Draft compromises - LIBE opinion on the NIS2 Directive

Rapporteur: Lukas MANDL

Chapters III - VII

RECITALS 27-84

CA28	Covers AMs 14 (rapp), 15 (rapp), 16 (rapp), 17 (rapp), 18 (rapp), 19 (rapp), 20 (rapp), 21 (rapp), 22 (rapp), 23 (rapp), 24 (rapp), 25 (rapp), 26 (rapp), 27 (rapp), ~~28 (rapp),~~ 102 (S&D), 103 (S&D), 104 (RE), 105 (RE), 107 (S&D), 110 (Left), 112 (ECR), 114part (Greens), 115 (Greens), 116 (Left), 117 (RE), 118 (Greens), 119 (S&D), 120part (S&D), 124 (RE), 132 (S&D), 135 (S&D), 136 (Left) Fall: AMs 28 (rapp), 106 (ECR), 109 (ECR), 111 (ECR), 113 (ECR), 121 (S&D), 122 (ECR), 123 (ECR), 125 (Greens), 126 (Greens), 127 (Greens), 128 (Greens), 129 (ECR), 130 (Greens), 131 (Greens), 133 (ECR)~~,~~ (27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20] , 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 risks 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, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union. ***Member States should monitor the way in which EU rules are implemented, support each other in the event of any cross-border problems, establish a more structured dialogue with the private sector and cooperate on security risks and the threats associated with new technologies, as was the case with 5G technology. (AM 14, 102, 103)*** (28) - (32) *[...] COM proposal* (33) When developing guidance documents, the Cooperation Group should consistently: map national ***and sectoral*** solutions and experiences, assess the impact of Cooperation Group deliverables on national ***and sectoral*** approaches, discuss implementation challenges and formulate specific recommendations to be addressed through better implementation of existing rules. (AM 15) (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 ***invite relevant*** Union bodies and agencies involved in cybersecurity policy, ***notably Europol***, the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work. (AM 16) (35) *[...] COM proposal*

	(36) The Union should, 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 and the CSIRTs network. ***To the extent that personal data is transferred to a third country or international organisation, Chapter V of Regulation (EU) 2016/679*** should ***apply***. (AM 17, 104) (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 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 ***concerns two or more Member States and is suspected to be of criminal nature, the activation of the EU Law Enforcement Emergency Response Protocol should be considered. 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. (38)-(44) *[...] COM proposal* (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 ***and report any cyber attacks that they identify***. (AM 107) (46) *[...] COM proposal* (AM 109 falls). (46a) ***Particular consideration should be given to the fact that ICT services, systems or products subject to specific requirements in the country of origin that might represent an obstacle to compliance with EU privacy and data protection law. Where appropriate, the EDPB should be consulted in the framework of such risk assessments. Free and open source software as well as open source hardware could bring huge benefits in terms of cybersecurity, in particular as regards transparency and verifiability of features. As this could help address and mitigate specific supply chain risks, their use should be preferred where feasible in line with Opinion 5/2021 of the EDPS[1]. (AMs 108, 110, 114)***

[1] ***Opinion 5/2021 of the European Data Protection Supervisor on the Cybersecurity Strategy and the NIS 2.0 Directive, 11 March 2021***

	(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 ***that should be further specified by the Coordination Group, and which include*** 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. (AM 18) (48) *[...] COM proposal* ***(48a) Small and medium-sized enterprises (SMEs) often lack the scale and resources to fulfil a broad and growing range of cybersecurity needs in an interconnected world with an increase of remote work. Member States should therefore address in their national cybersecurity strategies guidance and support for SMEs. (AM 112)*** (49) *[...] COM proposal* (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 ***cyber***security 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. (AM 19) (51) *[...] COM proposal* (AM 113 falls) (52) Where appropriate, entities should ***be enabled to*** 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 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. (AM 20) (53) In particular, providers of public electronic communications networks or publicly available electronic communications services, should ***implement security by design and by default and be enabled to*** 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 software or encryption technologies. ***To increase the security of hardware and***

	software, providers should be encouraged to use open source and open hardware. (AM 21) (54) In order to safeguard the security of electronic communications networks and services ***as well as the fundamental rights to data protection and privacy***, 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' ***responsibility*** to ensure the protection of their essential security interests and public security, and to permit the ***prevention***, detection and prosecution of criminal offences in compliance with Union ***and national*** 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. ***Nothing in this Regulation should be viewed as an effort to weaken*** end-to-end encryption ***through "backdoors" or similar*** solutions, ***as encryption shortfalls may be exploited for malicious purposes***. ***Any measure aimed at weakening encryption or circumventing the technology's architecture may incur significant risks to the effective protection capabilities it entails. Any unauthorised decryption, ~~reverse engineering of encryption codes~~ or monitoring of electronic communications other than by legal authorities should be prohibited to ensure the effectiveness of the technology and its wider use. It is important/essential that Member States address problems encountered by legal authorities and vulnerability researchers. In some Member States entities and natural persons researching vulnerabilities are exposed to criminal and civil liability; Member States are therefore encouraged to issue guidelines for non-prosecution and non-liability of information security research.*** (AM 22, 116, 117, 118, 119, 120part) (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 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. (AM 23) (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 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 ***and the European Data Protection Board,*** 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. (AM 24)

(57) Where it is suspected that an incident is related to serious criminal activities under Union or national law, essential and important entities, on the basis of applicable criminal proceedings rules in compliance with Union law, ***should*** 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 ***European Cybercrime Centre (EC3) of Europol*** and ENISA. (AM 25, 124)

(58) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities should cooperate and exchange information on all relevant matters with data protection authorities and the supervisory authorities pursuant to ***Regulation (EU) 2016/679 and*** Directive 2002/58/EC. (AM 26)

(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 ***applicable*** Union data protection law. (AM 27)

(60) *[...] COM proposal.* (AM 28 falls)

~~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. (AM 28)~~

(61) *[...] COM proposal.* (AM 127 falls)

(62) ***To comply with a legal obligation in terms of Article 6(1)(c) and Article 6(3) of Regulation (EU) 2016/679,*** TLD registries and the entities providing domain name registration services for them should make ***publicly*** available ***certain*** domain name registration data ***specified in the Member State law to which they are subject***, such as ***the domain name and the name of the*** legal ***person***. 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, ***notably to competent authorities under this Directive***

	or supervisory authorities under Regulation (EU) 2016/679 in accordance with ***their powers***. Member States should ensure that TLD registries and the entities providing domain name registration services for them should respond without undue delay to ***lawful and duly justified*** requests from ***public authorities, including competent authorities under this Directive, competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences***, ***or supervisory authorities under Regulation (EU) 2016/679***, 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. (AM 29) (63) ***Fur the purposes of this Directive,*** 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 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 ***agree on constituent classifications,*** cooperate ***wherever possible***, provide ***real time*** mutual assistance to each other and where appropriate, carry out joint supervisory actions. (AM 30) (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 providers and digital providers, only one Member State should have jurisdiction over these entities. ***For the purposes of this Directive,*** 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 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. (AM 31) (65) *[...] COM proposal* (AM 130 falls) (66) *[...] COM proposal* (67) *[...] COM proposal*

	(68) *[...] COM proposal* (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, CSIRTs, and providers of security technologies and services ***is necessary for compliance with their legal obligations under national law transposing this Directive, and is therefore covered by Articles 6(1)(c) and 6(3) of Regulation (EU) 2016/679. Moreover, such processing*** should constitute a legitimate interest of the data controller concerned, as referred to in ***Article 6(1)(f) of*** 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. ***In many cases, personal data are compromised following cyber incidents and, therefore, the competent authorities and data protection authorities of EU Member States should cooperate and exchange information on all relevant matters in order to tackle any personal data breaches.*** Such measures may require the processing of ***certain categories*** of personal data***, including*** IP addresses, uniform resources locators (URLs), domain names, and email addresses. (AM 32, 132) (70) *[...] COM proposal* (AM 133 falls) (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 ***seriousness*** and duration of the infringement, the actual damage caused or losses incurred or potential damage or losses that could have been triggered***, any relevant previous infringements, the manner in which the infringement became known to the competent authority***, 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 penalties ***imposed,*** 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. (72) *[...] COM proposal.* (73) *[...] COM proposal.* (74) Member States should be able to lay down the rules on criminal penalties for infringements of the national rules transposing this Directive***. *Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation***. 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. (AM 34) (75) *[...] COM proposal*

	(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. Given their ***seriousness*** 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 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 ***remedies***, due process, presumption of innocence and right of defence. (AM 35) (77) This Directive should establish cooperation rules between the competent authorities ***under this Directive*** and the supervisory ***under*** Regulation (EU) 2016/679 to deal with infringements related to personal data. (AM 36) (78)This Directive should aim at ensuring a high level of responsibility for the cybersecurity 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. (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. ***The EU should facilitate a coordinated response to large-scale cyber incidents and crises and offer assistance in order to aid recovery following such cyber attacks. (AM 135)*** (80) *[...] COM proposal* (81) *[...] COM proposal* (82) *[...] COM proposal* ***(82a) This Directive does not apply to Union institutions, offices, bodies and agencies. However, Union bodies could be considered essential or important entities under this Directive. To achieve a uniform level of protection through consistent and homogeneous rules, the Commission should publish a legislative proposal to include Union institutions, offices, bodies and agencies in the EU-wide cybersecurity framework by 31 December 2022. (AM 136)*** (83) *[...] COM proposal* (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, principles, ***and in***

	full compliance with existing Union legislation regulating these issues. Any processing of personal data under this Directive is subject to Regulation (EU) 2016/679 and Directive 2002/58/EC, in their respective scope of application, including the tasks and powers of the supervisory authorities competent to monitor compliance with those legal instruments. (AM 37)

CHAPTER III - Cooperation

CA8	**ARTICLE 12 - Cooperation Group** Covers AMs 48 (rapp), 49 (rapp), 190 (RE), 191 (RE), 192 (Left) Fall: AMs 189 (Left), 193 (Left) 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. 2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 6. 3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service, ***the European Cybercrime Centre at Europol and the European Data Protection Board*** 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. Where ***relevant for the performance of its tasks*** ~~***appropriate***~~, the Cooperation Group ***shall*** ~~***may***~~ invite representatives of relevant stakeholders~~, *including academia and civil society,*~~ to participate in its work ***and the European Parliament to participate as observer***. The Commission shall provide the secretariat. (AM 48, 190, 191, 192) 4. The Cooperation Group shall have the following tasks: (a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive; (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; (c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives; (d) exchanging advice and cooperating with the Commission on draft Commission implementing or delegated acts adopted pursuant to this Directive; (e) exchanging best practices and information with relevant Union institutions, bodies, offices and agencies; (f) discussing reports on the peer review referred to in Article 16(7); (g) discussing results from joint-supervisory activities in cross-border cases as referred to in Article 34; (h) providing strategic guidance to the CSIRTs network on specific emerging issues;

	(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; (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; (k) discussing the work undertaken in relation to cybersecurity exercises, including the work done by ENISA. 5. The Cooperation Group may request from the CSIRT network a technical report on selected topics. 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. 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). 8. The Cooperation Group shall meet regularly and at least ***twice*** a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to ***facilitate*** strategic cooperation and ***real time*** information ***exchange***. (AM 49)

CA9	**Article 13 - CSIRT network** Covers AM 194 (RE) 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. 2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT–EU. The Commission ***and the European Cybercrime Centre at Europol*** shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support cooperation among the CSIRTs. (AM 194) 3. The CSIRTs network shall have the following tasks: (a) exchanging information on CSIRTs' capabilities; (b) exchanging relevant information on incidents, near misses, 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; (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;

	(e) providing Member States with support in addressing cross–border incidents pursuant to this Directive; (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; (g) discussing and identifying further forms of operational cooperation, including in relation to: (i) categories of cyber threats and incidents; (ii) early warnings; (iii) mutual assistance; (iv) principles and modalities for coordination in response to cross–border risks and incidents; (v) contribution to the national cybersecurity incident and crisis response plan referred to in Article 7 (3); (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; (i) taking stock from cybersecurity exercises, including from those organised by ENISA; (j) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT; (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; (l) discussing the peer-review reports referred to in Article 16(7); (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. 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. 5. The CSIRTs network shall adopt its own rules of procedure.

CA10	**ARTICLE 14 - The European cyber crises liaison organisation network (EU - CyCLONe)** Covers AM 195 (RE), 197 (RE) Falls: AM 196 (ECR) 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. 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. ***The European Cybercrime Centre at Europol shall participate in the activities of EU-CyCLONe as an observer.*** ENISA shall provide the secretariat of the network and support the secure exchange of information. (AM 195) 3. EU-CyCLONe shall have the following tasks: (a) increasing the level of preparedness of the management of large scale incidents and crises; (b) developing a shared situational awareness of relevant cybersecurity events; (c) coordinating large scale incidents and crisis management and supporting decision-making at political level in relation to such incidents and crisis; (d) discussing national cybersecurity incident and response plans referred to in Article 7(2). 4. EU-CyCLONe shall adopt its rules of procedure. 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. 6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements***, and with law enforcement in the framework of the EU Law Enforcement Emergency Response Protocol***. (AM 197)

CA11	**ARTICLE 15 - Report on the state of cybersecurity in the Union** Covers: AMs 50 (rapp), 51 (rapp), 198 (Greens), 199 (ID), 200 (Greens) Fall: AMs 1. ENISA shall issue, in cooperation with the Commission, ***an annual*** report on the state of cybersecurity in the Union. The report shall ***be delivered in machine-readable format and*** in particular include an assessment of the following: (AMs 50, 198, 199) (a) the development of cybersecurity capabilities across the Union; (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; (c) a cybersecurity index providing for an aggregated assessment of the maturity level of cybersecurity capabilities ***(ca) the impact of cybersecurity incidents on the protection of personal data in the Union***. (AM 51) ***(ca) an overview of the general level of cybersecurity awareness and use of cybersecurity measures amongst citizens as well as on the general level of security of consumer-oriented connected devices put on the market in the Union. (AM 200)***

	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 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 16 - Peer reviews (no AMs tabled = COM text)

CHAPTER IV - Cybersecurity risk management and reporting obligations

SECTION I - Cybersecurity risk management and reporting

CA12	**ARTICLE 17 - Governance** Covers AMs 52 (rapp), 202 (RE) Fall: AM 201 (ECR) 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 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. 2. Member States shall ensure that members of the management body ***and responsible specialists for cybersecurity*** follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess ***evolving*** cybersecurity risks and management practices and their impact on the operations of the entity. (AM 52, 20)

CA13	**ARTICLE 18 - Cybersecurity risk management measures** Covers AMs 53 (rapp), 54 (rapp), 203 (RE), 205 (Greens), 206 (ID), 207 (Greens) Fall: AM 204 (ECR) 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 ***cybersecurity*** of network and information systems ***used for*** the provision of their ***services, and in view of assuring the continuity of these*** services, ***and to mitigate the risks posed to the rights of individuals when their personal data are processed***. Having regard to the state of the art, those measures shall ensure a level of ***cybersecurity*** of network and information systems appropriate to the risk presented. (AM 53, 203) 2.The measures referred to in paragraph 1 shall include at least the following: (a) risk analysis and information system security policies; (b) incident handling (prevention, detection, and response to incidents); (c) business continuity and crisis management;

	(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; (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure; (f) policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures; (g) the use of cryptography and ***strong*** encryption. (AM 205) 3. Member States shall ensure that, where considering appropriate ***and proportionate*** 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. ***Competent authorities shall provide guidance to entities on the practical and proportionate application. (AM 54, 206)*** 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. 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. 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. ***6a. Member States shall give the user of a network and information system provided by an essential or important entity the right to obtain from the entity information on the technical and organisational measures in place to mitigate the risks posed to the security of network and information systems. Member States shall define the limitations to that right. (AM 207)***

CA14	**ARTICLE 19 - EU coordinated risk assessments of critical supply chains** Covers AM 208 (Greens) Fall: AM 209 (RE), 210 (Greens) 1. The Cooperation Group, in cooperation with the Commission and ENISA, ***shall*** 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. (AM 208) 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. (AM 210)

CA15	**ARTICLE 20 - Reporting obligations**

	Covers AMs 55 (rapp), 56 (rapp), 57 (rapp), 58 (rapp), 59 (rapp), 211 (Greens), 212 (RE), 213 (ECR), 217 (RE) Fall: AM 214 (ID), 215 (ECR), 216 (Greens), 218 (Greens) 1. Member States shall ensure that essential and important entities notify, without undue delay ***and in any event within 24 hours,*** 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***, and the competent law enforcement authorities if the incident is of a suspected or known malicious nature***. ***T***hose entities shall notify, without undue delay, ***and in any event within 24 hours***, the recipients of their services of incidents that are likely to adversely affect the provision of that service ***and provide information that would enable them to mitigate the adverse effects of the cyberattacks. By way of exception, where public disclosure could trigger further cyberattacks, those ~~essential and important~~ entities may delay the notification***. 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. (AMs 211, 212, 213) 2. Member States shall ***ensure*** that essential and important entities ***are able to*** notify the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident. (AM 55) Where applicable, those entities ***shall be allowed to*** notify 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 ***such notification is provided,*** the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability. (AM 56) 3. An incident shall be considered significant if: (a) the incident has caused or has the potential to cause substantial operational disruption or financial losses for the entity concerned; (b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses. 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: (a) without undue delay and in any event within ***24*** hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action; (b) upon the request of a competent authority or a CSIRT, an intermediate report on relevant status updates; (c) a ***comprehensive*** report not later than one month after the submission of the report under point (a), including at least the following: (AM 58) (i) a detailed description of the incident, its severity and impact; (ii) the type of ***cyber*** threat or root cause that likely triggered the incident; (AM 59) (iii) applied and ongoing mitigation measures ***or remedies***. (AM 60) 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).

	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. 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. ***If the incident concerns two or more Member States and is suspected to be of criminal nature, the competent authority or the CSIRT shall inform EUROPOL***. 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. (AM 217) 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. 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. 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. 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]. 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 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 21 - Use of European cybersecurity certification schemes

No compromise - AM 220 (ECR) as a consequential AM should fall

CA16	**ARTICLE 22 - Standardisation** Covers AMs 221 (Greens), 222 (RE) 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. 2. ENISA, ***after having consulted the EDPB and*** 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. (AMs 221, 222)

CA17	**ARTICLE 23 - Databases of domain names and registration data** Covers AMs 62 (rapp), 63 (rapp), 64 (rapp), 65 (rapp), 224 (Left), 225 (Left), 226 (Left), 227 (RE) Fall: AMs 223 (Greens) 1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD ***have policies and procedures in place to ensure that*** accurate and complete domain name registration data ***is collected and maintained*** in a dedicated database facility ***in accordance with*** to Union data protection law as regards data which are personal data. ***Member States shall ensure that such policies and procedures are made publicly available. (AM 62, 224)*** 2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain ***the*** information ***necessary*** to identify and contact the holders of the domain names***, namely their name, their physical and e-mail address as well as their telephone number,*** and the points of contact administering the domain names under the TLDs. (AMs 63, 225) ~~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 information. Member States shall ensure that such policies and procedures are made publicly available~~. (AM 64) 4. Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD publish, ***in accordance with Article 6(1)(c) and Article 6(3) of Regulation (EU) 2016/679 and*** without undue delay after the registration of a domain name, ***certain*** domain ***name*** registration data***, such as the domain name and the name of the legal person.*** (AM 65) 5. Member States shall ensure that 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 ***public authorities, including competent authorities under this Directive, competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, or supervisory authorities under Regulation (EU) 2016/679***, 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 ***lawful and duly justified*** requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available. (AM 66, 226, 227)

Section II - Jurisdiction and Registration

CA18	**ARTICLE 24 - Jurisdiction and territoriality** Covers AM 67 (rapp) Fall: AMs 228 (Greens) 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 of the Member State in which they have their main establishment in the Union. 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 number of employees in the Union. 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. ***Without prejudice to the competences of the supervisory authorities under Regulation (EU) 2016/679,*** 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-compliance with the obligations under this Directive. (AM 67) 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.

CA19	**ARTICLE 25 - Registry for essential and important entities** Covers AM 229 (Greens) 1. ENISA shall create and maintain a ***secure*** 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]: (AM 229) (a) the name of the entity; (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);

	(c) up-to-date contact details, including email addresses and telephone numbers of the entities. 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. 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. 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.

CHAPTER V - Information sharing

CA20	**ARTICLE 26 - Cybersecurity information-sharing arrangements** Covers AMs 68 (rapp), 230 (ID) Fall: AMs 231 (ECR), 232 (ECR), 233 (ECR) 1. Without prejudice to Regulation (EU) 2016/679 ***or Directive 2002/58/EC***, 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 ***and the location or identity of the attacker***, where such information sharing: (AM 68, 230) (a) aims at preventing, detecting, responding to or mitigating incidents; (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. 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. 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 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). 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. 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.

ARTICLE 27 - Voluntary notification of relevant information No compromise proposal as no AMs tabled

CHAPTER VI - Supervision and enforcement

CA21	**ARTICLE 28 - General aspects concerning supervision and enforcement** Covers AMs 69 (rapp), 234 (Greens) 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 Articles 18 and 20. 2. Competent authorities shall work in close cooperation with ***supervisory*** authorities when addressing incidents resulting in personal data breaches ***without prejudice to the competences, tasks and powers of supervisory authorities pursuant to Regulation (EU) 2016/679. To this end, competent authorities and supervisory authorities shall exchange information relevant for their respective area of competence. Moreover, competent authorities shall, upon request of the competent supervisory authorities, provide them with all information obtained in the context of any audits and investigations that relate to the processing of personal data. (AM 69, 234)***

CA22	**ARTICLE 29 - Supervision and enforcement for essential entities** Covers AMs 70 (rapp), 71 (rapp), 72 (rapp), 73 (rapp), 74 (rapp), 75 (rapp), 76 (rapp), 77 (rapp), 78 (rapp) 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. 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: (a) on-site inspections and off-site supervision, including random checks; (b) regular audits; (c) targeted security audits based on risk assessments or risk-related available information; (d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria; (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);

	(f) requests to access data, documents or any information necessary for the performance of their supervisory tasks; (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. 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. 4. Member States shall ensure that competent authorities, where exercising their enforcement powers in relation to essential entities, have the power to: (a) issue warnings on the entities' non-compliance with 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; (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; (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; (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; (f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline; (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; ~~(h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner~~; (AM 70) (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 nature of that infringement; (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. 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 power to:

	(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; ~~(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.~~ (AM 71) ***This sanction*** 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. (AM 72) 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 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. 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: (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. (b) the duration of the infringement, including the element of repeated infringements; (c) the actual ***material or non-material*** 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; (AM 73) ***(ca) any relevant previous infringements by the entity concerned;*** (AM 74) ***(cb) the manner in which the infringement became known to the competent authority, in particular whether, and if so to what extent, the entity notified the infringement;*** (AM 75) (d) the intentional or negligent character of the infringement; (e) measures taken by the entity to prevent or mitigate the damage and/or losses; (f) adherence to approved codes of conduct or approved certification mechanisms; (g) the level of cooperation with the competent authorities ***in order to remedy the infringement and mitigate possible adverse effects of the infringements;*** (AM 76)

	(ga) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained or losses avoided, directly or indirectly, from the infringement. (AM 77) 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. 9. Member States shall ensure that their competent authorities inform ***in real time*** the relevant competent authorities of ***all*** 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 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. (AM 78)

CA23	**ARTICLE 30 - Supervision and enforcement for important entities** Covers AMs 79 (rapp), 80 (rapp) Falls: AM 235 (ECR) 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 supervisory measures. 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: (a) on-site inspections and off-site ex post supervision; (b) targeted security audits based on risk assessments or risk-related available information; (c) security scans based on objective, fair and transparent risk assessment criteria; (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); (e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks. 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. 4. Member States shall ensure that the competent authorities, where exercising their enforcement powers in relation to important entities, have the power to: (a) issue warnings on the entities' non-compliance with 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; (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; (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; (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; (f) order those entities to implement the recommendations provided as a result of a security audit within a reasonable deadline; ~~(g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner~~; (AM 79) (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; (AM 80) (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. 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.

CA24	**ARTICLE 31- General conditions for imposing administrative fines on essential and important entities** Covers AMs 81(rapp), 82 (rapp) Fall: AMs 237 (ECR), 238 (ECR) 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. 2. Administrative fines shall 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)***, depending on the circumstances of each individual case***. (AM 81) 3. Deciding whether to impose an administrative fine ***shall depend on the circumstances of each individual case, and when*** deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article 29(7). (AM 82) 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. 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. 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.

CA25	**ARTICLE 32 - Infringements entailing a personal data breach** Covers AMs 84 (rapp), 240 (RE), 241 (Greens), 242 (Greens) Fall: AMs 239 (ECR) 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 ***without undue delay, and in any case within 24 hours***. (AM 84, 240, 241) 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. 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 ***shall*** inform the supervisory authority established in the same Member State. (AM 242)

ARTICLE 33 - Penalties **ARTICLE 34 - Mutual assistance** No compromise as no AMs were tabled

CHAPTER VII - Transitional and final provisions

CA26	**ARTICLE 35 - Review** Covers AMs 244 (RE), 245 (Greens) The Commission shall review the functioning of this Directive ***every 3 years***, and report to the European Parliament and to the Council. The report shall in particular assess ***to what extent the Directive has contributed to ensuring a high common***

	level of security and integrity of network and information systems, while giving an optimal protection to private life and personal data, and 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… ***[36*** months after the date of entry into force of this Directive***]***. (AM 244, 245)

ARTICLE 36-40
No compromises as no AMs were tabled

AMs 243, 246 and 247 (Greens) concerning articles 34a, 40 and 40a respectively should be voted separately.