Non-paper by BE, DE, HU, IT, MT, NL, PL and SE

on the inclusion of public administration in the NIS2 directive framework

I. State of play

The NIS2[1] proposal includes public administration as one of the sectors included in the Annex I to the proposal. The following types of entities from the public administration sector are to be included in the NIS2 scope:

1) Public administration entities of central governments
2) Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003[2]
3) Public administration entities of NUTS level 2 regions listed in Annex I of Regulation (EC) No 1059/2003

Art. 4 point 23 of the NIS2 defines 'public administration entity' as an entity in a Member State that complies with the following criteria:

(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

(b) it has legal personality;

(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 are appointed by the State, regional authorities, or by other bodies governed by public law;

(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.

Public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded from the scope of this definition.

In addition art. 2 para. 2 (b) of the NIS2 foresees that the public administration entities as defined above, will fall under the scope of the NIS2 regardless of their size.

Therefore, all public administration entities of a type referred to in Annex I, fulfilling the criteria described in the definition will be covered by the NIS2 provisions.

[1] 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, doc. COM(2020) 823 final – so-called "NIS-Directive 2.0" or "NIS2" for short.

[2] 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)

II. Position

It is crucial to raise the cyber awarness and resilience in the public administration entities. However, we believe that the proposed approach on how to include the public administration entities in the NIS2 scope does not take into account the specificities of the composition of national public administrations.

We see the following arguments for a change in the Commission's approach to public administration entities:

1) The public administration sector is far more differential than other sectors in the NIS2 due to specific national solutions when it comes to the organisation, structures and degree of decentralization.
2) The NUTS classification is not suitable for the purposes of defining the NIS2 scope. The NUTS classification was designed only for statistical purposes. In particular, implementation of European funds, which have different aims than those foreseen to be accomplished by the NIS2 framework, namely high common level of cybersecurity across the EU. Many public entities with crucial cybersecurity roles would, in fact, be excluded from the scope if the NUTS classification prevails. For example in Poland NUTS 1 classification refers to macro regions established for statistical purposes only. There aren't any public administration structures in macro regions.
3) The management bodies of public administration entities have different structures and liability regimes, especially if they include political appointees. This significant difference to other sectors is not duly taken into account in the provisions of the NIS2.
4) The model of supervision and enforcement in public administration entities also varies significantly amongst Member States.

Therefore, we believe that Member States should be given a flexibility to decide (A) if and which public administration entities should be covered by the NIS2 and (B) to exclude obligations for these entities regarding security requirements, incident notification, supervision, and sanctions. These matters should be at the individual Member State's sole discretion.

A. Identification of public administration entities by the individual Member State

In light of the above, we propose to exclude the public administration sector from Annex I (essential entities) of the NIS2 proposal and redraft the respective provisions. The mechanism in the NIS Directive currently in force whereby Member States identify the operators/entities that fall under the NIS Directive remains appropriate with regard to public administration entities. Moreover, the new wording of articles should foresee criteria for such an identification that could be, in principal, in line with the definition 'public administration entity' in the current NIS2 proposal.

Having in mind the legal basis of the NIS2, namely art. 114 TFEU (functioning of the internal market), the criterion of decisions affecting rights in the cross-border movement of persons, goods, services or capital should be included. Establishment for the purpose of meeting needs in the general interest and not having an industrial or commercial character should also stay.

As well as the condition of public financing or being subject to management supervision by authorities or bodies; or it having an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities, or by other bodies governed by public law.

The criterion of having the legal personality seems to not to be necessary. In fact in some Member States having such a criterion would mean that many entities with crucial cybersecurity roles would be excluded. For example in Poland most of entities of central government act within the legal personality of the State Treasury. Also some regional authorities do not have separate legal personality.

At the same time it should be clear that public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security should be excluded from the scope of NIS2. General exclusion in Article 2 para 3 of the NIS2 should reflect this matter.

B. Exclusion of obligations for 'public administration entities' by the individual Member State

Regarding the different structures and liabilities of management bodies of public administration, we believe we should include a possibility for Member States to derogate public administration entities from all or some obligations foreseen in art. 17 and 18 of the NIS2. In particular, the accountability of the management bodies of the public administration for non-compliance should be executed in line with existing national regulations, therefore the NIS2 should not regulate this issue.

Member States should also have a possibility to derogate public administration entities from all or some measures in art. 29 of the NIS2, to take into account different, national models of supervision and enforcement.

III. Drafting proposal

In order to reflect the above in the NIS2, we propose the following amendments.

No.	Reference	EC proposal	Proposal for amendment
1.	Recital 8	(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[3], 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.	(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[4], 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. Nevertheless, taking into account the difference in composition of public administration in the Member States, the identification process provided in Directive (EU) 2016/1148 remains an appropriate mechanism to determine which public

[3] 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).

[4] 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).

No.	Reference	EC proposal	Proposal for amendment
			administration entities should fall under the scope of this Directive.
2.	Recital 8a		(8a) **Taking into consideration the differences in the national public administration frameworks, Member States retain full decision-making autonomy regarding the question of whether to identify public administration entities and if Member States decided to do so which entities are to be identified. It would also be possible to foresee in the national legislation that particular categories of public administration entities are identified as falling under the scope of this Directive. Member States should also be able to structure the obligations for public administration entities regarding security requirements, incident notification, supervision and sanctions.**
3.	Recital 11	(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 reporting obligations. The supervisory and penalty regimes between these two categories of entities should be differentiated to ensure a fair balance between 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 three categories: essential, important, and public administration. 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. Essential and important entities and public administration entities should be subject to the same risk management requirements and reporting obligations. Member States should have right to exclude obligations for public administration entities. The supervisory and

No.	Reference	EC proposal	Proposal for amendment
		obligations on one hand, and the administrative burden stemming from the supervision of compliance on the other hand.	penalty regimes between essential and important 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. The supervisory and penalty regimes for public administration entities should be foreseen in line with the national legislation and legal system.
4.	New Recital 20a		**(20a) It is crucial to raise the cyber awarness and resilience in public administration entities. At the same time it is also essential to take into account the specificities of the composition of national public administrations. Therefore Member States should be given a flexibility to decide if and which public administration entities should be covered by this Directive and should have right to exclude select obligations for these entities. Identification of public administration entities should be at the individual Member State's sole discretion.**
5.	Recital 21	(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	(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 and public administration entities under this Directive. Member

No.	Reference	EC proposal	Proposal for amendment
		Directive. Member States should be able to assign this role to an existing authority.	States should be able to assign this role to an existing authority.
6.	Recital 42	(42) Essential and important entities should ensure the security of the network and information systems which they use in their activities. Those are primarily 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.	(42) Essential and important entities and public administration entities should ensure the security of the network and information systems which they use in their activities. Those are primarily 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 and public administration entities regardless of whether they perform the maintenance of their network and information systems internally or outsource it.
7.	Recital 46	(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[5], with the aim of identifying per sector	(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive and public administration entities 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[6], with the aim of identifying per sector which are the critical

[5] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

[6] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

No.	Reference	EC proposal	Proposal for amendment
		which are the critical ICT services, systems or products, relevant threats and vulnerabilities.	ICT services, systems or products, relevant threats and vulnerabilities.
8.	Recital (47)	(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.	(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 and public administration 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.
9.	Recital 52	(52) 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	(52) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities and public administration entities are dependent on services provided over the internet. In order to ensure the

No.	Reference	EC proposal	Proposal for amendment
		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.	smooth provision of services provided by essential and important entities and public administration 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.
10.	Recital 56	(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 law and decrease the burdens for companies.	(56) Essential and important entities and public administration 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 law and decrease the burdens for companies.
11.	Recital 57	(57) Where it is suspected that an incident is related to serious criminal activities under Union or national law,	(57) Where it is suspected that an incident is related to serious criminal activities under Union or national law,

No.	Reference	EC proposal	Proposal for amendment
		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.	Member States should encourage essential and important entities and public administration 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.
12.	Recital (63)	(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 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.	(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 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. Public administration entities shall fall under the jurisdiction of the Member State in which they were identified pursuant to Article 2a.
13.	Recital (70)	(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	(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

No.	Reference	EC proposal	Proposal for amendment
		important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important 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 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.	important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important 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 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. When it comes to public administration entities the supervisory powers should be executed in line with the national frameworks and it should be up to Member States discretion to impose suitable measures of supervision and enforcement.
14.	Art. 1 (2)	2. To that end, this Directive: (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); (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;	2. To that end, this Directive: (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); (b) lays down cybersecurity risk management and reporting obligations for entities of a type referred to as essential entities in Annex I, important

No.	Reference	EC proposal	Proposal for amendment
		(c) lays down obligations on cybersecurity information sharing.	entities in Annex II and public administration entities; (c) lays down obligations on cybersecurity information sharing.
15.	New art. 2 (1a) and (1b)		**1a This Directive also applies to public administration entities indentified by the Member States in accordance with art. 2a, notwithstanding para 1b.** **1b This Directive does not apply to public administration entities that carry out activities in the areas of public security, defence or national security.**
16.	Art. 2 (2)	2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where: (a) the services are provided by one of the following entities: (i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I; (ii) trust service providers referred to 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; (b) the entity is a public administration entity as defined in point 23 of Article 4; (c) the entity is the sole provider of a service in a Member State;	2. However, regardless of their size, this Directive also applies to entities referred to in Annexes I and II, where: (a) the services are provided by one of the following entities: (i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I; (ii) trust service providers referred to 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; (b) the entity is the sole provider of a service in a Member State;

No.	Reference	EC proposal	Proposal for amendment
		(d) a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health; (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; (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; (g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive. 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.	(c) 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 induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact; (e) 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; (f) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive. Member States shall establish a list of entities identified pursuant to points (b) to (e) 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.
17.	Art.2(5)	5. Without prejudice to Article 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	5. Without prejudice to Article 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

No.	Reference	EC proposal	Proposal for amendment
		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.	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 or public administration entities.
18.	New Art. 2a		***Article 2a*** ***Identification of Public Administration Entities*** **1. By [date] Member States may identify public administration entities established on their territory.** **2. The criteria for the progressive identification of public administration entities shall be as follows:** **(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;** **(b) 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 are appointed by the State, regional authorities, or by other bodies governed by public law;** **(c) 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.** **3. The public administration entities identified in line with this Article shall be reviewed and where appropriate updated by Member States when necessary.**

No.	Reference	EC proposal	Proposal for amendment
			4. Member States shall inform the Commission about the result of the process of identification of public administration entities in accordance with this Article.
19.	Art. 4 (23)	(23) 'public administration entity' means an entity in a Member State that complies with the following criteria: (a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character; (b) it has legal personality; (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 are appointed by the State, regional authorities, or by other bodies governed by public law; (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. Public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded.	(23) 'public administration entity' means an entity in a Member State **that was identified by the Member State in accordance with Article 2a.**
20.	Art. 5(2)	2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies: (a) a policy addressing cybersecurity in the supply chain for ICT products and services used by	2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies: (a) a policy addressing cybersecurity in the supply chain for ICT products and services used by

No.	Reference	EC proposal	Proposal for amendment
		essential and important entities for the provision of their services;	essential and important entities and public administration entities for the provision of their services;
21.	Art.6(2)	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 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.	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 public administration 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 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.
22.	Art. 9 (3) and (4)	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,	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 public administration entities and other relevant interested parties. To this end, Member States

No.	Reference	EC proposal	Proposal for amendment
		Member States shall ensure that the CSIRTs contribute to the deployment of secure information sharing tools. 4. CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 26 with trusted sectorial or cross-sectorial communities of essential and important entities.	shall ensure that the CSIRTs contribute to the deployment of secure information sharing tools. 4. CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 26 with trusted sectorial or cross-sectorial communities of essential and important entities and public administration entities.
23.	Art.10(2)(b)	2. CSIRTs shall have the following tasks: […] (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;	2. CSIRTs shall have the following tasks: […] (b) providing early warning, alerts, announcements and dissemination of information to essential and important entities and public administration entities as well as to other relevant interested parties on cyber threats, vulnerabilities and incidents;
24.	Art.11(2)	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 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 or public administration entities, pursuant to Article 20.
25.	Art.14(5)	5. EU-CyCLONe shall regularly report to the Cooperation Group on cyber threats, incidents and trends, focusing in	5. EU-CyCLONe shall regularly report to the Cooperation Group on large scale incidents , focusing in particular on

No.	Reference	EC proposal	Proposal for amendment
		particular on their impact on essential and important entities.	their impact on essential and important entities and public administration entities.
26.	Art.17(1)	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.	1. Member States shall ensure that the management bodies of essential and important entities and public administration 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.
27.	Art.18(1)	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 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.	1. Member States shall ensure that essential and important entities and public administration 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 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.
28.	Art. 20 (1) and (2)	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	1. Member States shall ensure that essential and important entities and public administration 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

No.	Reference	EC proposal	Proposal for amendment
		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. 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.	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. 2. Member States shall ensure that essential and important entities and public administration 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.
29.	New Art. 20a		***Article 20a*** ***Divergence for Public Administration Entities*** **Member States may lay down the rules on whether and to what extent public administration entities are excluded from the obligations provided in Article 17, Article 18 and Article 20.**
30.	Art.21(1)	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 essential and important entities and public administration 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 public administration entities or procured from third parties.

No.	Reference	EC proposal	Proposal for amendment
31.	Art. 24	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: (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	1. Without prejudice to Regulation (EU) 2016/679, Member States shall ensure that essential and important entities and public administration 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: (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 and public administration 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

No.	Reference	EC proposal	Proposal for amendment
		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.	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 and public administration 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.
32.	New Art. 30a		***Article 30a*** ***Supervision and enforcement for public administration entities*** **1. Member States shall ensure that the measures of supervision or enforcement imposed on public administration 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 and enforcement powers in relation to public administration entities have the appropriate powers in accordance with national legislation.**

No.	Reference	EC proposal	Proposal for amendment
33.	Art. 31	*Article 31* *General conditions for imposing administrative fines on essential and important entities* 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, 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). 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 29(7). 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.	*Article 31* *General conditions for imposing administrative fines on essential and important entities and public administration entities* 1. Member States shall ensure that the imposition of administrative fines on essential and important entities and public adminisration 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, 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). 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 29(7). 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

No.	Reference	EC proposal	Proposal for amendment
		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.	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 identified in accordance with Article 2a subject to the obligations provided for by this Directive.
34.	Art. 32 (1)	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 **or public administration 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.
35.	Annex I	9. Public administration – Public administration entities of central governments – Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003 – Public administration entities of NUTS level 2 regions listed in Annex I of Regulation (EC) No 1059/2003	~~9. Public administration~~ ~~– Public administration entities of central governments~~ ~~– Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003~~ ~~– Public administration entities of NUTS level 2 regions listed in Annex I of Regulation (EC) No 1059/2003~~