Council of the European Union

Brussels, 13 September 2021
(OR. en)

11724/21

Interinstitutional File:
2020/0359(COD)

LIMITE

CYBER 233
JAI 978
DATAPROTECT 215
TELECOM 335
MI 660
CSC 312
CSCI 119
CODEC 1204

NOTE

From:	Presidency
To:	Delegations
Subject:	Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148 - Presidency compromise proposal on the scope of the NIS 2 Directive

Delegations will find in Annex the Presidency compromise proposal on the scope of the NIS 2 Directive based on the written comments and non-papers received from Member States. This proposal will be discussed at the HWPCI meeting on 15 September 2021.

The changes compared to the Commission proposal are marked in **bold and underlined.** Those that strictly concern the scope of the directive are also highlighted in **yellow**.

ANNEX

Presidency compromise proposal on the scope of the NIS 2 Directive

I. Reasoning

The Presidency compromise proposal on the scope of the NIS 2 Directive, specifically in relation to the "size-cap rule" builds on the following key principles: promoting a higher level of cybersecurity in the Union and a greater level of harmonisation, while also ensuring the necessary proportionality, a greater level of risk management and elements for determining the entities that fall under the scope of the directive.

The proposal changes to a certain extent the original proposal by the European Commission with regard to the size-cap. It maintains the size-cap rule for large entities, but it introduces changes with regard to medium size entities.

It includes changes to Article 2 by merging Annexes I and II of NIS 2 proposal into a single Annex covering all sectors and types of services under the NIS 2 scope. Furthermore, it proposes to ensure all large entities provided for in the Annex and all entities identified as critical entities under the CER Directive, as well as other entities as described in Article 2(2), would be considered as essential entities. All medium entities provided for in the annex would be considered as important entities. However, by amending Article 2(2) of the NIS 2 proposal, Member States, based on criteria (c) to (f), may establish that such medium entities are essential entities; the same principle applies also for small and micro entities.

Following the changes made, the proposal includes also changes to recitals 8 and 9, and Article 2 with regard to the registration and the role of the Member States.

The proposal maintains the differentiation between *ex ante* supervision for essential entities and *ex post* supervision for important entities. At the same time, it includes new proposal on prioritisation of supervision and risk based approach in recital 70, new recital 70 bis, Articles 28, 29, and 30 to ensure greater level or proportionality.

In the current proposal on the scope, the Presidency does not address the question of public administration in its totality, neither the question of scope of individual sectors from the annexes. The proposal includes references to some of the amendments that will be included in the comprehensive Presidency compromise proposal, as planned for the HWPCI meeting on 27 September. These proposals are still subject to change and will not be discussed on 15 September.

II. Proposed changes

A) Amended recitals in relation to the scope:

(8) In accordance with Directive (EU) 2016/1148, Member States were responsible for determining which entities meet the criteria to qualify as operators of essential services ('identification process'). In order to eliminate the wide divergences among Member States in that regard and ensure legal certainty for the risk management requirements and reporting obligations for all relevant entities, a uniform criterion should be established that determines the entities falling within the scope of application of this Directive. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[1], that operate within the sectors or provide the type of services covered by this Directive, fall within its scope. ~~Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion.~~ **In order to ensure a clear overview of the entities falling within the scope of this Directive, Member States should establish national registration mechanisms which may require entities that meet this generally applicable size-related criterion and to which this Directive applies to register with the relevant authorities designated for this purpose by the Member States. These registries should also include public administration entities to which this Directive applies.**

[1] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

(9) However, small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit ~~it~~ to the Commission **relevant information relating to the list, including the number of identified entities, their type, their size, the specific criteria based on which they were identified and, where in line with national security rules, the names of the entities**.

(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance, this Directive should provide for a minimum list of supervisory actions and means through which competent authorities may supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to 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. **For important entities, *ex-post* supervision may be triggered by evidence or any indication or information brought to the attention of competent authorities deemed by these authorities as suggesting potential non-compliance with the obligations laid down in this Directive. For example, such evidence, indication or information could be of the type provided to the competent authorities by other autorities, entities, citizens, media or other sources, publicly available information, or may emerge from other activities conducted by the competent authorities in the fulfilment of their tasks.**

(70bis) **In the exercise of *ex-ante* supervision, competent authorities should be able to decide on the prioritisation of the use of supervisory actions and means at their disposal in a proportionate manner. This entails that competent authorities may decide on such prioritisation based on supervisory methodologies which should take account of a risk-based approach. More specifically, such methodologies could include criteria and/or benchmarks for the classification of essential entities into risk categories and corresponding supervisory actions and means recommended per risk category, such as: use and/or frequency or type of on-site inspections or targeted security audits or security scans, type of information to be requested and level of detail, etc. Such supervisory methodologies may also be accompanied by work programmes and be assessed and consequently reviewed regularly, including on aspects such as resource-allocation and needs.**

B) Amended Articles in relation to the scope:

Article 2

Scope

1. This Directive applies to public and private entities of the type ~~reffered to as~~ provided for in **the** Annex ~~I and as important entities in Annex II~~. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.[2] **Article 3 paragraph 4 of the Annex to the Commission Recommendation 2003/361/EC shall not apply.**

2. However, regardless of their size, this Directive also applies to entities referred to in the Annexes ~~I and II~~, where:

(a) the services are provided by one of the following entities:

[2] 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).

(i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of **the** Annex ~~I~~;

(ii) qualified trust service providers as referred to in point XX of the Annex;

(iii) non-qualified trust service providers as referred to in point XX of the Annex;

(iv) top–level domain name registries ~~and domain name system (DNS)~~ referred to in point 8 of **the** 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 **which is essential for the maintenance of critical societal and/or economic activities;**

(d) a potential disruption of the service provided by the entity could have a~~n~~ **significant** impact on public safety, public security or public health;

(e) a potential disruption of the service provided by the entity could induce **significant** 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[3] [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive.

[3] *[insert the full title and OJ publication reference when known]*

Member States shall establish a list of entities identified pursuant to point ~~(b)~~ **(c)** to (f) and submit to the Commission **relevant information relating to the list, including the number of identified entities, their type as per the Annex, their size, the specific provision of Article 2(2) based on which they were identified and, where in accordance with national security rules, the names of the entities 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.]

2a. Entities of the type provided for in the Annex to this Directive which exceed the ceilings for medium-sized enterprises as defined in Commission Recommendation 2003/361/EC as well as entities referred to in Article 2(2) (a) (i) (ii) and (iv) and Article 2(2)(b)*[public administration]* and (g) shall be considered essential entities.

2b. Entities of the type provided for in the Annex to this Directive which qualify as medium-sized entreprises within the meaning of Commission Recommendation 2003/361/EC as well entities referred to in Article 2(2)(iii) *[non-qualified TSP]* and Article 2(2)(c) to (f) shall be considered important entities. Member States may however establish, based on the criticality criteria referred to in Article 2(2)(c) to (f), that medium-sized entreprises within the meaning of Commission Recommendation 2003/361/EC are essential entities. Member States may also establish that, based on specific national risk assessments, micro or small-sized entities within the meaning of Commission Recommendation 2003/361/EC identified pursuant to paragraph (2) points (b) to (f) of this article, are essential entities.]

3. This Directive is without prejudice **to actions taken by the** Member States **and their relevant competences to safeguard their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. These actions include activities, irrespective whether conducted by public entities or by private entities on behalf of public authorities,** concerning the maintenance of public security, defence and national security **and activities in areas of criminal law, including the protection of information the disclosure of which Member states consider contrary to the essential interests of their national security or defence,** in compliance with Union law. **Public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security shall be excluded of the scope of this Directive**.

(…)

Article 4

Definitions

For the purposes of this Directive, the following definitions apply:

(…)

(25) 'essential entity' means any entity of the type provided for in the Annex and designated 'essential' in accordance with Article 2 of this Directive;

(26) 'important entity' means any entity of the type provided for in the Annex and designated 'important' in accordance with Article 2 of this Directive.

(…)

Article 28

General aspects concerning supervision and enforcement

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. **Member States may allow competent authorities to prioritise supervision based on a risk-based approach.**

2. Competent authorities shall work in close cooperation with data protection authorities**, competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and other competent authorities designated under sector-specific Union legal acts when addressing cybersecurity incidents.**.

Article 29

Supervision and enforcement for essential entities

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, **follow a risk-based approach and** have the power to subject those entities **at least** to:

   (a) on-site inspections and off-site supervision, including random checks;

   (b) regular **security** 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**, where technically necessary with the cooperation of the entity concerned**;

(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.

2a. Where exercising their supervisory tasks provided for in paragraph 2 of this Article, competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.

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 **at least** 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 **the nature of the threat, as well as** any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;

(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;

(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 **or courts according to national laws** to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;

   (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.

   These sanctions shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.

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. **As regards public administration entities, this provision shall be without prejudice to the Member States' laws as regards the accountability of elected and appointed public servants and officials.**

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 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 the risk of actual or potential loss of life and physical, social, emotional and psychological well-being,** actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;

(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 of the natural or legal person(s) held responsible with the competent authorities.

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.

(…)

Article 30

Supervision and enforcement for important entities

1. When provided with evidence, indication **or information** 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, **follow a risk-based approach and** have the power to subject those entities **at least** 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, **non-discriminatory,** fair and transparent risk assessment criteria, **where technically necessary, with the cooperation of the entity concerned**;

   (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**;**

(f) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by an independent qualified auditor and the respective underlying evidence.

2a. Where exercising their supervisory tasks provided for in paragraph 2 of this Article, competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.

3. Where exercising their powers pursuant to points (d) **to (f)** 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 **at least** 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 **the nature of the threat, as well as** any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;

(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;

(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;

(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.