Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359 (COD)

Brussels, 27 July 2021

WK 9879/2021 INIT

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
CSC
CSCI
CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From: To:	General Secretariat of the Council Delegations
N° prev. doc.: N° Cion doc.:	WK 8953/21 14150/20
Subject:	Presidency Options paper on the scope of the NIS 2 Directive - Comments by DE, FI , LU and PT delegations

Delegations will find in Annex comments by DE, FI, LU and PT delegations on the Presidency options paper on the scope of the NIS 2 Directive.

Table of Contents

FINLAND

Presidency Options Paper on the scope of the NIS 2 Directive, WK 8953/2021

I. SCOPE of the NIS 2 proposal – "size-cap"

1. Is the original Commission proposal acceptable as the basis for further work or are there alternative proposals?

We think that the original proposal by COM is acceptable as basis for further work. We see that the size-cap is a sufficiently adequate base criterion in relation to the objective of NIS2, which is to cover a larger scope of sectors that are critical to the functioning of society across the EU.

It is also natural to think that mid-size and large entities would have a larger impact in societies across Member States as they most probably constitute the majority of services provided falling in the scope of NIS2.

Small and micro entities should be exempted from the scope (taking into account possible exceptions according to art. 2.) to avoid excessive and disproportionate administrative burden.

We also welcome the size-cap criterion as a way to harmonise the NIS2 scope across all Member States and as way to ease the administrative burden deriving from the national identification process applied in NIS1.

For NIS2 to really be a better version of its predecessor, we see that going back to the national identification process as in NIS1 could undermine this objective and hinder the added value of NIS2 obligations. We see that introducing a national identification process in NIS2 would bring us back to the same challenges we faced with NIS1. This would also hinder the objective of balancing the administrative burden, which is already increasing in NIS2.

In addition, it is important to bear in mind the risks of possible cascading effects of cybersecurity threats, incidents and crises between all Member States and sectors. The scope of NIS2 should respond to this increasing inter-dependency between MS and sectors.

Still, we acknowledge the need to fine-tune the proportionality of NIS2 in other ways in the text.

2. If Member States are willing to work on the Commission proposal as the basis, what changes are needed to address the Member States' concerns?

While we welcome the current size-cap as a starting point, we warmly welcome the discussion on this matter.

It is important to ensure sufficient national leeway throughout NIS2. This applies to this topic as well. Does NIS2 provide Member States' competent supervising authorities the possibility to prioritise their tasks accordingly, in light of the provisions in art. 18.1. and art. 29.1.?

The possibility of prioritising could be further clarified in the text to strengthen the proportionality of the obligations. We have suggested a draft amendment on this to article 28.

3. Is the proposal in the non-paper prepared by AT, CZ, DE, PL and NL an acceptable way forward as the basis for further discussions in the Council?

We would prefer the original COM proposal.

One possible option to be explored as a compromise, if the majority of MS prefer this option, could be to introduce an opt-out mechanism in NIS2. This would entail that competent supervising authorities could decide on transferring an entity from essential to important category or from important to be exempted from the scope, based on application submitted by the entity and if the required criteria for this transfer are met. Still, this would not solve the issue of varying identification of entities between Member States and could pose risks especially from the perspective of supply chains across the EU.

4. In relation to the preferred way forward, how do Member States see the differentiation between important and essential entities? What are possible implications with regard to the supervision, as well as risk management and reporting provisions?

For NIS2 to be better than NIS1, we see that it should respond also to the need of prevention. Therefore, the proposed supervision mechanism provides a good basis to prevent cyber threats, incidents and crises in essential entities via ex ante supervision. Transferring all entities to the important category could hinder possibilities of prevention.

Introducing a varying supervising mechanism and risk management measures between all entities in NIS2 could bring more challenges for streamlining competent supervising authorities' tasks.

5. In relation to the "size-cap", some Member States expressed concerns in relation to the SMEs from the perspective of proportionality of the NIS 2 proposal. What are Member States alternative proposals with regard to the inclusion of the SMEs in the scope of the NIS 2 Directive?

For Finland, it is important that small and micro entities are in principle excluded from the scope (taking into account the possible exceptions according to article 2). This is important to limit the burden from NIS2 obligations both on the entities as well as on competent supervising authorities.

We see that NIS2 obligations should be promoted as an investment to the continuity of operations of large and mid-size entities, as any cyber threat, incident or crisis can induce significant damages going beyond the costs to comply with the NIS2 obligations in the long run. On the other hand, NIS2 should find a balance between imposing obligations and generating benefit (or return on investment, in a sense) for entities, especially when discussing any possible obligations for smaller entities, to ensure a proportionate NIS2 framework.

One possibility to clarify the proportionality of the NIS2 framework without destabilising the size-cap base, could be to specify in the text that if a small or micro entity is identified nationally as critical within NIS2 (according to art. 2 (c)-(f), its risk management measures and supervision should be strongly proportionated to its size and operations. This could also apply to other exceptions from the size-cap according to art. 2 (a)-(b).

6. What are the legal implications of the proposed changes?

As mentioned in our comments, we see that the changes proposed in the non-paper could lead to the same challenges faced with NIS1 across the EU, where entities are identified differently between Member States. Furthermore, the suggested changes could lead to possible interpretation issues between Member States.

II. Inclusion of Public administration

1. Is the original Commission proposal acceptable as the basis for further work or are there alternative proposals?

Yes, we see that the original Commission proposal is more appropriate for the NIS2 framework compared to the suggestion in the non-paper.

2. Is the proposal in the non-paper prepared by BE, DE, HU, IT, MT, NL, PL and SE an acceptable way forward as the basis for further discussions in the Council?

At this stage, we see that the original proposal is more suitable for NIS2. Still, we understand the need for discussion on this topic as Member States' public administration structures can differ greatly.

For us, it is important also for this reason to ensure sufficient national margin in the appropriate implementation of NIS2 obligations as regards the sector of public administration. Sufficient national flexibility is also important to avoid excessive costs for the public sector, while a high level of cybersecurity is important.

While we understand that the NUTS classification can be seen as challenging because it was originally designed for statistical purposes, at this stage we have not identified similar challenges as in some other Member States on this topic.

3. What are the legal implications of the proposed changes?

We see that the proposed changes could lead to different levels of application of NIS2 obligations among Member States.

III. EXCLUSION CLAUSE

1. Is the proposal in the non-paper prepared by CZ, DE, IE, IT and SE an acceptable way forward as the basis for further discussions in the Council?

We see that the current wording of art. 2.3. in NIS2 text is adequate. If most MS see the proposal in the non-paper as a better option, we are open to continue discussions on this option. We will also gladly participate in drafting this article further. We present our suggestion for amendment below.

In any case, for us it is imperative to keep this article in NIS2.

We emphasise striving for a coherent wording between NIS2 and DORA on this matter. These provisions are currently aligned between both proposals. The benefit of aligning these is that we avoid any problems of interpretation between the two.

2. What are other additional proposals to seek further legal clarity?

-

3. What are the legal implications of the proposed changes?

For Finland, it is imperative to keep art. 2.3. in the text, as mentioned above.

If most MS prefer the proposal in the non-paper, a similar wording should also be discussed in negotiations of other relevant proposals, such as DORA and CER, to ensure wording coherence and prevent any interpretation issues.

While we understand that the proposed wording in the non-paper is more detailed, this alternative should not lead to any interpretation issues on EU or national level.

Additional comments and drafting suggestion on the exclusion clause:

As a general comment, we express at this stage our scrutiny reservation to the details of the proposed wording for art. 2.3 in the non-paper.
To clarify the article, we suggest reintroducing “defence” in addition to national and public security to the wording. If art. 2(3)(b) is maintained and this section includes “public security”, that would be sufficient in that regard.

We also propose making slight amendments to "essential State functions" to better clarify that functions essential to a State can also be provided by private entities. This amendment would also be in line with the spirit of subsection (iii).

A small amendment is suggested at the end of subsection (ii) to avoid misinterpretation as follows: "…without limiting the rights of Member State's authorities to receive such information,". The addition would clarify that the intention of the wording is not to actually create an obstacle for the authorities to receive crucial information, but to make sure that access is guaranteed.

A minor amendment is also suggested in subsection (iii) to clarify that in addition to a request from a public entity, requirements concerning private entities may also be based on national law. Alternatively "acting at the request of a public entity or pursuant to national law" could also be deleted altogether for the same effect.

Regarding art. 2(3)(b), we would like to highlight the need to clarify further the relation between each subsection.

Proposed wording in non-paper – art. 2.3.

3. This Directive **does not**
(a) is without prejudice to the competences **affect the sole responsibility** of Member States **to safeguard** concerning the maintenance of public security, defence and national security **or their power to protect other essential State functions . In particular, this Directive does not**

(i) apply to entities with importance to Member States' defence or national security,

(ii) oblige Member States or entities to supply information where such a supply of information would be contrary to national security or defence interests,

(iii) apply to those activities of entities, which fall outside the scope of in compliance with Union law **and in any event all activities concerning national security and defence, regardless of who is carrying out those activities whether it is a public entity or a private entity acting at the request of a public entity**.

(b) apply in the area of public security and the judiciary. In particular, this Directive does not

(i) apply to entities with importance to Member States' judiciary and public security, including public administration entities to any extent concerned with law enforcement,

(ii) oblige Member States or entities to supply information where such a supply of information would be contrary to public security,

(iii) apply to those activities of entities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

FI amendment suggestions – art. 2.3.

3. This Directive **does not**
a) is without prejudice to the competences **affect the sole responsibility** of Member States **to safeguard** concerning the maintenance of public security, defence and the maintenance of defence and national security **or their power to protect other functions essential to a State. In particular, this Directive does not**

(i) apply to entities with importance to Member States' defence or national security,

(ii) oblige Member States or entities to supply information where such a supply of information would be contrary to national security or defence interests, without limiting the rights of Member State's authorities to receive such information,

(iii) apply to those activities of entities, which fall outside the scope of in compliance with Union law **and in any event all activities concerning national security and defence, regardless of who is carrying out those activities whether it is a public entity or a private entity [acting at the request of a public entity or pursuant to national law].**

(b) apply in the area of public security and the judiciary. In particular, this Directive does not

(i) apply to entities with importance to Member States' judiciary and public security, including public administration entities to any extent concerned with law enforcement,

(ii) oblige Member States or entities to supply information where such a supply of information would be contrary to public security,

(iii) apply to those activities of entities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

GERMANY

Presidency Options Paper on the Scope of NIS2 – Answers by DE
12 July 2021

Scope of NIS2, Size-Cap-Rule

Is the original Commission proposal acceptable as the basis for further work or are there alternative proposals?

Answer by DE – We are currently evaluating alternatives to the Size-Cap-Rule. As stated previously, we believe that a company's size as the single criterion for including it in the scope of NIS2 does not sufficiently reflect the criticality of the services it supplies.

At the same time, we acknowledge that it will probably be difficult to identify different concrete criteria that take into account the local criticality of supply and are equally applicable in all Member States across the Union. The two main issues we see with the current proposal is that (1) the total number of entities in the scope is too high, and (2) neither the scope nor the cybersecurity obligations themselves sufficiently take the criticality of supply of the concerned entity into account.

If Member States are willing to work on the Commission proposal as the basis, what changes are needed to address the Member States' concerns?

Answer by DE – DE is a co-signatory of the non-paper on scope of NIS2. Therefore, from our point of view, regarding the question of scope, adjustments should be made to the Size-Cap-Rule in order to achieve a more manageable total number of entities inside the scope of NIS2, which at the same time also leads to an overall increase in the level of cybersecurity. This can be achieved by e.g. by sharpening the sector definitions (for example, but not limited to, the food sector), and/or by discussions about either excluding medium-sized enterprises in certain sectors or at least making their inclusion in certain sectors optional.

In addition to these measures, we believe a differentiation of the actual obligations of entities in the scope of NIS2 as described in the non-paper is crucial in achieving an overall proportionate approach of NIS2.

Is the proposal in the non-paper prepared by AT, CZ, DE, PL and NL an acceptable way forward as the basis for further discussions in the Council?

Answer by DE – Yes. On the basis of the non-paper, text proposals should be presented.

In relation to the preferred way forward, how do Member States see the differentiation between important and essential entities? What are possible implications with regard to the supervision, as well as risk management and reporting provisions?

Answer by DE – With our IT-Security Law 2.0 of this year, we already established a second category of entities besides OES, called companies in the particular public interest. Such companies are subject to a lower level of cybersecurity requirements. In this vein, we believe it is necessary to differentiate between the essential entities and important entities. In detail:

In order to prevent lowering the level of cybersecurity across the Union, it should be made clear that entities that have been identified as OES under NIS1 should also be identified as essential entities under NIS2.

- *Supervision: The current (and thus far only) differentiation of supervision (ex-ante vs. ex-post) should remain.*
- *Risk management: We identified cybersecurity requirements to be the main cost driver for entities. Therefore, we believe introducing a sensibly lowered cybersecurity baseline for important entities is an important step in bringing overall costs down. The requirements for essential entities on the other hand should remain at the current level of the proposal, with specific enhancements and/or clarifications, where appropriate.*
- *Reporting obligations: Generally, we believe that reporting obligations will need to be amended in order to find the right balance between the necessity for NCAs for situational awareness and administrative burden on entities. This includes clearer definitions of cyber-threats as well as more appropriate reporting deadlines.*
- *We also believe that important entities should not be subject to the identical sanctions as essential entities, as this would in our view not be proportionate.*
- *Further differentiation might be needed in the services NCAs and CSIRTs have to offer important and essential entities.*

In relation to the "size-cap", some Member States expressed concerns in relation to the SMEs from the perspective of proportionality of the NIS 2 proposal. What are Member States alternative proposals with regard to the inclusion of the SMEs in the scope of the NIS 2 Directive?

Answer by DE – See above.

What are the legal implications of the proposed changes?

Answer by DE – After the presentation of concrete text proposals by the co-signatories of the non-paper on scope, the legal implications will become clear.

Inclusion of Public Administration

Is the original Commission proposal acceptable as the basis for further work or are there alternative proposals?

Answer by DE – DE is a co-signatory of the non-paper on public administration. The original Commission proposal (i.e. mandatory inclusion of public administration entities) is unacceptable for DE for the reasons described in the non-paper.

Is the proposal in the non-paper prepared by BE, DE, HU, IT, MT, NL, PL and SE an acceptable way forward as the basis for further discussions in the Council?

Answer by DE – Yes.

What are the legal implications of the proposed changes?

Answer by DE – The legal implications are well described in the elaborate non-paper on public administration. In essence, a public administration entity will only be in the scope of NIS2 if a Member State so chooses and will be only subject to those provisions (requirements, supervision, sanctions) that the Member State declares to be applicable to public administration entities.

Exclusion Clause

Is the proposal in the non-paper prepared by CZ, DE, IE, IT and SE an acceptable way forward as the basis for further discussions in the Council?

Answer by DE – Yes. DE is a co-signatory of the non-paper on the exclusion clause.

What are other additional proposals to seek further legal clarity?

Answer by DE – The wording proposed by the PT-Presidency on the advice of the Council Legal Service would be unacceptable to DE.

What are the legal implications of the proposed changes?

Answer by DE – We propose to structure the exclusion clause three-fold in order to clarify exemptions with regard to public security, national security and defense on the one hand (as this is based on Art. 4 of the EU treaty) and public security on the other hand. The term public security encompasses all activities related to law enforcement as well as security activities by police as it does in Art. 1 (1) Directive (EU) 2016/680. In this frame, it should be clear that Member States may: (i) exclude relevant entities entirely, (ii) exclude relevant information to be supplied by Member States or entities, and (iii) exclude relevant activities by entities generally in scope of NIS2.

LUXEMBOURG

SCOPE of the NIS 2 proposal – "size-cap"

Luxembourg largely promotes a qualitative and cooperative approach that builds on a common understanding of the importance of assuring a high level of security for networks and information systems for entities of essential importance for the society and the economy, and of the challenges that entities face in implementing the right level of security. In a close exchange with the entities, we aim at providing appropriate guidance, support and tools in order to gradually step up the cyber security level across the global ecosystem.

In the context of the implementation of NIS 1, the national identification process that was based on clear and objective criteria as the number of users relying on the service, the dependency of other essential sectors on the service, the impact of a potential incident, the market share of the entity and the importance of the entity for maintaining a sufficient level of the service, allowed us to identify in a quite comprehensible, objective and transparent manner the entities of essential importance for society and economy.

Although we have not yet fully evaluated the impact of the size-cap rule at a national level, the proposed proceedings might result in a considerable, non-gradual increase of the number of entities in scope, or might extend the scope to entities that are not really of essential importance for society and economy. Care must be taken not to end up jeopardizing existing qualitative national models, inducing disproportionate administrative burden for competent authorities, exposing obviously non-critical entities to regulatory burden or raising a sentiment of arbitrariness among concerned entities.

Thus, in-line with the expressed concerns and the outlined alternative proposal in the *non-paper by AT, CZ, DE, PL, LV and NL on the scope of NIS2*, Luxembourg is in favor of a more proportionate and risk-based approach for the determination of entities in scope and a larger differentiation of requirements and supervision for important and essential entities. We support the idea of a common, clearly defined, baseline level of security and risk management measures for important entities and advanced, eventually sector specific, security and risk management measures for essential entities.

As worked out in the non-paper paper by Hungary on the scope of the NIS2 Directive, entities that provide only auxiliary services or entities for which their activity in scope of the directive is not part of their core activities should not be considered as important or essential entities.

In order to provide a controlled manner to exclude entities that fall under the scope of the directive because of the size-cap rule or because of any other determination criteria, but that obviously do not provide services of vital importance for key societal and economic activities within the internal market or that the provision of those services does not depend on network and information systems , member states should be given the option to setup an opt-out mechanism, where competent authorities may, upon justified request by entities, exempt the requesting entities from obligations of the directive.

INCLUSION OF PUBLIC ADIMINISTRATION

As outlined in the National cyber security strategy, assurance of a high level of cyber security for national public administrations is of outmost importance and a key priority of the Luxembourgish Government.

Cyber security of luxembourgish public administrations that are part of the central government (ministries and administrations) is governed by a common overarching information security policy issued by the Government. Three governmental agencies work closely together in order to assure a high level of cyber security:

- The National Agency for the Security of Information Systems (ANSSI) is the national authority for the security of classified and unclassified information systems operated by the State. Its missions are to establish the general information security policy for the public sector, to define, in consultation with concerned players, information security policies and guidelines for specific domains, to define the information security risk management approach and to promote information security by awareness raising measures.
- The Governmental CERT (GOVCERT) is the single point of contact dedicated to handling large-scale security incidents affecting the networks and information systems of State administrations and departments. It provides a watch for detecting, alerting and responding to large-scale IT attacks and security incidents.
- The Government IT Centre (CTIE) provides IT services to public administrations. Its mission includes ensuring the security of information technology and the management and security of networks and information systems.

Most part of public administrations of the central government do not operate their own information systems. Also, those entities do not have a legal personality.
Besides the public administrations of the central government, there are some public agencies and public companies that might be in scope of the directive and that have a legal personality. Some of those entities operate their own information systems.

In accordance with the position argued in the *non-paper by BE, DE, HU, IT, MT, NL, PL and SE on the inclusion of public administrations in the NIS2 directive framework*, we agree that the public administration sector is far more differential than other sectors and that organization and governance models of public administration entities are country specific.

Therefore, in our opinion, member states should be given the flexibility to decide which national public administrations should be in scope and to adapt requirements and supervision of public administrations in scope to national specificities.

PORTUGAL

Presidency Options paper on the scope of the NIS 2 Directive (WK 8953/2021)

PORTUGAL

22.07.2021

Portugal would like to thank all member states for presenting the non-papers on the "scope of the NIS 2 proposal", on the "inclusion of Public Administration" and on the "exclusion clause" allowing an opportunity to further discuss such important matters.

The following sections summarizes Portugal's views and position on these topics

I. The scope of the NIS 2 proposal

Portugal recognizes the challenges of the entities' identification process introduced by NIS 1, leaving it up to the Member States de decision on the criteria to be applied, and acknowledges the fragmentation between Member States resulting from it. Such fragmentation led Member States to have different approaches to similar issues thus raising barriers to a common level of cybersecurity in the European Union (EU).

It is Portugal's view that NIS 2 must learn from NIS 1 avoiding maintaining the same conditions for fragmentation approaches within the EU. Therefore, welcomes all proposals for harmonization within the EU in this regard.

Although the "size-cap" rule in the NIS 2 proposal may not present itself as the perfect approach, seems to have some merits on establishing a common criterion for entities' identification between all Member States.

On the other hand, using risk-based assessment approaches may not be effective for identification of entities, as Portugal understands risk assessment as an instrument to identify which cybersecurity measures should be adopted by entities (operational aspects) and not for the designation of operator of essential/important service. For entities' identification purposes Portugal considers impact assessment approaches the most adequate instrument since it may better reveal their criticality and of the services they provide. The criterion for such impact assessment approaches should be established during the NIS 2 discussion process providing clarity for Member States in its further transposition.

Therefore, Portugal welcomes the discussion on concurrent identification processes in the NIS 2 proposal provided that do not compromise the objective of harmonization in the EU.

II. Inclusion of Public Administration

Portugal used its national prerogative to include Public Administration in the NIS 1 transposition to national legislation. In that sense Portugal defends the principle that cybersecurity requirements, notification procedures and supervision should be also applied to Public Administration.

With this view, Portugal supports the NIS 2 proposal of keeping Public Administration within its scope and is open for discussion on an alternative criterion to NUTS classification, assuring that important parts of the Public Administration are under its dispositions (e.g., "smartcities" regardless the municipalities level in NUTS).

III. Exclusion clause

It is Portugal's understanding that the NIS 2 text proposal reflects the Treaties dispositions.

However, Portugal is available to discuss improvements on the wording to accommodate the concerns raise by some Member States.