5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity is requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the	5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity is requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the	5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity is requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the	5. Where enforcement actions adopted pursuant to points (a) to (d) and (f) of paragraph (4) prove ineffective, Member States shall ensure that competent authorities have the power to establish a deadline within which the essential entity is requested to take the necessary action to remedy the deficiencies or comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that the competent authorities have the	G

		power to:	power to:	power to:	power to: Text Origin: Commission Proposal + Annexes
Article 29(5), point (a)					
G	421	(a) suspend or request a certification or authorisation body to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;	(a) ***temporarily*** suspend or request a certification or authorisation body to ***temporarily*** suspend a certification or authorisation concerning part or all ~~the~~***relevant*** services or activities provided by an essential entity;	(a) suspend or request a certification or authorisation body ***or courts according to national laws*** to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;	(a) ***temporarily*** suspend or request a certification or authorisation body ***or courts according to national laws to temporarily*** ~~to~~ suspend a certification or authorisation concerning part or all ~~the~~***relevant*** services or activities provided by an essential entity;
Article 29(5), point (b)					
G	422	(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.	(b) ~~impose or~~***as ultima ratio,*** request the imposition by the relevant bodies or courts ~~according to~~***in accordance with*** national ~~laws~~***law*** of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, ~~and of any other natural person held responsible for the breach,~~ from exercising managerial functions in that entity.	(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.	(b) ~~impose or~~ request the imposition by the relevant bodies or courts ~~according to~~***in accordance with*** national ~~laws~~***law*** of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, ~~and of any other natural person held responsible for the breach,~~ from exercising managerial functions in that entity.
Article 29(6), first paragraph					

G	423	These sanctions shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.	~~These sanctions~~***Temporary suspensions or bans pursuant to this paragraph*** shall be applied only until the entity ***concerned*** takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. ***The imposition of such temporary suspensions or bans shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection, due process, presumption of innocence and right of defence.***	These sanctions shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. ***The sanctions provided in this paragraph are not applicable to public administration entities subject to this Directive.***	~~These sanctions~~***Temporary suspensions or bans pursuant to this paragraph*** shall be applied only until the entity ***concerned*** takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. ***The imposition of such temporary suspensions or bans shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection, due process, presumption of innocence and right of defence. The sanctions provided in this paragraph are not applicable to public administration entities subject to this Directive.***	G
	Article 29(6)					
G	424	6. Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its	6. Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its	6. Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its	6. Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its	G

		compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive.	compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive.	compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive. ***As regards public administration entities, this provision shall be without prejudice to the Member States' laws as regards the liability of public servants and elected and appointed officials.***	compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive. ***As regards public administration entities, this provision shall be without prejudice to the Member States' laws as regards the liability of public servants and elected and appointed officials.*** Text Origin: Council Mandate
Article 29(7), introductory part					
G	425	7. Where taking any of the enforcement actions or applying any sanctions pursuant to paragraphs 4 and 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:	7. Where taking any of the enforcement actions or applying any sanctions pursuant to paragraphs 4 and 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:	7. Where taking any of the enforcement actions or applying any sanctions pursuant to paragraphs 4 and 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:	7. Where taking any of the enforcement actions or applying any sanctions pursuant to paragraphs 4 and 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of: Text Origin: Commission Proposal + Annexes
Article 29(7), point (a)					
G	426				

		(a) the seriousness of the infringement and the importance of the provisions breached. Among the infringements that should be considered as serious: repeated violations, failure to notify or remedy incidents with a significant disruptive effect, failure to remedy deficiencies following binding instructions from competent authorities obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement, providing false or grossly inaccurate information in relation to risk management requirements or reporting obligations set out in Articles 18 and 20.	(a) the seriousness of the infringement and the importance of the provisions breached. Among the infringements that should be considered as serious: repeated violations, failure to notify or remedy incidents with a significant disruptive effect, failure to remedy deficiencies following binding instructions from competent authorities obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement, providing false or grossly inaccurate information in relation to risk management requirements or reporting obligations set out in Articles 18 and 20.	(a) the seriousness of the infringement and the importance of the provisions breached. Among the infringements that should be considered as serious: repeated violations, failure to notify or remedy incidents with a significant disruptive effect, failure to remedy deficiencies following binding instructions from competent authorities obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement, providing false or grossly inaccurate information in relation to risk management requirements or reporting obligations set out in Articles 18 and 20.	(a) the seriousness of the infringement and the importance of the provisions breached. Among the infringements that should be considered as serious: repeated violations, failure to notify or remedy incidents with a significant disruptive effect, failure to remedy deficiencies following binding instructions from competent authorities obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement, providing false or grossly inaccurate information in relation to risk management requirements or reporting obligations set out in Articles 18 and 20. `Text Origin: Commission Proposal + Annexes`	
	Article 29(7), point (b)					
G	427	(b) the duration of the infringement, including the element of repeated infringements;	(b) the duration of the infringement, including the element of repeated infringements;	(b) the duration of the infringement, including the element of repeated infringements;	(b) the duration of the infringement~~, including the element of repeated infringements~~**;** ***ba) any relevant previous infringements by the entity concerned***; EP text from row 428 a	G

	Article 29(7), point (c)				
G	428	(c) the actual damage caused or losses incurred or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;	(c) the ~~actual~~ damage caused or losses incurred ~~or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential~~, ***including*** financial or economic losses, effects on other services~~,~~ ***and the*** number of users affected ~~or potentially affected;~~**;**	(c) the actual damage caused or losses incurred or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;	(c) the ~~actual~~ damage caused or losses incurred ~~or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others, of actual or potential~~, ***including*** financial or economic losses, effects on other services~~,~~ ***and the*** number of users affected ~~or potentially affected;~~**;** Text Origin: EP Mandate	G
	Article 29(7), point (ca)				
G	428a		***(ca) any relevant previous infringements by the entity concerned;***		inserted in row 427 Text Origin: EP Mandate	G
	Article 29(7), point (d)				
G	429	(d) the intentional or negligent character of the infringement;	(d) the intentional or negligent character of the infringement;	(d) the intentional or negligent character of the infringement;	(d) the intentional or negligent character of the infringement; Text Origin: Commission Proposal + Annexes	G

Article 29(7), point (e)					
G	430	(e) measures taken by the entity to prevent or mitigate the damage and/or losses;	(e) measures taken by the entity to prevent or mitigate the damage and/or losses;	(e) measures taken by the entity to prevent or mitigate the damage and/or losses;	(e) measures taken by the entity to prevent or mitigate the damage and/or losses; Text Origin: Commission Proposal + Annexes
Article 29(7), point (f)					
G	431	(f) adherence to approved codes of conduct or approved certification mechanisms;	(f) adherence to approved codes of conduct or approved certification mechanisms;	(f) adherence to approved codes of conduct or approved certification mechanisms;	(f) adherence to approved codes of conduct or approved certification mechanisms; Text Origin: Commission Proposal + Annexes
Article 29(7), point (g)					
G	432	(g) the level of cooperation of the natural or legal person(s) held responsible with the competent authorities.	(g) the level of cooperation of the natural or legal person(s) held responsible with the competent authorities.	(g) the level of cooperation of the natural or legal person(s) held responsible with the competent authorities.	(g) the level of cooperation of the natural or legal person(s) held responsible with the competent authorities. Text Origin: Commission Proposal + Annexes
Article 29(8)					
G	433	8. The competent authorities shall set out a detailed reasoning for their enforcement decisions.	8. The competent authorities shall set out a detailed reasoning for their enforcement decisions.	8. The competent authorities shall set out a detailed reasoning for their enforcement decisions.	8. The competent authorities shall set out a detailed reasoning for their enforcement decisions.

		Before taking such decisions, the competent authorities shall notify the entities concerned of their preliminary findings and allow a reasonable time for those entities to submit observations.	Before taking such decisions, the competent authorities shall notify the entities concerned of their preliminary findings and allow a reasonable time for those entities to submit observations.	Before taking such decisions, the competent authorities shall notify the entities concerned of their preliminary findings and allow a reasonable time for those entities to submit observations***, unless in case of imminent danger***.	Before taking such decisions, the competent authorities shall notify the entities concerned of their preliminary findings***. They shall also*** ~~*and*~~ allow a reasonable time for those entities to submit observations***, except in duly justified cases where this could impede immediate action to prevent or respond to incidents***. To be reflected in a recital
Article 29(9)					
G	434	9. Member States shall ensure that their competent authorities inform the relevant competent authorities of the Member State concerned designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, or as an entity equivalent to a critical entity, under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] with the obligations pursuant to this Directive. Upon request of competent authorities under Directive (EU) XXXX/XXXX	9. Member States shall ensure that their competent authorities inform the relevant competent authorities of ~~*the Member State concerned*~~***all relevant Member States*** designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, or as an entity equivalent to a critical entity, under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] with the obligations pursuant to this Directive. Upon request of competent authorities under	9. Member States shall ensure that their competent authorities ***under this Directive*** inform the relevant competent authorities ~~*of the*~~ ***within that same*** Member State ~~*concerned*~~ designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, ***[***or as an entity equivalent to a critical entity***]***, under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] with the obligations pursuant to this Directive. ~~*Upon request of*~~***Where***	9. Member States shall ensure that their competent authorities ***under this Directive*** inform the relevant competent authorities ~~*of the*~~ ***within that same*** Member State ~~*concerned*~~ designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, ***[***or as an entity equivalent to a critical entity***]***, under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] with the obligations pursuant to this Directive. ~~*Upon request of*~~***Where***

		[Resilience of Critical Entities Directive], competent authorities may exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent.	Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], competent authorities may exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent.	***appropriate,*** competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]~~,~~ ***may request*** competent authorities ~~*may*~~***under this Directive to*** exercise their supervisory and enforcement powers ~~*on*~~***in relation to*** an essential entity ***under the scope of this Directive that is also*** identified as critical ***[***or equivalent***[under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]***.	***appropriate,*** competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]~~,~~ ***may request*** competent authorities ~~*may*~~***under this Directive to*** exercise their supervisory and enforcement powers ~~*on*~~***in relation to*** an essential entity ***under the scope of this Directive that is also*** identified as critical ***[***or equivalent***[under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]***. To be checked with CER. Text Origin: Council Mandate
Article 29(10)					
G	434a			***10. Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum pursuant to Article 29 (1) of Regulation (EU) XXXX/XXXX [DORA] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity designated as critical ICT third-party service provider pursuant to Article 28 of Regulation (EU) XXXX/XXXX***	deleted

				[DORA] with the obligations pursuant to this Directive.	
Article 29(9a)					
G	434b		***9a. Member States shall ensure that their competent authorities cooperate with the relevant competent authorities of the Member State concerned designated pursuant to Regulation (EU) XXXX/XXXX [DORA].***		***9b. Member States shall ensure that their competent authorities cooperate with the relevant competent authorities of the Member State concerned designated pursuant to Regulation (EU) XXXX/XXXX [DORA], in particular Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum pursuant to Article 29 (1) of Regulation (EU) XXXX/XXXX [DORA] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity designated as critical ICT third-party service provider pursuant to Article 28 of Regulation (EU) XXXX/XXXX [DORA] with the obligations pursuant to this Directive.***
Article 29(10a)					
G	434c			***10a. Member States shall ensure that their competent authorities***	deleted

				under this Directive inform the relevant competent authorities designated pursuant to Regulation (EU) 910/2014 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an entity designated as trust service providers pursuant to Regulation (EU) 910/2014, with the obligations pursuant to this Directive.	
Article 30					
435	Article 30 Supervision and enforcement for important entities	Article 30 Supervision and enforcement for important entities	Article 30 Supervision and enforcement for important entities	Article 30 Supervision and enforcement for important entities Text Origin: Commission Proposal + Annexes	
Article 30(1)					
436	1. When provided with evidence or indication that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through ex post	1. When provided with evidence or indication that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through ex post	1. When provided with evidence or indication ***or information*** that an important entity is ***allegedly*** not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through	1. When provided with evidence or indication***, or information*** that an important entity is ***allegedly*** not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through	

		supervisory measures.	supervisory measures. ***Member States shall ensure that those measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.***	***ex post*** ~~*ex post*~~ supervisory measures.	ex post supervisory measures. ***Member States shall ensure that those measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.***
	Article 30(2), introductory part				
G	437	2. Member States shall ensure that the competent authorities, where exercising their supervisory tasks in relation to important entities, have the power to subject those entities to:	2. Member States shall ensure that the competent authorities, where exercising their supervisory tasks in relation to important entities, have the power to subject those entities to:	2. Member States shall ensure that the competent authorities, where exercising their supervisory tasks in relation to important entities, ***follow a risk-based approach and*** have the power to subject those entities ***at least*** to:	2. Member States shall ensure that the competent authorities, where exercising their supervisory tasks in relation to important entities, have the power to subject those entities ***at least*** to:
	Article 30(2), point (a)				
G	438	(a) on-site inspections and off-site ex post supervision;	(a) on-site inspections and off-site ex post supervision ***conducted by trained professionals***;	(a) on-site inspections and off-site ex post supervision;	(a) on-site inspections and off-site ex post supervision ***conducted by trained professionals***; recital - see Art. 29
	Article 30(2), point (aa)				
G	438a		***(aa) investigation of cases of non-compliance and the effects thereof on the security of the services;***		deleted

	Article 30(2), point (b)				
G	439	(b) targeted security audits based on risk assessments or risk-related available information;	(b) targeted security audits ~~based on risk assessments or risk-related available information~~***carried out by a qualified independent body or a competent authority***;	(b) targeted security audits based on risk assessments or risk-related available information;	(b) targeted security audits ~~based on risk assessments or risk-related available information~~***carried out by an independent body or a competent authority***;
	Article 30(2), point (c)				
G	440	(c) security scans based on objective, fair and transparent risk assessment criteria;	(c) security scans based on objective, ***non-discriminatory,*** fair and transparent risk assessment criteria;	(c) security scans based on objective, ***non-discriminatory,*** fair and transparent risk assessment criteria***, where necessary for technical reasons, with the cooperation of the entity concerned***;	(c) security scans based on objective, ***non-discriminatory,*** fair and transparent risk assessment criteria***, where necessary, with the cooperation of the entity concerned***;
	Article 30(2), point (d)				
G	441	(d) requests for any information necessary to assess ex-post the cybersecurity measures, including documented cybersecurity policies, as well as compliance with the obligation to notify ENISA pursuant to Article 25(1) and (2);	(d) requests for any information necessary to assess ex-post the cybersecurity measures, including documented cybersecurity policies, as well as compliance with the obligation to notify ENISA pursuant to Article 25(1) and (2);	(d) requests for any information necessary to assess ex-post the cybersecurity measures~~, including documented cybersecurity policies, as well as compliance with the obligation to notify ENISA pursuant to Article 25(1) and (2)~~;	(d) requests for any information necessary to assess ex-post the cybersecurity measures, including documented cybersecurity policies, as well as compliance with the obligation to notify ~~ENISA~~***competent authorities*** pursuant to Article ~~25(1) and (2)~~***25***;
	Article 30(2), point (e)				
G	442				

		(e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks.	(e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks.	(e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks.	(e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks. Text Origin: Commission Proposal + Annexes
Article 30(2), point (ea)					
G	442a			***(ea) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.***	***(ea) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.*** Text Origin: Council Mandate
Article 30(2a)					
G	442b			***(2a) Where exercising their supervisory tasks provided for in paragraph 2 of this Article, competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.***	deleted
Article 30(2), subparagraphs 1a & 1b					
G	442c		***The targeted security audits,***		***2a. The targeted security audits,***

			referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information. ***The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by a qualified independent body shall be paid by the entity concerned.***		***referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.*** ***The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the entity concerned, except in duly justified cases when the competent authority decides otherwise.***
Article 30(3)					
G	443	3. Where exercising their powers pursuant to points (d) or (e) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.	3. Where exercising their powers pursuant to points (d) or (e) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.	3. Where exercising their powers pursuant to points (d) ~~or (e)~~***to (ea)*** of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.	3. Where exercising their powers pursuant to points (d) ~~or (e)~~***to (ea)*** of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested. Text Origin: Council Mandate
Article 30(4), introductory part					
G	444	4. Member States shall ensure that	4. Member States shall ensure that	4. Member States shall ensure that	4. Member States shall ensure that

		the competent authorities, where exercising their enforcement powers in relation to important entities, have the power to:	the competent authorities, where exercising their enforcement powers in relation to important entities, have the power to:	the competent authorities, where exercising their enforcement powers in relation to important entities, have the power ***at least*** to:	the competent authorities, where exercising their enforcement powers in relation to important entities, have the power ***at least*** to: Text Origin: Council Mandate
	Article 30(4), point (a)				
G	445	(a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;	(a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;	(a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;	(a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive; Text Origin: Commission Proposal + Annexes
	Article 30(4), point (b)				
G	446	(b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringement of the obligations laid down in this Directive;	(b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringement of the obligations laid down in this Directive;	(b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringement of the obligations laid down in this Directive;	(b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringement of the obligations laid down in this Directive; Text Origin: Commission Proposal + Annexes
	Article 30(4), point (c)				
G	447	(c) order those entities to cease conduct that is in non-compliant	(c) order those entities to cease conduct that is in non-compliant	(c) order those entities to cease conduct that is in non-compliant	(c) order those entities to cease conduct that is in non-compliant

		with the obligations laid down in this Directive and desist from repeating that conduct;	with the obligations laid down in this Directive and desist from repeating that conduct;	with the obligations laid down in this Directive and desist from repeating that conduct;	with the obligations laid down in this Directive and desist from repeating that conduct; Text Origin: Commission Proposal + Annexes
Article 30(4), point (d)					
G	448	(d) order those entities to bring their risk management measures or the reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;	(d) order those entities to bring their risk management measures or the reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;	(d) order those entities to bring their risk management measures or the reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;	(d) order those entities to bring their risk management measures or the reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period; Text Origin: Commission Proposal + Annexes
Article 30(4), point (e)					
G	449	(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;	(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;	(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of ***the nature of the threat, as well as*** any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;	(e) order those entities to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat of ***the nature of the threat, as well as*** any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat; Text Origin: Council Mandate

Article 30(4), point (f)					
G	450	(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;	(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;	(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline;	(f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline; Text Origin: Commission Proposal + Annexes
Article 30(4), point (g)					
G	451	(g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner;	(g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner;	(g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner, ***when such public disclosure does not lead to a harmful exposure of the respective entity***;	(g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner; Text Origin: Commission Proposal + Annexes
Article 30(4), point (h)					
G	452	(h) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;	~~*(h) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;*~~	(h) ~~*make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;*~~	Deleted
Article 30(4), point (i)					

G	453	(i) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (h) of this paragraph, depending on the circumstances of each individual case.	(i) impose or request the imposition by the relevant bodies or courts ~~according to~~***in accordance with*** national ~~laws~~***law*** of an administrative fine pursuant to Article 31 in addition to~~, or instead of,~~ the measures referred to in points (a) to (h) of this paragraph, depending on the circumstances of each individual case.	(i) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (h) of this paragraph, depending on the circumstances of each individual case.	(i) impose or request the imposition by the relevant bodies or courts ~~according to~~***in accordance with*** national ~~laws~~***law*** of an administrative fine pursuant to Article 31 in addition to~~, or instead of,~~ ***any of*** the measures referred to in points (a) to ~~(h)~~***(g)*** of this paragraph, depending on the circumstances of each individual case.	G
Article 30(5)					
G	454	5. Article 29 (6) to (8) shall also apply to the supervisory and enforcement measures provided for in this Article for the important entities listed in Annex II.	5. Article 29 (6) to (8) shall also apply to the supervisory and enforcement measures provided for in this Article for the important entities listed in Annex II.	5. Article 29 (6) to (8) shall also apply to the supervisory and enforcement measures provided for in this Article for ~~the~~ important entities ~~listed in Annex II~~.	5. Article 29 (6) to (8) shall also apply to the supervisory and enforcement measures provided for in this Article for ~~the~~ important entities ~~listed in Annex II~~. Text Origin: Council Mandate	G
Article 31					
G	455	Article 31 General conditions for imposing administrative fines on essential and important entities	Article 31 General conditions for imposing administrative fines on essential and important entities	Article 31 General conditions for imposing administrative fines on essential and important entities	Article 31 General conditions for imposing administrative fines on essential and important entities Text Origin: Commission Proposal + Annexes	G
Article 31(1)					

G	456	1. Member States shall ensure that the imposition of administrative fines on essential and important entities pursuant to this Article in respect of infringements of the obligations laid down in this Directive are, in each individual case, effective, proportionate and dissuasive.	1. Member States shall ensure that the imposition of administrative fines on essential and important entities pursuant to this Article in respect of infringements of the obligations laid down in this Directive are, in each individual case, effective, proportionate and dissuasive.	1. Member States shall ensure that the imposition of administrative fines on essential and important entities pursuant to this Article in respect of infringements of the obligations laid down in this Directive are, in each individual case, effective, proportionate and dissuasive.	1. Member States shall ensure that the imposition of administrative fines on essential and important entities pursuant to this Article in respect of infringements of the obligations laid down in this Directive are, in each individual case, effective, proportionate and dissuasive. Text Origin: Commission Proposal + Annexes	G
Article 31(2)					
G	457	2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4).	2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to~~, or instead of,~~ measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4).	2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4).	2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to~~, or instead of,~~ ***any of the*** measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4).	G
Article 31(3)					
G	458	3. Where deciding whether to impose an administrative fine and deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article	3. Where deciding whether to impose an administrative fine and deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article	3. Where deciding whether to impose an administrative fine and deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article	3. Where deciding whether to impose an administrative fine and deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article	G

		29(7).	29(7).	29(7).	29(7). Text Origin: Commission Proposal + Annexes
	Article 31(4)				
R	459	4. Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.	4. Member States shall ensure that infringements of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the essential or important entity belongs in the preceding financial year, whichever is higher.	4. Member States shall ensure that infringements ***by the essential entities*** of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least ~~*10 000 000*~~***4 000 000*** EUR or***, in the case of a legal person,*** ~~*up to*~~ 2% of the total worldwide annual turnover of the undertaking to which the essential ~~*or important*~~ entity belongs in the preceding financial year, whichever is higher.	4. Member States shall ensure that infringements ***by essential entities*** of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least 10 000 000 EUR or up to 2% of the total worldwide annual turnover of the undertaking to which the ~~*essential or important*~~ entity belongs in the preceding financial year, whichever is higher. EP political check Text Origin: EP Mandate	R
	Article 31(4a)				
R	459a		***4a. Member States shall ensure that infringements by the important entities of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to***	***4a. Member States shall ensure that infringements by the important entities of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to***	R

				administrative fines of a maximum of at least 2 000 000 EUR or, in the case of a legal person, 1% of the total worldwide annual turnover of the undertaking to which the important entity belongs in the preceding financial year, whichever is higher.	***administrative fines of a maximum of at least 2 000 000 EUR or, in the case of a legal person, 1% of the total worldwide annual turnover of the undertaking to which the important entity belongs in the preceding financial year, whichever is higher.*** EP political issue Text Origin: Council Mandate
Article 31(5)					
G	460	5. Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement in accordance with a prior decision of the competent authority.	5. Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement in accordance with a prior decision of the competent authority.	5. Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement in accordance with a prior decision of the competent authority.	5. Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement in accordance with a prior decision of the competent authority. Text Origin: Commission Proposal + Annexes
Article 31(6)					
G	461	6. Without prejudice to the powers of competent authorities pursuant to Articles 29 and 30, each Member State may lay down the rules on whether and to what	6. Without prejudice to the powers of competent authorities pursuant to Articles 29 and 30, each Member State may lay down the rules on whether and to what	6. Without prejudice to the powers of competent authorities pursuant to Articles 29 and 30, each Member State may lay down the rules on whether and to what	6. Without prejudice to the powers of competent authorities pursuant to Articles 29 and 30, each Member State may lay down the rules on whether and to what

		extent administrative fines may be imposed on public administration entities referred to in Article 4(23) subject to the obligations provided for by this Directive.	extent administrative fines may be imposed on public administration entities referred to in Article 4(23) subject to the obligations provided for by this Directive.	extent administrative fines may be imposed on public administration entities referred to in Article 4(23) subject to the obligations provided for by this Directive.	extent administrative fines may be imposed on public administration entities referred to in Article 4(23) subject to the obligations provided for by this Directive. Text Origin: Commission Proposal + Annexes
Article 31(6a)					
G	461a			***6a. Where the legal system of the Member State does not provide for administrative fines, Member States shall ensure that this Article may be applied in such a manner that the fine is initiated by the competent authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by the competent authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by […] and, without delay, any subsequent amendment law or amendment affecting them.***	***6a. Where the legal system of the Member State does not provide for administrative fines, Member States shall ensure that this Article may be applied in such a manner that the fine is initiated by the competent authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by the competent authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by […] and, without delay, any subsequent amendment law or amendment affecting them.*** Text Origin: Council Mandate

Article 32					
G	462	Article 32 Infringements entailing a personal data breach	Article 32 Infringements entailing a personal data breach	Article 32 Infringements entailing a personal data breach	Article 32 Infringements entailing a personal data breach Text Origin: Commission Proposal + Annexes
Article 32(1)					
G	463	1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation within a reasonable period of time.	1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined ~~by~~***in*** Article 4***, point*** (12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ***without undue delay and in any event*** within ~~a reasonable period of time~~***72 hours of becoming aware of a data breach***.	1. Where***, in the course of supervision or enforcement,*** the competent authorities have ~~indications~~***become aware*** that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 ~~entails~~***of this Directive may entail*** a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall***, without undue delay,*** inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ~~within a reasonable period of time~~.	1. Where***, in the course of supervision or enforcement,*** the competent authorities have ~~indications~~***become aware*** that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 ~~entails~~***of this Directive may entail*** a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall***, without undue delay,*** inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ~~within a reasonable period of time~~.
Article 32(2)					

G	464	2. Where the supervisory authorities competent in accordance with Articles 55 and 56 of Regulation (EU) 2016/679 decide to exercise their powers pursuant to Article 58(i) of that Regulation and impose an administrative fine, the competent authorities shall not impose an administrative fine for the same infringement under Article 31 of this Directive. The competent authorities may, however, apply the enforcement actions or exercise the sanctioning powers provided for in points (a) to (i) of Article 29 (4), Article 29 (5), and points (a) to (h) of Article 30 (4) of this Directive.	2. Where the supervisory authorities competent in accordance with Articles 55 and 56 of Regulation (EU) 2016/679 decide to exercise their powers pursuant to Article 58(i) of that Regulation and impose an administrative fine, the competent authorities shall not impose an administrative fine for the same infringement under Article 31 of this Directive. The competent authorities may, however, apply the enforcement actions or exercise the sanctioning powers provided for in points (a) to (i) of Article 29 (4), Article 29 (5), and points (a) to (h) of Article 30 (4) of this Directive.	2. Where the supervisory authorities competent in accordance with Articles 55 and 56 of Regulation (EU) 2016/679 decide to exercise their powers pursuant to Article ~~58(i)~~***58(2)(i)*** of that Regulation and impose an administrative fine, the competent authorities ***referred to in Article 8 of this Directive*** shall not impose an administrative fine for ***an infringement by*** the same ~~infringement under~~***deed of*** Article 31 of this Directive. The competent authorities may, however, apply the enforcement actions or exercise the sanctioning powers provided for in points (a) to (i) of Article 29 (4), Article 29 (5), and points (a) to (h) of Article 30 (4) of this Directive.	2. Where the supervisory authorities competent in accordance with Articles 55 and 56 of Regulation (EU) 2016/679 decide to exercise their powers pursuant to Article ~~58(i)~~***58(2)(i)*** of that Regulation and impose an administrative fine, the competent authorities ***referred to in Article 8 of this Directive*** shall not impose an administrative fine for ***an infringement by*** the same ~~infringement under~~***deed of*** Article 31 of this Directive. The competent authorities may, however, apply the enforcement actions or exercise the sanctioning powers provided for in points (a) to (i) of Article 29 (4), Article 29 (5), and points (a) to (h) of Article 30 (4) of this Directive. Text Origin: Council Mandate	G
Article 32(3)					
G	465	3. Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority may inform the supervisory authority established	3. Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority ~~may~~***shall*** inform the supervisory authority established	3. Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority may inform the supervisory authority established	3. Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority ~~may~~***shall*** inform the supervisory authority established	G

		in the same Member State.	in the same Member State.	in the same Member State.	in the same Member State. Text Origin: EP Mandate
	Article 33				
G	466	Article 33 Penalties	Article 33 Penalties	Article 33 Penalties	Article 33 Penalties Text Origin: Commission Proposal + Annexes
	Article 33(1)				
G	467	1. Member States shall lay down rules on penalties applicable to the infringements of national provisions adopted pursuant to this Directive, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.	1. Member States shall lay down rules on penalties applicable to the infringements of national provisions adopted pursuant to this Directive, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.	1. Member States shall lay down rules on penalties applicable to the infringements of national provisions adopted pursuant to this Directive, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.	1. Member States shall lay down rules on penalties applicable to the infringements of national provisions adopted pursuant to this Directive, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Text Origin: Commission Proposal + Annexes
	Article 33(2)				
G	468	2. Member States shall, by [two] years following the entry into force of this Directive, notify the	2. Member States shall, by [two] years following the entry into force of this Directive, notify the	2. Member States shall, by [two] years following the entry into force of this Directive, notify the	2. Member States shall, by [two] years following the entry into force of this Directive, notify the

		Commission of those rules and of those measures and shall notify it, without undue delay of any subsequent amendment affecting them.	Commission of those rules and of those measures and shall notify it, without undue delay of any subsequent amendment affecting them.	Commission of those rules and of those measures and shall notify it, without undue delay of any subsequent amendment affecting them.	Commission of those rules and of those measures and shall notify it, without undue delay of any subsequent amendment affecting them. Text Origin: Commission Proposal + Annexes
Article 34					
G	469	Article 34 Mutual assistance	Article 34 Mutual assistance	Article 34 Mutual assistance	Article 34 Mutual assistance Text Origin: Commission Proposal + Annexes
Article 34(1), introductory part					
G	470	1. Where an essential or important entity is providing services in more than one Member State, or has its main establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or other establishment or of the representative, and the competent authorities of those other Member States shall cooperate with and	1. Where an essential or important entity is providing services in more than one Member State, or has its main establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or other establishment or of the representative, and the competent authorities of those other Member States shall cooperate with and assist each other as necessary. That	1. Where an essential or important entity is providing services in more than one Member State, or ***is providing services in one or more*** ~~has its main establishment or a representative in a~~ Member ~~State~~***States***, but its network and information systems are located in one or more other Member States, the competent ~~authority~~***authorities*** of the Member ~~State of the main establishment or other establishment or of the representative, and the competent authorities of those other Member~~	1. Where an essential or important entity is providing services in more than one Member State, or ***is providing services in one or more*** ~~has its main establishment or a representative in a~~ Member ~~State~~***States***, but its network and information systems are located in one or more other Member States, the competent ~~authority~~***authorities*** of the Member ~~State of the main establishment or other establishment or of the representative, and the competent authorities of those other Member~~

		assist each other as necessary. That cooperation shall entail, at least, that:	cooperation shall entail, at least, that:	States ***concerned*** shall cooperate with and assist each other as necessary. That cooperation shall entail, at least, that:	States ***concerned*** shall cooperate with and assist each other as necessary. That cooperation shall entail, at least, that: Text Origin: Council Mandate
	Article 34(1), point (a)				
G	471	(a) the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken and their follow-up, in accordance with Articles 29 and 30;	(a) the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken and their follow-up, in accordance with Articles 29 and 30;	(a) the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken ~~*and their follow-up, in accordance with Articles 29 and 30*~~;	(a) the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken ~~*and their follow-up, in accordance with Articles 29 and 30*~~; Text Origin: Council Mandate
	Article 34(1), point (b)				
G	472	(b) a competent authority may request another competent authority to take the supervisory or enforcement measures referred to in Articles 29 and 30;	(b) a competent authority may request another competent authority to take the supervisory or enforcement measures referred to in Articles 29 and 30;	(b) a competent authority may request another competent authority to take the supervisory or enforcement measures ~~*referred to in Articles 29 and 30*~~;	(b) a competent authority may request another competent authority to take ~~*the*~~ supervisory or enforcement measures ~~*referred to in Articles 29 and 30*~~;
	Article 34(1), point (c)				
G	473				

	(c) a competent authority shall, upon receipt of a justified request from another competent authority, provide the other competent authority with assistance so that the supervision or enforcement actions referred to in Articles 29 and 30 can be implemented in an effective, efficient and consistent manner. Such mutual assistance may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed may not refuse that request unless, after an exchange with the other authorities concerned, ENISA and the Commission, it is established that either the authority is not competent to provide the requested assistance or the requested assistance is not proportionate to the supervisory tasks of the competent authority carried out in accordance with Article 29 or Article 30.	(c) a competent authority shall, upon receipt of a justified request from another competent authority, provide the other competent authority with assistance so that the supervision or enforcement actions referred to in Articles 29 and 30 can be implemented in an effective, efficient and consistent manner. Such mutual assistance may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed may not refuse that request unless, after an exchange with the other authorities concerned, ENISA and the Commission, it is established that either the authority is not competent to provide the requested assistance or the requested assistance is not proportionate to the supervisory tasks of the competent authority carried out in accordance with Article 29 or Article 30.	(c) a competent authority shall, upon receipt of a justified request from another competent authority, provide the other competent authority with assistance ~~so that the supervision or enforcement actions referred to in Articles 29 and 30~~***proportionate to the resources at its own disposal so that the supervision or enforcement actions*** can be implemented in an effective, efficient and consistent manner. Such mutual assistance may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed may not refuse that request unless, after an exchange with the other authorities concerned, ~~ENISA and the Commission,~~ it is established that ~~either~~ the authority is not competent to provide the requested assistance or ***does not have the necessary resources or*** the requested assistance is not proportionate to the supervisory tasks of the competent authority carried out ***or the request concerns information or entails activities which are in conflict***	(c) a competent authority shall, upon receipt of a justified request from another competent authority, provide the other competent authority with assistance ~~so that the supervision or enforcement actions referred to in Articles 29 and 30~~***proportionate to the resources at its own disposal so that the supervision or enforcement actions*** can be implemented in an effective, efficient and consistent manner. Such mutual assistance may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed may not refuse that request unless, after an exchange with the other authorities concerned, ~~ENISA and~~***and, upon request of one of the Member States concerned, with*** the Commission ***in consultation with ENISA***, it is established that ~~either~~ the authority is not competent to provide the requested assistance or the requested assistance is not proportionate to the supervisory tasks of the competent authority carried out ***or the request***

				with that Member State's national security or public security or defence ~~*in accordance with Article 29 or Article 30*~~.	***concerns information or entails activities which are in conflict with that Member State's national security or public security or defence*** ~~*in accordance with Article 29 or Article 30*~~. Text Origin: Council Mandate
Article 34(2)					
G	474	2. Where appropriate and with common agreement, competent authorities from different Member States may carry out the joint supervisory actions referred to in Articles 29 and 30.	2. Where appropriate and with common agreement, competent authorities from different Member States may carry out the joint supervisory actions referred to in Articles 29 and 30.	2. Where appropriate and with common agreement, competent authorities from different Member States may carry out the joint supervisory actions ~~*referred to in Articles 29 and 30.*~~	2. Where appropriate and with common agreement, competent authorities from different Member States may carry out the joint supervisory actions ~~*referred to in Articles 29 and 30.*~~ Text Origin: Council Mandate
CHAPTER VII					
G	475	CHAPTER VII Transitional and final provisions	CHAPTER VII Transitional and final provisions	CHAPTER VII Transitional and final provisions	CHAPTER VII Transitional and final provisions Text Origin: Commission Proposal + Annexes
Article 35					
G	476	Article 35 Review	Article 35 Review	Article 35 Review	Article 35 Review Text Origin: Commission

					Proposal + Annexes
Article 35, first paragraph					
G	477	The Commission shall periodically review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of sectors, subsectors, size and type of entities referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The first report shall be submitted by… □54 months after the date of entry into force of this Directive□.	***By... [42 months after the date of entry into force of this Directive] and every 36 months thereafter,*** the Commission shall ~~*periodically*~~ review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of ***the*** sectors, subsectors, size and type of entities referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. ~~*For this purpose*~~***To that end*** and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. ~~*The first*~~ ***The*** report shall be ~~*submitted by… □54 months after the date of entry into force of this Directive□.*~~***accompanied, where necessary, by a legislative proposal.***	The Commission shall periodically review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of sectors, subsectors, size and type of entities referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. For ~~*this*~~***the*** purpose ~~*and with a view to further advancing the strategic and operational cooperation*~~***of the review,*** , the Commission shall take into account the reports of the ~~*Cooperation Group and the*~~ CSIRTs network on the experience gained at a ~~*strategic and*~~ operational level. The first report shall be submitted by… ~~□~~***[***54 months after the date of entry into force of this Directive~~□~~***]***.	***By... [42 months after the date of entry into force of this Directive] and every 36 months thereafter,*** the Commission shall ~~*periodically*~~ review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of ***the*** sectors, subsectors, size and type of entities referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. ~~*For this purpose*~~***To that end*** and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. ~~*The first*~~ ***The*** report shall be ~~*submitted by… □54 months after the date of entry into force of this Directive□.*~~***accompanied, where necessary, by a legislative proposal.***	G

					Period of transposition COM align with Art 12 (Cooperation Group reporting) Text Origin: EP Mandate	
	Article 36					
R	478	Article 36 Exercise of the delegation	Article 36 Exercise of the delegation	~~*Article 36*~~ ~~*Exercise of the delegation*~~		R
	Article 36(1)					
R	479	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	~~*1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.*~~		R
	Article 36(2)					
R	480	2. The power to adopt delegated acts referred to in Articles 18(6) and 21(2) shall be conferred on the Commission for a period of five years from […]	2. The power to adopt delegated acts referred to in Articles 18(6), ***20(11a)*** and 21(2) shall be conferred on the Commission for a period of five years from […]	~~*2. The power to adopt delegated acts referred to in Articles 18(6) and 21(2) shall be conferred on the Commission for a period of five years from […]*~~		R
	Article 36(3)					
R	481	3. The delegation of power	3. The delegation of power	~~*3. The delegation of power*~~		R

		referred to in Articles 18(6) and 21(2) 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.	referred to in Articles 18(6), ***20(11a)*** and 21(2) 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.	~~*referred to in Articles 18(6) and 21(2) 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.*~~	
Article 36(4)					
R	482	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.	~~*4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.*~~	R
Article 36(5)					
R	483	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	~~*5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.*~~	R
Article 36(6)					

R	484	6. A delegated act adopted pursuant to Articles 18(6) and 21(2) 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 to 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.	6. A delegated act adopted pursuant to Articles 18(6)***, 20(11a)*** and 21(2) 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 to 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.	~~*6. A delegated act adopted pursuant to Articles 18(6) and 21(2) 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 to 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.*~~		R
	Article 37					
G	485	Article 37 Committee procedure	Article 37 Committee procedure	Article 37 Committee procedure	Article 37 Committee procedure Text Origin: Commission Proposal + Annexes	G
	Article 37(1)					
G	486	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation	1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation	G

		(EU) No 182/2011.	(EU) No 182/2011.	(EU) No 182/2011.	(EU) No 182/2011. Text Origin: Commission Proposal + Annexes
Article 37(2)					
G	487	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. Text Origin: Commission Proposal + Annexes
Article 37(3)					
G	488	3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.	3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.	3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.	3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests. Text Origin: Commission Proposal + Annexes
Article 38					
G	489	Article 38 Transposition	Article 38 Transposition	Article 38 Transposition	Article 38 Transposition Text Origin: Commission

					Proposal + Annexes
Article 38(1)					
R	490	1. Member States shall adopt and publish, by … 18 months after the date of entry into force of this Directive, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from … [one day after the date referred to in the first subparagraph].	1. Member States shall adopt and publish, by … 18 months after the date of entry into force of this Directive, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from … [one day after the date referred to in the first subparagraph].	1. ~~*Member States shall adopt and publish, by … 18*~~***By … [24*** months after the date of entry into force of this Directive~~.~~*]. Member States shall adopt and publish* the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from … [one day after the date referred to in the first subparagraph].	R
Article 38(2)					
G	491	2. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.	2. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.	2. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.	2. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States. Text Origin: Commission Proposal + Annexes	G

Article 39					
G	492	Article 39 Amendment of Regulation (EU) No 910/2014	Article 39 Amendment of Regulation (EU) No 910/2014	Article 39 Amendment of Regulation (EU) No 910/2014	Article 39 Amendment of Regulation (EU) No 910/2014 Text Origin: Commission Proposal + Annexes
Article 39, first paragraph					
G	493	Article 19 of Regulation (EU) No 910/2014 is deleted.	Article 19 of Regulation (EU) No 910/2014 is deleted.	~~*Article 19 of*~~***In*** Regulation (EU) No 910/2014***, Article 19*** ~~-~~is deleted ***with effect from… [date of the transposition deadline of this Directive]***.	~~*Article 19 of*~~***In*** Regulation (EU) No 910/2014***, Article 19*** ~~-~~is deleted ***with effect from… [the transposition deadline of this Directive]***. Text Origin: Commission Proposal + Annexes
Article 40					
G	494	Article 40 Amendment of Directive (EU) 2018/1972	Article 40 Amendment of Directive (EU) 2018/1972	Article 40 Amendment of Directive (EU) 2018/1972	Article 40 Amendment of Directive (EU) 2018/1972 Text Origin: Commission Proposal + Annexes
Article 40, first paragraph					
G	495	Articles 40 and 41 of Directive (EU) 2018/1972 are deleted.	Articles 40 and 41 of Directive (EU) 2018/1972 are deleted.	***In Directive (EU) 2018/1972,*** Articles 40 and 41 ***are deleted***	***In Directive (EU) 2018/1972,*** Articles 40 and 41 ***are deleted***

				with effect from… [date of the transposition deadline of this Directive] ~~*of Directive (EU) 2018/1972 are deleted*~~.	***with effect from… [the transposition deadline of this Directive]*** ~~*of Directive (EU) 2018/1972 are deleted.*~~ Text Origin: Commission Proposal + Annexes
Article 41					
G	496	Article 41 Repeal	Article 41 Repeal	Article 41 Repeal	Article 41 Repeal Text Origin: Commission Proposal + Annexes
Article 41, first paragraph					
G	497	Directive (EU) 2016/1148 is repealed with effect from.. [date of transposition deadline of the Directive].	Directive (EU) 2016/1148 is repealed with effect from.. [date of transposition deadline of the Directive].	Directive (EU) 2016/1148 is repealed with effect from.. [date of transposition deadline of the Directive].	Directive (EU) 2016/1148 is repealed with effect from.. [date of transposition deadline of the Directive]. Text Origin: Commission Proposal + Annexes
Article 41, second paragraph					
G	498	References to Directive (EU) 2016/1148 shall be construed as references to this Directive and read in accordance with the correlation table set out in Annex III.	References to Directive (EU) 2016/1148 shall be construed as references to this Directive and read in accordance with the correlation table set out in Annex III.	References to Directive (EU) 2016/1148 shall be construed as references to this Directive and read in accordance with the correlation table set out in Annex III.	References to Directive (EU) 2016/1148 shall be construed as references to this Directive and read in accordance with the correlation table set out in Annex III.

					Text Origin: Commission Proposal + Annexes
Article 42					
499	Article 42 Entry into force	Article 42 Entry into force	Article 42 Entry into force	Article 42 Entry into force Text Origin: Commission Proposal + Annexes
Article 42, first paragraph				
500	This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	This Directive 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 + Annexes
Article 42, first paragraph a				
500a		***However, Articles 39 and 40 shall apply from ... [18 months after the date of entry into force of this Directive].***		Deleted Text Origin: EP Mandate
Article 43				
501				

		Article 43 Addressees	Article 43 Addressees	Article 43 Addressees	Article 43 Addressees Text Origin: Commission Proposal + Annexes
Article 43, first paragraph					
G	502	This Directive is addressed to the Member States.	This Directive is addressed to the Member States.	This Directive is addressed to the Member States.	This Directive is addressed to the Member States. Text Origin: Commission Proposal + Annexes
Formula					
G	503	Done at Brussels,	Done at Brussels,	Done at Brussels,	Done at Brussels, Text Origin: Commission Proposal + Annexes
Formula					
G	504	For the European Parliament	For the European Parliament	For the European Parliament	For the European Parliament Text Origin: Commission Proposal + Annexes
Formula					
G	505	The President	The President	The President	The President Text Origin: Commission Proposal + Annexes

Formula					
G	506	For the Council	For the Council	For the Council	For the Council Text Origin: Commission Proposal + Annexes
Formula					
G	507	The President	The President	The President	The President Text Origin: Commission Proposal + Annexes
Formula					
G	507a	ESSENTIAL ENTITIES	ESSENTIAL ENTITIES	ESSENTIAL ENTITIES	~~*ESSENTIAL ENTITIES*~~***SECTORS OF HIGH CRITICALITY***
Annex I.					
G	507b	SECTORS, SUBSECTORS AND TYPES OF ENTITIES	SECTORS, SUBSECTORS AND TYPES OF ENTITIES	SECTORS, SUBSECTORS AND TYPES OF ENTITIES	
Formula					
G	507c	Sector	Sector	Sector	
Formula					

G	507d	Subsector	Subsector	Subsector		G
	Formula					
G	507e	Type of entity	Type of entity	Type of entity		G
	Annex I. 1					
G	507f	1. Energy	1. Energy	1. Energy		G
	Annex I. 1(a)					
G	507g	(a) Electricity — Electricity undertakings referred to in point (57) of Article 2 of Directive (EU) 2019/944, which carry out the function of ‘supply’ referred to in point (12) of Article 2 of that Directive (1) — Distribution system operators referred to in point (29) of Article 2 of Directive (EU) 2019/944 — Transmission system operators referred to in point (35) of Article 2 of Directive (EU) 2019/944 — Producers referred to in point (38) of Article 2 of Directive (EU) 2019/944 — Nominated electricity market operators referred to in point 8 of Article 2 of Regulation (EU)	(a) Electricity — Electricity undertakings referred to in point (57) of Article 2 of Directive (EU) 2019/944, which carry out the function of ‘supply’ referred to in point (12) of Article 2 of that Directive (1) — Distribution system operators referred to in point (29) of Article 2 of Directive (EU) 2019/944 — Transmission system operators referred to in point (35) of Article 2 of Directive (EU) 2019/944 — Producers referred to in point (38) of Article 2 of Directive (EU) 2019/944 — Nominated electricity market operators referred to in point 8 of Article 2 of Regulation (EU)	(a) Electricity — Electricity undertakings referred to in point (57) of Article 2 of Directive (EU) 2019/944, which carry out the function of ‘supply’ referred to in point (12) of Article 2 of that Directive (1) — Distribution system operators referred to in point (29) of Article 2 of Directive (EU) 2019/944 — Transmission system operators referred to in point (35) of Article 2 of Directive (EU) 2019/944 — Producers referred to in point (38) of Article 2 of Directive (EU) 2019/944 — Nominated electricity market operators referred to in point 8 of Article 2 of Regulation (EU)		G

		2019/943 (2) — Electricity market participants referred to in point (25) of Article 2 of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services referred to in points (18), (20) and (59) of Article 2 of Directive (EU) 2019/944 __________ 1. Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p.125). 2. Regulation (EU) 2019/943 of the European Parliament and of the Council on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).	2019/943 (2) — Electricity market participants referred to in point (25) of Article 2 of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services referred to in points (18), (20) and (59) of Article 2 of Directive (EU) 2019/944 __________ 1. Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p.125). 2. Regulation (EU) 2019/943 of the European Parliament and of the Council on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).	2019/943 (2) — Electricity market participants referred to in point (25) of Article 2 of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services referred to in points (18), (20) and (59) of Article 2 of Directive (EU) 2019/944 __________ 1. Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p.125). 2. Regulation (EU) 2019/943 of the European Parliament and of the Council on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).		
	Annex I. 1(b)					
G	507h	(b) District heating and cooling — District heating or district cooling referred to in point (19) of Article 2 of the Directive (EU) 2018/2001 (1) on the promotion of the use of energy from renewable sources __________ 1. Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).	(b) District heating and cooling — District heating or district cooling referred to in point (19) of Article 2 of the Directive (EU) 2018/2001 (1) on the promotion of the use of energy from renewable sources __________ 1. Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).	(b) District heating and cooling — District heating or district cooling referred to in point (19) of Article 2 of the Directive (EU) 2018/2001 (1) on the promotion of the use of energy from renewable sources __________ 1. Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).		G

	Annex I. 1(c)					
G	507i	(c) Oil — Operators of oil transmission pipelines — Operators of oil production, refining and treatment facilities, storage and transmission — Central oil stockholding entities referred to in point (f) of Article 2 of Council Directive 2009/119/EC (1) __________ 1. Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p.9).	(c) Oil — Operators of oil transmission pipelines — Operators of oil production, refining and treatment facilities, storage and transmission — Central oil stockholding entities referred to in point (f) of Article 2 of Council Directive 2009/119/EC (1) __________ 1. Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p.9).	(c) Oil — Operators of oil transmission pipelines — Operators of oil production, refining and treatment facilities, storage and transmission — Central oil stockholding entities referred to in point (f) of Article 2 of Council Directive 2009/119/EC (1) __________ 1. Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p.9).		G
	Annex I. 1(d)					
G	507j	(d) Gas — Supply undertakings referred to in point (8) of Article 2 of Directive (EU) 2009/73/EC (1) — Distribution system operators referred to in point (6) of Article 2 of Directive 2009/73/EC — Transmission system operators referred to point (4) of Article 2 of Directive 2009/73/EC — Storage system operators referred to in point (10) of Article	(d) Gas — Supply undertakings referred to in point (8) of Article 2 of Directive (EU) 2009/73/EC (1) — Distribution system operators referred to in point (6) of Article 2 of Directive 2009/73/EC — Transmission system operators referred to point (4) of Article 2 of Directive 2009/73/EC — Storage system operators referred to in point (10) of Article	(d) Gas — Supply undertakings referred to in point (8) of Article 2 of Directive (EU) 2009/73/EC (1) — Distribution system operators referred to in point (6) of Article 2 of Directive 2009/73/EC — Transmission system operators referred to point (4) of Article 2 of Directive 2009/73/EC — Storage system operators referred to in point (10) of Article		G

		2 of Directive 2009/73/EC — LNG system operators referred to in point (12) of Article 2 of Directive 2009/73/EC — Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC — Operators of natural gas refining and treatment facilities __________ 1. Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).	2 of Directive 2009/73/EC — LNG system operators referred to in point (12) of Article 2 of Directive 2009/73/EC — Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC — Operators of natural gas refining and treatment facilities __________ 1. Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).	2 of Directive 2009/73/EC — LNG system operators referred to in point (12) of Article 2 of Directive 2009/73/EC — Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC — Operators of natural gas refining and treatment facilities __________ 1. Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).		
	Annex I. 1(e)					
G	507k	(e) Hydrogen Operators of hydrogen production, storage and transmission	(e) Hydrogen Operators of hydrogen production, storage and transmission	(e) Hydrogen Operators of hydrogen production, storage and transmission		G
	Annex I. 2.					
G	507l	2. Transport	2. Transport	2. Transport		G
	Annex I. 2(a)					
G	507m	(a) Air — Air carriers referred to in point (4) of Article 3 of Regulation (EC) No 300/2008 (1)	(a) Air — Air carriers referred to in point (4) of Article 3 of Regulation (EC) No 300/2008 (1)	(a) Air — Air carriers referred to in point (4) of Article 3 of Regulation (EC) No 300/2008 (1) ***used for***	(a) Air — Air carriers referred to in point (4) of Article 3 of Regulation (EC) No 300/2008 (1) ***used for***	G

	— Airport managing bodies referred to in point (2) of Article 2 of Directive 2009/12/EC([2]), airports referred to in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 ([3]), and entities operating ancillary installations contained within airports — Traffic management control operators providing air traffic control (ATC) services referred to in point (1) of Article 2 of Regulation (EC) No 549/2004 ([4]) _____ 1. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p.72). 2. Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p.11). 3. Regulation (EC) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p.1). 4. Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation)	— Airport managing bodies referred to in point (2) of Article 2 of Directive 2009/12/EC([2]), airports referred to in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 ([3]), and entities operating ancillary installations contained within airports — Traffic management control operators providing air traffic control (ATC) services referred to in point (1) of Article 2 of Regulation (EC) No 549/2004 ([4]) _____ 1. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p.72). 2. Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p.11). 3. Regulation (EC) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p.1). 4. Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation)	***commercial purposes*** — Airport managing bodies referred to in point (2) of Article 2 of Directive 2009/12/EC([2]), airports referred to in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 ([3]), and entities operating ancillary installations contained within airports — Traffic management control operators providing air traffic control (ATC) services referred to in point (1) of Article 2 of Regulation (EC) No 549/2004 ([4]) _____ 1. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p.72). 2. Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p.11). 3. Regulation (EC) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p.1). 4. Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the	***commercial purposes*** — Airport managing bodies referred to in point (2) of Article 2 of Directive 2009/12/EC([2]), airports referred to in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 ([3]), and entities operating ancillary installations contained within airports — Traffic management control operators providing air traffic control (ATC) services referred to in point (1) of Article 2 of Regulation (EC) No 549/2004 ([4]) _____ 1. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p.72). 2. Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p.11). 3. Regulation (EC) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p.1). 4. Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the

		(OJ L 96, 31.3.2004, p.1).	(OJ L 96, 31.3.2004, p.1).	framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p.1).	framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p.1). `Text Origin: Council Mandate`	
Annex I. 2(b)						
G	507n	(b) Rail — Infrastructure managers referred to in point (2) of Article 3 of Directive 2012/34/EU(1) — Railway undertakings referred to in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities referred to in point (12) of Article 3 of Directive 2012/34/EU __________ 1. Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p.32).	(b) Rail — Infrastructure managers referred to in point (2) of Article 3 of Directive 2012/34/EU(1) — Railway undertakings referred to in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities referred to in point (12) of Article 3 of Directive 2012/34/EU __________ 1. Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p.32).	(b) Rail — Infrastructure managers referred to in point (2) of Article 3 of Directive 2012/34/EU(1) — Railway undertakings referred to in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities referred to in point (12) of Article 3 of Directive 2012/34/EU __________ 1. Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p.32).		G
Annex I. 2(c)						
G	507o	(c) Water — Inland, sea and coastal passenger and freight water transport companies, referred to for maritime transport in Annex I to Regulation (EC) No 725/2004 (1),	(c) Water — Inland, sea and coastal passenger and freight water transport companies, referred to for maritime transport in Annex I to Regulation (EC) No 725/2004 (1),	(c) Water — Inland, sea and coastal passenger and freight water transport companies, referred to for maritime transport in Annex I to Regulation (EC) No 725/2004 (1),	(c) Water — Inland, sea and coastal passenger and freight water transport companies, referred to for maritime transport in Annex I to Regulation (EC) No 725/2004 (1),	G

		not including the individual vessels operated by those companies — Managing bodies of ports referred to in point (1) of Article 3 of Directive 2005/65/EC (2), including their port facilities referred to in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports — Operators of vessel traffic services referred to in point (o) of Article 3 of Directive 2002/59/EC (3) ________ 1. Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p.6). 2. Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28). 3. Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p.10)	not including the individual vessels operated by those companies — Managing bodies of ports referred to in point (1) of Article 3 of Directive 2005/65/EC (2), including their port facilities referred to in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports — Operators of vessel traffic services referred to in point (o) of Article 3 of Directive 2002/59/EC (3) ________ 1. Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p.6). 2. Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28). 3. Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p.10)	not including the individual vessels operated by those companies — Managing bodies of ports referred to in point (1) of Article 3 of Directive 2005/65/EC (2), including their port facilities referred to in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports — Operators of vessel traffic services referred to in point (o) of Article 3 of Directive 2002/59/EC (3) ________ 1. Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p.6). 2. Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28). 3. Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p.10)	not including the individual vessels operated by those companies — Managing bodies of ports referred to in point (1) of Article 3 of Directive 2005/65/EC (2), including their port facilities referred to in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports — Operators of vessel traffic services referred to in point (o) of Article 3 of Directive 2002/59/EC (3) ________ 1. Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p.6). 2. Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28). 3. Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p.10) Text Origin: Commission Proposal + Annexes	
	Annex I. 2(d)					
Y	507p					Y

	(d) Road — Road authorities referred to in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 ([1]) responsible for traffic management control — Operators of Intelligent Transport Systems referred to in point (1) of Article 4 of Directive 2010/40/EU ([2]) 1. Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU–wide real–time traffic information services (OJ L 157, 23.6.2015, p. 21). 2. Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).	(d) Road — Road authorities referred to in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 ([1]) responsible for traffic management control ***— Operators of smart charging services for electric vehicles*** — Operators of Intelligent Transport Systems referred to in point (1) of Article 4 of Directive 2010/40/EU ([2]) 1. Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU–wide real–time traffic information services (OJ L 157, 23.6.2015, p. 21). 2. Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).	(d) Road — Road authorities referred to in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 ([1]) responsible for traffic management control***, excluding public entities for whom traffic-management or operators of intelligent transport systems is only a non-essential part of their general activity*** — Operators of Intelligent Transport Systems referred to in point (1) of Article 4 of Directive 2010/40/EU ([2]) 1. Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU–wide real–time traffic information services (OJ L 157, 23.6.2015, p. 21). 2. Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).	(d) Road — Road authorities referred to in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 ([1]) responsible for traffic management control***, excluding public entities for whom traffic-management or operators of intelligent transport systems is only a non-essential part of their general activity*** ***— Operators of a recharging points [definition contained in the future Regulation on the deployment of alternative fuels infrastructure to be added].*** — Operators of Intelligent Transport Systems referred to in point (1) of Article 4 of Directive 2010/40/EU ([2]) 1. Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU–wide real–time traffic information services (OJ L 157, 23.6.2015, p. 21). 2. Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1). Council to check

					Copy definition of operators of recharging points in the text if agreed to add these operators
Annex I. 3					
G	507q	3. Banking	3. Banking	3. Banking	3. Banking Text Origin: Commission Proposal + Annexes
Annex I. 3					
G	507r	— Credit institutions referred to in point (1) of Article 4 of Regulation (EU) No 575/2013 ([1]) _____ 1. Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).	— Credit institutions referred to in point (1) of Article 4 of Regulation (EU) No 575/2013 ([1]) _____ 1. Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).	— Credit institutions referred to in point (1) of Article 4 of Regulation (EU) No 575/2013 ([1]), ***[except those referred to in point (8) of Article 2(5) of Directive 2013/36/EU which are exempted in accordance with Article 2(4) of Regulation XX [DORA]]*** _____ 1. Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).	— Credit institutions referred to in point (1) of Article 4 of Regulation (EU) No 575/2013 ([1]) _____ 1. Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1). green pending final text exclusion clause Text Origin: Commission Proposal + Annexes
Annex I. 4					
G	507s	4. Financial market infrastructures	4. Financial market infrastructures	4. Financial market infrastructures	4. Financial market infrastructures

					Text Origin: Commission Proposal + Annexes	
Annex I. 4						
G	507t	— Operators of trading venues referred to in point (24) of Article 4 of Directive 2014/65/EU (1) — Central counterparties (CCPs) referred to in point (1) of Article 2 of Regulation (EU) No 648/2012 (2) __________ 1. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349). 2. Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).	— Operators of trading venues referred to in point (24) of Article 4 of Directive 2014/65/EU (1) — Central counterparties (CCPs) referred to in point (1) of Article 2 of Regulation (EU) No 648/2012 (2) __________ 1. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349). 2. Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).	— Operators of trading venues referred to in point (24) of Article 4 of Directive 2014/65/EU (1) — Central counterparties (CCPs) referred to in point (1) of Article 2 of Regulation (EU) No 648/2012 (2) __________ 1. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349). 2. Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).	— Operators of trading venues referred to in point (24) of Article 4 of Directive 2014/65/EU (1) — Central counterparties (CCPs) referred to in point (1) of Article 2 of Regulation (EU) No 648/2012 (2) __________ 1. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349). 2. Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1). Text Origin: Commission Proposal + Annexes	G
Annex I. 5						
G	507u	5. Health	5. Health	5. Health	5. Health Text Origin: Commission Proposal + Annexes	G

	Annex I. 5					
G	507v	— Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU (1) — EU reference laboratories referred to in Article 15 of Regulation XXXX/XXXX on serious cross-border threats to health (2) — Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC (3) — Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 — Entities manufacturing medical devices considered as critical during a public health emergency (‘the public health emergency critical devices list’) referred to in Article 20 of Regulation XXXX[4] __________ 1. Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross–border healthcare (OJ L 88, 4.4.2011, p. 45). 2. [Regulation of the European Parliament and of the Council on serious cross-border	— Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU (1) — EU reference laboratories referred to in Article 15 of Regulation XXXX/XXXX on serious cross-border threats to health (2) — Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC (3) — Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 — Entities manufacturing medical devices considered as critical during a public health emergency (‘the public health emergency critical devices list’) referred to in Article 20 of Regulation XXXX[4] __________ 1. Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross–border healthcare (OJ L 88, 4.4.2011, p. 45). 2. [Regulation of the European Parliament and of the Council on serious cross-border	— Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU (1) — EU reference laboratories referred to in Article 15 of Regulation XXXX/XXXX on serious cross-border threats to health (2) — Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC (3) — Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 — Entities manufacturing medical devices considered as critical during a public health emergency (‘the public health emergency critical devices list’) referred to in Article 20 of Regulation XXXX[4] __________ 1. Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross–border healthcare (OJ L 88, 4.4.2011, p. 45). 2. [Regulation of the European Parliament and of the Council on serious cross-border	— Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU (1) — EU reference laboratories referred to in Article 15 of Regulation XXXX/XXXX on serious cross-border threats to health (2) — Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC (3) — Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 — Entities manufacturing medical devices considered as critical during a public health emergency (‘the public health emergency critical devices list’) referred to in Article 20 of Regulation XXXX[4] __________ 1. Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross–border healthcare (OJ L 88, 4.4.2011, p. 45). 2. [Regulation of the European Parliament and of the Council on serious cross-border	G

		threats to health and repealing Decision No 1082/2013/EU, reference to be updated once the proposal COM (2020)727 final is adopted] 3. Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p.67). 4. [Regulation of the European Parliament and of the Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal produces and medical devices, reference to be updated once the proposal COM(2020)725 final is adopted]	threats to health and repealing Decision No 1082/2013/EU, reference to be updated once the proposal COM (2020)727 final is adopted] 3. Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p.67). 4. [Regulation of the European Parliament and of the Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal produces and medical devices, reference to be updated once the proposal COM(2020)725 final is adopted]	threats to health and repealing Decision No 1082/2013/EU, reference to be updated once the proposal COM (2020)727 final is adopted] 3. Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p.67). 4. [Regulation of the European Parliament and of the Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal produces and medical devices, reference to be updated once the proposal COM(2020)725 final is adopted]	threats to health and repealing Decision No 1082/2013/EU, reference to be updated once the proposal COM (2020)727 final is adopted] 3. Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p.67). 4. [Regulation of the European Parliament and of the Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal produces and medical devices, reference to be updated once the proposal COM(2020)725 final is adopted] Text Origin: Commission Proposal + Annexes	
	Annex I. 6.					
G	507w	6. Drinking water	6. Drinking water	6. Drinking water	6. Drinking water Text Origin: Commission Proposal + Annexes	G
	Annex I. 6					
G	507x	Suppliers and distributors of water intended for human consumption referred to in point (1)(a) of Article 2 of Council Directive 98/83/EC([1]) but excluding distributors for whom distribution of water for human consumption is only part of their general activity of	Suppliers and distributors of water intended for human consumption referred to in point (1)(a) of Article 2 of Council Directive 98/83/EC([1]) but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing	Suppliers and distributors of water intended for human consumption referred to in point (1)(a) of Article 2 of Council Directive 98/83/EC([1]) but excluding distributors for whom distribution of water for human consumption is only ***non-essential*** part of their general	Suppliers and distributors of water intended for human consumption referred to in point (1)(a) of Article 2 of Council Directive 98/83/EC([1]) but excluding distributors for whom distribution of water for human consumption is only ***non-essential*** part of their general	G

		distributing other commodities and goods which are not considered essential or important services _____ 1. Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).	other commodities and goods which are not considered essential or important services _____ 1. Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).	activity of distributing other commodities and goods ~~*which are not considered essential or important services*~~ _____ 1. Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).	activity of distributing other commodities and goods ~~*which are not considered essential or important services*~~ _____ 1. Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32). Text Origin: Council Mandate
Annex I. 7.					
G	507y	7. Waste water	7. Waste water	7. Waste water	7. Waste water Text Origin: Commission Proposal + Annexes
Annex I. 7.					
G	507z	Undertakings collecting, disposing or treating urban, domestic and industrial waste water referred to in points (1) to (3) of Article 2 of Council Directive 91/271/EEC ([1]) _____ 1. Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p.40).	Undertakings collecting, disposing or treating urban, domestic and industrial waste water referred to in points (1) to (3) of Article 2 of Council Directive 91/271/EEC ([1]) _____ 1. Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p.40).	Undertakings collecting, disposing or treating urban, domestic and industrial waste water referred to in points (1) to (3) of Article 2 of Council Directive 91/271/EEC ([1]) ***but excluding undertakings for whom collecting, disposing or treating of urban, domestic and industrial waste water is only a non-essential part of their general activity.*** _____ 1. Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water	Undertakings collecting, disposing or treating urban, domestic and industrial waste water referred to in points (1) to (3) of Article 2 of Council Directive 91/271/EEC ([1]) ***but excluding undertakings for whom collecting, disposing or treating of urban, domestic and industrial waste water is only a non-essential part of their general activity.*** _____ 1. Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water

				treatment (OJ L 135, 30.5.1991, p.40).	treatment (OJ L 135, 30.5.1991, p.40). Text Origin: Council Mandate
Annex I. 8					
G	507aa	8. Digital infrastructure	8. Digital infrastructure	8. Digital infrastructure	8. Digital infrastructure Text Origin: Commission Proposal + Annexes
Annex I. 8 indents					
G	507ab	— Internet Exchange Point providers — DNS service providers — TLD name registries — Cloud computing service providers — Data centre service providers — Content delivery network providers — Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014([1]) — Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972([2]) or providers of electronic communications services referred to in point (4) of Article 2 of Directive (EU) 2018/1972 where	— Internet Exchange Point providers — DNS service providers — TLD name registries — Cloud computing service providers — Data centre service providers — Content delivery network providers — Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014([1]) — Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972([2]) or providers of electronic communications services referred to in point (4) of Article 2 of Directive (EU) 2018/1972 where	— Internet Exchange Point providers — DNS service providers, ***excluding operators of root name servers*** — TLD name registries — Cloud computing service providers — Data centre service providers — Content delivery network providers — Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014([1]) — Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972([2]) or providers of electronic communications services referred	— Internet Exchange Point providers — DNS service providers, ***excluding operators of root name servers*** — TLD name registries — Cloud computing service providers — Data centre service providers — Content delivery network providers — Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014([1]) — Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972([2]) or providers of electronic communications services referred

		their services are publicly available _____ 1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p.73). 2. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communication Code (OJ L 321, 17.12.2018, p. 36).	their services are publicly available _____ 1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p.73). 2. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communication Code (OJ L 321, 17.12.2018, p. 36).	to in point (4) of Article 2 of Directive (EU) 2018/1972 where their services are publicly available _____ 1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p.73). 2. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communication Code (OJ L 321, 17.12.2018, p. 36).	to in point (4) of Article 2 of Directive (EU) 2018/1972 where their services are publicly available _____ 1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p.73). 2. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communication Code (OJ L 321, 17.12.2018, p. 36). Text Origin: Council Mandate
Annex I. 8a					
G	507ac			***8.a ICT-service management (B2B)***	***8.a. ICT-service management (B2B)*** Text Origin: Council Mandate
Annex I. 8a					
G	507ad			***— Managed service providers (MSP)*** ***— Managed Security service providers (MSSP)***	***— Managed service providers (MSP)*** ***— Managed Security service providers (MSSP)*** Text Origin: Council Mandate
Annex I. 9					

Y	507ae	9. Public administration	9. Public administration	9. Public administration ***entities***	***9.*** ~~9.~~ Public administration ***entities excluding the judiciary, parliaments and central banks.***	Y
	Annex I. 9 indents					
R	507af	— Public administration entities of central governments — Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003 ([1]) — Public administration entities of NUTS level 2 regions listed in Annex I of Regulation (EC) No 1059/2003 _____ 1. Regulation (EC) No 1059/2003 of the European Parliament and of the Council of 26 May 2003 on the establishment of a common classification of territorial units for statistics (NUTS) (OJ L 154, 21.6.2003, p. 1).	— Public administration entities of central governments — Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003 ([1]) — Public administration entities of NUTS level 2 regions listed in Annex I of Regulation (EC) No 1059/2003 _____ 1. Regulation (EC) No 1059/2003 of the European Parliament and of the Council of 26 May 2003 on the establishment of a common classification of territorial units for statistics (NUTS) (OJ L 154, 21.6.2003, p. 1).	***—*** ~~—~~ Public administration entities of central governments ~~*— Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003 ([1])*~~ ~~*— Public administration entities of NUTS level 2 regions listed in Annex I of Regulation (EC) No 1059/2003*~~ ***as defined by a Member State in accordance with national law*** _____ ~~*1. Regulation (EC) No 1059/2003 of the European Parliament and of the Council of 26 May 2003 on the establishment of a common classification of territorial units for statistics (NUTS) (OJ L 154, 21.6.2003, p. 1).*~~		R
	Annex I. 10					
G	507ag	10. Space	10. Space	10. Space	10. Space Text Origin: Commission Proposal + Annexes	G

Annex I. 10					
G	507ah	Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972	Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972	Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972	Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972 Text Origin: Commission Proposal + Annexes
Annex II.					
G	507ai	IMPORTANT ENITIES:	IMPORTANT ENITIES:	IMPORTANT ENITIES:	~~*IMPORTANT ENITIES:*~~ ***OTHER CRITICAL SECTORS***
Formula					
G	507aj	SECTORS, SUBSECTORS AND TYPES OF ENTITIES	SECTORS, SUBSECTORS AND TYPES OF ENTITIES	SECTORS, SUBSECTORS AND TYPES OF ENTITIES	SECTORS, SUBSECTORS AND TYPES OF ENTITIES Text Origin: Commission Proposal + Annexes
Formula					
G	507ak	Sector	Sector	Sector	Sector

					Text Origin: Commission Proposal + Annexes
Formula					
G	507al	Subsector	Subsector	Subsector	Subsector Text Origin: Commission Proposal + Annexes
Formula					
G	507am	Type of entity	Type of entity	Type of entity	Type of entity Text Origin: Commission Proposal + Annexes
Annex II. 1					
G	507an	1. Postal and courier services	1. Postal and courier services	1. Postal and courier services	1. Postal and courier services Text Origin: Commission Proposal + Annexes
Annex II.1					
G	507ao	Postal service providers referred to in point (1) of Article 2 of Directive 97/67/EC ([1])and providers of courier services _____ 1. Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the	Postal service providers referred to in point (1) of Article 2 of Directive 97/67/EC ([1])and providers of courier services _____ 1. Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the	~~*Postal service providers referred to in*~~ point (1) of Article 2 of Directive 97/67/EC ([1])~~*and*~~ ***including*** providers of courier services _____ 1. Directive 97/67/EC of the European	Postal service providers referred to in point (1) of Article 2 of Directive 97/67/EC ([1])~~*and*~~ ***including*** providers of courier services _____ 1. Directive 97/67/EC of the European

		development of the internal market of Community postal services and the improvement of the quality of service (OJ L 15, 21.1.98, p.14).	development of the internal market of Community postal services and the improvement of the quality of service (OJ L 15, 21.1.98, p.14).	Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of the quality of service (OJ L 15, 21.1.98, p.14)***, as amended by Directive 2008/6/EC of the European Parliament and of the Council of 20 February 2008 amending Directive 97/67/EC with regard to the full accomplishment of the internal market of Community postal services (OJ L 52, 27.2.2008, p. 3)***.	Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of the quality of service (OJ L 15, 21.1.98, p.14).	
	Annex II. 2					
G	507ap	2. Waste management	2. Waste management	2. Waste management	2. Waste management `Text Origin: Commission Proposal + Annexes`	G
	Annex II. 2					
G	507aq	Undertakings carrying out waste management referred to in point (9) of Article 3 of Directive 2008/98/EC (1) but excluding undertakings for whom waste management is not their principal economic activity __________ 1. Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3)	Undertakings carrying out waste management referred to in point (9) of Article 3 of Directive 2008/98/EC (1) but excluding undertakings for whom waste management is not their principal economic activity __________ 1. Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3)	Undertakings carrying out waste management referred to in point (9) of Article 3 of Directive 2008/98/EC (1) but excluding undertakings for whom waste management is not their principal economic activity __________ 1. Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3)	Undertakings carrying out waste management referred to in point (9) of Article 3 of Directive 2008/98/EC (1) but excluding undertakings for whom waste management is not their principal economic activity __________ 1. Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3)	G

					Text Origin: Commission Proposal + Annexes
Annex II. 3					
G	507ar	3. Manufacture, production and distribution of chemicals	3. Manufacture, production and distribution of chemicals	3. Manufacture, production and distribution of chemicals	3. Manufacture, production and distribution of chemicals Text Origin: Commission Proposal + Annexes
Annex II. 3					
G	507as	Undertakings carrying out the manufacture, production and distribution of substances and articles referred to in points (4), (9) and (14) of Article 3 of Regulation (EC) No 1907/2006 ([1]) _____ 1. Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning registration, evaluation, authorisation and restriction of chemicals (REACH), establishing a European Chemicals Agency amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155.EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1).	Undertakings carrying out the manufacture, production and distribution of substances and articles referred to in points (4), (9) and (14) of Article 3 of Regulation (EC) No 1907/2006 ([1]) _____ 1. Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning registration, evaluation, authorisation and restriction of chemicals (REACH), establishing a European Chemicals Agency amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155.EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1).	Undertakings carrying out the manufacture~~, *production*~~ and distribution of substances and ~~*articles*~~***mixtures*** referred to in points ~~*(4)*~~***()***, (9) and (14) of Article 3 of Regulation (EC) No 1907/2006 ([1]) ***and undertakings carrying out the production of articles referred to in point (3) of Article 3 of that Regulation from substances or mixtures.*** _____ 1. Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning registration, evaluation, authorisation and restriction of chemicals (REACH), establishing a European Chemicals Agency amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155.EEC,	Undertakings carrying out the manufacture~~, *production*~~ and distribution of substances and ~~*articles*~~***mixtures*** referred to in points ~~*(4),*~~ (9) and (14) of Article 3 of Regulation (EC) No 1907/2006 ([1]) ***and undertakings carrying out the production of articles referred to in point (3) of Article 3 of that Regulation from substances or mixtures.*** _____ 1. Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning registration, evaluation, authorisation and restriction of chemicals (REACH), establishing a European Chemicals Agency amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155.EEC,

				93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1).	93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1). Text Origin: Council Mandate
Annex II. 4					
G	507at	4. Food production, processing and distribution	4. Food production, processing and distribution	4. Food production, processing and distribution	4. Food production, processing and distribution Text Origin: Commission Proposal + Annexes
Annex II 4					
Y	507au	Food businesses referred to in point (2) of Article 3 of Regulation (EC) No 178/2002 ([1]) _____ 1. Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p.1).	Food businesses referred to in point (2) of Article 3 of Regulation (EC) No 178/2002 ([1]) _____ 1. Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p.1).	Food businesses referred to in point (2) of Article 3 of Regulation (EC) No 178/2002 ([1]) ***which are engaged in wholesale distribution and industrial production and processing*** _____ 1. Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p.1).	Food businesses referred to in point (2) of Article 3 of Regulation (EC) No 178/2002 ([1]) ***which are engaged in wholesale distribution and industrial production and processing*** _____ 1. Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p.1). Check against CER Text Origin: Council Mandate
Annex II. 5					

G	507av	5. Manufacturing	5. Manufacturing	5. Manufacturing	5. Manufacturing Text Origin: Commission Proposal + Annexes	G
	Annex II. 5(a)					
G	507aw	(a) Manufacture of medical devices and in vitro diagnostic medical devices Entities manufacturing medical devices referred to in Article 2 point 1 of Regulation (EU) 2017/745(1), and entities manufacturing in vitro diagnostic medical devices referred to in Article 2 point 2 of Regulation (EU) 2017/746 (2) with exception of entities manufacturing medical devices mentioned in Annex 1, point 5. ___ 1. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p.1) 2. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU	(a) Manufacture of medical devices and in vitro diagnostic medical devices Entities manufacturing medical devices referred to in Article 2 point 1 of Regulation (EU) 2017/745(1), and entities manufacturing in vitro diagnostic medical devices referred to in Article 2 point 2 of Regulation (EU) 2017/746 (2) with exception of entities manufacturing medical devices mentioned in Annex 1, point 5. ___ 1. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p.1) 2. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU	(a) Manufacture of medical devices and in vitro diagnostic medical devices Entities manufacturing medical devices referred to in Article 2 point 1 of Regulation (EU) 2017/745(1), and entities manufacturing in vitro diagnostic medical devices referred to in Article 2 point 2 of Regulation (EU) 2017/746 (2) with exception of entities manufacturing medical devices mentioned in Annex 1, point 5. ___ 1. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p.1) 2. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU	(a) Manufacture of medical devices and in vitro diagnostic medical devices Entities manufacturing medical devices referred to in Article 2 point 1 of Regulation (EU) 2017/745(1), and entities manufacturing in vitro diagnostic medical devices referred to in Article 2 point 2 of Regulation (EU) 2017/746 (2) with exception of entities manufacturing medical devices mentioned in Annex 1, point 5. ___ 1. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p.1) 2. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU	G

		(OJ L 117, 5.5.2017, p.176)	(OJ L 117, 5.5.2017, p.176)	(OJ L 117, 5.5.2017, p.176)	(OJ L 117, 5.5.2017, p.176) Text Origin: Commission Proposal + Annexes
Annex II. 5(b)					
G	507ax	(b) Manufacture of computer, electronic and optical products Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2	(b) Manufacture of computer, electronic and optical products Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2	(b) Manufacture of computer, electronic and optical products Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2	(b) Manufacture of computer, electronic and optical products Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2 Text Origin: Commission Proposal + Annexes
Annex II. 5(c)					
G	507ay	(c) Manufacture of electrical equipment Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2	(c) Manufacture of electrical equipment Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2	(c) Manufacture of electrical equipment Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2	(c) Manufacture of electrical equipment Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2 Text Origin: Commission Proposal + Annexes
Annex II. 5(d)					
G	507az	(d) Manufacture of machinery and	(d) Manufacture of machinery and	(d) Manufacture of machinery and	(d) Manufacture of machinery and

		equipment n.e.c. Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2	equipment n.e.c. Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2	equipment n.e.c. Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2	equipment n.e.c. Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2 Text Origin: Commission Proposal + Annexes
Annex II. 5(e)					
G	507ba	(e) Manufacture of motor vehicles, trailers and semi-trailers Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2	(e) Manufacture of motor vehicles, trailers and semi-trailers Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2	(e) Manufacture of motor vehicles, trailers and semi-trailers Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2	(e) Manufacture of motor vehicles, trailers and semi-trailers Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2 Text Origin: Commission Proposal + Annexes
Annex II. 5(f)					
G	507bb	(f) Manufacture of other transport equipment Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2	(f) Manufacture of other transport equipment Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2	(f) Manufacture of other transport equipment Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2	(f) Manufacture of other transport equipment Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2 Text Origin: Commission

					Proposal + Annexes
Annex II. 6					
G	507bc	6. Digital providers	6. Digital providers	6. Digital providers	6. Digital providers Text Origin: Commission Proposal + Annexes
Annex II. 6					
G	507bd	— Providers of online marketplaces — Providers of online search engines — Providers of social networking services platform	— Providers of online marketplaces — Providers of online search engines — Providers of social networking services platform	— Providers of online marketplaces — Providers of online search engines — Providers of social networking services platform	— Providers of online marketplaces — Providers of online search engines — Providers of social networking services platform Text Origin: Commission Proposal + Annexes
Annex II. 6(a)					
G	507be		***6a. Education and research***		***6a. Research***
Annex II. 6(a)					
G	507bf		***— Higher education institutions and research institutions***		***-Research organisation as defined in Article 4 : [for the purpose of this directive],***