Council of the European Union
General Secretariat



**Interinstitutional files:**
**2020/0359(COD)**

**Brussels, 16 April 2021**

**WK 5081/2021 INIT**

**LIMITE**

**CYBER**
**JAI**
**DATAPROTECT**
**TELECOM**
**MI**
**CSC**
**CSCI**

WORKING PAPER

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

**WORKING DOCUMENT**

| | |
|---|---|
| From: | General Secretariat of the Council |
| 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 (EU) 2016/1148<br>- Comments and questions by BE, DK, FI, DE, IE, MT, NL, PL, SI, ES and SE on Articles 35-43 |

Delegations will find in Annex comments by BE, DK, FI, DE, IE, MT, NL, PL, SI, ES and SE on Articles 35-43.

# TABLE OF CONTENT

**BELGIUM**

## Art.35 – Review

*The Commission shall periodically review the functioning of this Directive, and [..] The report shall in particular assess the relevance of sectors, subsectors, size and type of entities referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. [..] The first report shall be submitted by… [54 months after the date of entry into force of this Directive].*

- A first evaluation of the relevance of the scope is foreseen only more than 4 years after the entry into force of the Directive. Hence, the Directive will have a major impact on thousands of entities before the relevance of the scope has been confirmed by the evaluation.
  Did the Commission take into account to set up a first evaluation, earlier than after 54 months?
- Did the Commission consider a more gradual implementation approach, where the scope of the implementation can be fine-tuned earlier on?

  Illustrative examples of gradual implementation approaches might be:
  - A first implementation wave with entities having more than 250FTE/50 M€ turnover, followed by a go/no go for smaller entities
  - A first wave of the most critical sectors, followed by a go/no go for the other sector
- Is the indicated period of [54 months] to be understood as the proposed frequency of the Directive's review, or only as the period before the first review would take place?

## Art.39 – Regulation 910/2014

- Can the Commission clarify the rationale behind the need to delete art. 19 of eIDAS, beside the general comment from recital 48?
  What will be the collateral effects of repealing Article 19 of eIDAS? Has the Commission carried out an impact assessment and if so, could we have a copy?
- Is there a particular reason for modifying the eIDAS regulation via NIS2 (and not via eIDAS2)?
- Is it, legally, possible to repeal a regulation's article by means of a directive?

**DENMARK**

*Article 39 (Amendment of Regulation (EU) No 910/2014):*

- Deleting article 19 in eIDAS: We are concerned about deleting article 19 from the eIDAS regulation. Firstly, article 19 can not be seen as isolated from the other parts of the regulation, and can not be deleted without having an impact on the interpretation of other articles, such as article 13 on liability, and article 24 which relates to the measures implemented due to article 19. Secondly, the scope of NIS2 and the eIDAS regulation are different. Article 19 in eIDAS require trust service providers to take appropriate technical and organisational measures to manage the risks posed to the *security of the trust services* they provide, whereas article 18 in the NIS2 proposal only require the providers to manage the risks posed to the *security of network and information systems* which those entities use in the provision of their services. Thirdly, there is a risk that the security of trust services may actually become less harmonised if regulated through a directive, rather than through an existing regulation, due to differences in national legislation. Finally, deleting article 19 at the time of entry into force of the directive, while applying an 18 months transposition period may cause a period of non-regulation of the security aspects of trust services. Could the Commission please comment on that?

**FINLAND**

**Preliminary comments and questions:**



**Article 36**

In principle, the possibility for the Commission to issue delegated acts can be seen as justified according to art. 18 (6) and art. 21 (2). Still, it is important that Member States can contribute to the process as early as possible. Also, it is important that the power to adopt delegated acts conferred to the Commission is well-defined, proportionate, appropriate and well-justified. Furthermore, it is important that these delegated acts do not limit Member States' possibilities for additional national measures ensuring a high level of cybersecurity.

**Article 38**

As the proposal is a significant update from NIS1, it is important that NIS2 follows a longer transposition period than the proposed 18 months. The transposition period should be extended to 24 months. A transposition period of 24 months would also adjust the timing with other relevant proposals. In the context of NIS2 discussions, we should also take into account similar views on the transposition period from discussions on other relevant proposals, such as DORA and CER to ensure a harmonised approach.

**Article 39 and 40**

We should still look into the possibilities of lex specialis for trust service providers (eIDAS provisions) and telecom sector (provisions in EECC) to ensure coherent obligations.

**GERMANY**

Please note: The following list of comments and questions regarding Art. 35-43 NIS2 is non-exhaustive and may be expanded in future discussions. Comments and questions are sorted by order of the Articles.

1. Question regarding Art. 39 – Article 19 of Regulation (EU) No 910/2014 (eIDAS) contains sector-specific cybersecurity requirements and reporting obligations for trust service providers. As currently drafted, once NIS2 would enter into force, Art. 39 NIS2 will cause Art. 19 eIDAS to be deleted with immediate effect. Thereby the requirements and obligations of Art. 19 eIDAS would cease to exist and respective provisions of NIS2 would only begin to apply, once the respective member state has transposed NIS2 into national law. Was the Commission aware of this lacuna in the law while drafting the provision?

2. Question regarding Art. 39 – How does the Commission ensure that the regulatory measures under NIS2 are in line with the evaluation of the eIDAS-Regulation and the Commission's upcoming legislative proposal for an eIDAS review?

**IRELAND**

**Article 35**

What is the purpose of the reports from the Cooperation Group and CSIRTs Network? It is noted there is no reference to Article 35 in Article 12 in regard to the Cooperation Group. Why is a similar requirement not being made in regard to the Cyclone Network?

Why is there not a reference to Article 15 and the reports from ENISA in regard to the review process?

**Article 36**

Can the Commission further elaborate in regard to paragraph 4 on how it intends to consult experts designated by all of the Member States?

Does the Commission intend to undertake public and stakeholder consultations prior to adoption of delegated acts? If so, would such consultations take place before, during or after convening of experts from the Member States?

**Article 37**

Can the Commission elaborate on the differences between Article 22 in the NIS Directive and this Article as regards 'Committee Procedure' other than paragraph 3 on written procedure? In particular it is noted that there is no name given to the Committee.

**Article 38**

What is the reasoning for the transposition timeframe being set at 18 months? This is less than the transposition timeframe provided for the existing NIS Directive and Member States struggled with that timeframe. Given that this is much more ambitious than the existing Directive, why was a period of 2 years not considered?

**Article 39 and 40**

What are the precise impacts of the repeals?

In particular how is Recital 49 consistent with Article 40? How can transposed national legislation in regard to Articles 40 and 41 of the EECC continue to be applicable once the NIS2 Directive is transposed into national law?

**MALTA**

**Article 36.1**

**Text:**
The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

**Comments:**
Which authority within the Commission would be enabled to adopt the delegated acts.

**Article 36.3**

**Text:**
The delegation of power referred to in Articles 18(6) and 21(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

**Comments:**
The ability to revoke raises concerns as to importance of the delegated acts. Would be helpful to provide context necessitating the inclusion of this provision.

**Articles 39 and 40**

**Text:**
Article 19 of Regulation (EU) No 910/2014 is deleted.
Articles 40 and 41 of Directive (EU) 2018/1972 are deleted.

**Comments:**
Article 39 and 40 of the NIS2 Directive are expected to replace the security-related provisions contained in the eIDAS Regulation and European Electronic Communications Code respectively.

Malta is not convinced that repealing the above mentioned provisions of these two laws will translate into a better and more efficient regulation in the respective sectors.

**NETHERLANDS**

*Disclaimer: The Netherlands is still carefully studying the NIS 2.0 proposal and is in the process of establishing its position on the content of the proposal. The list of comments and questions about the proposal below is preliminary and may be expanded in the future.*



**Article 35 Review**
Will the Commission also take into account the strategic cooperation on supervision and enforcement as one of objects of the periodic review?

**Article 36 Exercise of the delegation**
Could the Commission further how the delegation process would work in practice, and which experts (public as well as private) would be consulted during the process?

**Article 38 Transposition**
Given the far-stretching consequences of this proposal for national legislation and the consequences for national authorities and entities, including their budgets, the 18 months proposed for transposition is not feasible. The Netherlands would propose extending the time for implementation to at least 24 months.

**Article 39 Amendment of Regulation (EU) No 910/2014 (eIDAS)**

- Could the Commission explain its reasoning behind the proposal to remove article 19 of the eIDAS regulation, instead of using the *lex specialis*-clause under article 2 (6) for eIDAS?
- Could the Commission give its assessment on what removing this provision of sectoral legislation (eIDAS) will mean for legal clarify for the sector of Trust Service Providers, because their obligations and supervision on those provisions will be spread over multiple EU legal instruments?
- Could the Commission clarify how liability is arranged when security requirements are removed from the eIDAS regulation? Liability is currently arranged in art. 14 of the eIDAS regulation, which depends on the security requirements of article 19 in this regulation.
- Could the Commission share its assessment on whether removing the security provision from the eIDAS regulation will not in effect lead to less harmonisation between Member States in the internal market of Trust Service Providers, since NIS2 is a directive that Member states can implement and interpret differently? The Netherlands has concerns that this could lead to a less coherent approach with negative consequences for the single market.
- Could the Commission clarify its proposal to include non-qualified Trust Service Providers in the list of essential entities, hereby leading to ex ante supervision on those entities instead of only ex post as under the eIDAS Regulation? How does this relate to article 17 (3) of the eIDAS regulation where only ex post regulatory tasks are conferred to the supervisory body in regard to non-qualified Trust Service Providers?

- Could the Commission clarify whether no important elements of article 19 of Regulation (EU) 910/2014 will be lost, because NIS2 focusses solely on the security of network- and information used to provide essential or important services whereas article 19 focusses on the secure provision of Trust Services in its entirety. For example, through adequate identification of persons to whom certificates are offered and physical security and transportation of physical means? The Netherlands is concerned that important elements of the security requirements in eIDAS might be lost by removing this article in its entirety.
- Could the Commission clarify how mutual assistance under article 18 of the eIDAS regulation and article 34 of NIS2 will relate to each other and will function in practice?
- Could the Commission clarify how supervision under NIS2 and the eIDAS regulation (section 2) will coincide, given that eIDAS supervision by a national supervisory body is limited to trust service providers established in the territory of the designating Member State, whereas NIS2 does not have a similar geographic limit for its jurisdiction?
- Could the Commission clarify how the current supervisory practice under the eIDAS regulation will be impacted by NIS2, since it seems that in the new situation supervisory authorities will have two applicable legal basis for supervision and enforcement?
- Could the Commission clarify to what extent the notification requirements under NIS2 differ from eIDAS, particularly in regard to what types of incidents have to reported and to which authorities (competent authority and/or CSIRT)? It seems that incidents not related to network- and information system would have to be reported under article 19 eIDAS, but not under NIS2. Also, NIS2 offers the possibility for Member States to report notifications only to the CSIRT, whereas eIDAS prescribes notification to the supervisory body.
- Could the Commission reflect on the transition gap that would arise when adopting NIS2 and removing article 19 of the eIDAS regulation? The period for national implementation of NIS2 is currently set at 18 months, while in between there would be no security requirements in regard to Trust Service Providers.
- In light of the questions raised above, the Netherlands has grave concerns regarding the removal of article 19 through the proposed amendment in article 39 of NIS2. In the current assessment of the Netherlands, there seem to be a number of potential (unintended) negative consequences of removing this article, while the problem that this article aims to solve seems unclear. Any problem in the application of the regulation could also be dealt with in the revision of the eIDAS regulation, which is currently under preparation by the Commission.

**Article 40 Amendment of Directive (EU) 2018/1972 (EECC)**

- Could the Commission explain its reasoning behind its proposed approach to remove article 40 and 41 of Directive 2018/1972, instead of using the *lex specialis*-clause under article 2 (6) of the proposal for of public electronic communications networks or of publicly available electronic communications services?

- Could the Commission give its assessment on the consequences of removing this provision of sectoral legislation (Regulation (EU) 2018/1972) for legal clarify for the sector public electronic communications networks or of publicly available electronic communications services?
- Could the Commission reflect on whether all aspects that are of importance for the security and continuity of public electronic communications networks or of publicly available electronic communications services that are currently covered by article 40 Directive (EU) 2018/1972 are also covered by article 18 of NIS2? For example, having enough capacity to prevent congestion and availability of network components and/or equipment.
- Could the Commission clarify whether competent authorities under NIS2 will have the power to obtain the assistance of CSIRT in the performance of their duties, as laid down in article 41 (4) of Directive (EU) 2018/1972?
- Could the Commission clarify why providers of public electronic communications networks or electronic communications services that do not have a (main) establishment in the Union are not required to designate a legal representative?
- Could the Commission clarify whether services that are related to the essential services of public electronic communications networks or of publicly available electronic communications services are also within scope of NIS2, for example voice mail services, data storage services or streaming services?
- Could the Commission clarify its opinion on the potential transition gap that is to arise when adopting NIS2 and removing articles 40 and 41 of Directive (EU) 2018/1972. The implementation period for NIS2 is currently set at 18 months, while the original European legal basis for the security requirements in national law would be removed and substituted for a different one that might have different legal implications.

**POLAND**

**Art. 35**

1) PL sees a need to indicate in the second sentence also the implementation of norms on jurisdiction and functioning of the mutual assistance mechanism.

**Art. 39**

1) PL is in favour of including the eIDAS cyber incident reporting to the NIS2 framework as it reduces the silo approach to the incident reporting. Trusted services are more and more provided online, therefore ensuring high level cybersecurity is of crucial importance.
2) There is a need for thorough analysis of the necessary changes to eIDAS following the inclusion of TSPs to the NIS2. Could the EC explain and share the analyses on if and how the removal of art. 19 eIDAS impacts other provisions of eIDAS (for example art. 13, art. 24).
3) It is worth noting also that NIS2 and eIDAS incident reporting schemes differ as to the scope. QTSP's as per Article 19 are expected to manage the "*security of the trust services provided*" whereas Article 18 of NIS 2 is focused on managing the "*security of network and information systems*" which is a subset of the security obligations of QTSP's under the eIDAS Regulation.

   It might be the case that with NIS 2 reporting certain relevant TSP incidents will not be covered by the obligation of notification, for example the procedures of issuing certificates, the production and distribution of physical tokens, the identification of natural persons. Could the EC present its views on that?
4) It should be noted that „supervisory body" from eIDAS is not the same as „competent authority" from NIS2. Different scenarios could emerge and there should be clarity on that. Would there be two authorities, one being the CA (for measures in art. 18 NIS2) and the other the supervisory body (for ex ante supervision of qualified TSPs - article 24 eIDAS and ex post supervision of non-qualified TSPs)? Could supervisory body be also the CA? The relations should be clear to avoid any conflict of competences.
5) The NIS2 would be applicable to both qualified and non-qualified TSPs regardless of their size. This represents a different approach in the supervision of non-qualified TSPs, given that under eIDAS regulation they are subject to a light-touch ex-post regulation. The NIS2 proposal implies that the authority will supervise the security obligations of non-Q TSPs ex-ante, which may have an important impact for these companies (a number of them are small and micro enterprises and this might represent a disproportionate burden) and also for the competent authority. We would like to hear more about the rationale behind this switch of approach for non-Q TSPs and know if the Commission has assessed the specific impact in the trust services sector?
6) Another issue is the cross border cooperation. What would be the relations of SPOCs and mutual cooperation (art. 8 and 34 NIS2) to art. 18 eIDAS (mutual assistance of supervisory bodies)?

7) There is also a formal issue. If NIS2 deletes art. 19 eIDAS, in the NIS2 implementation period, there will be no legislation in the scope covered by art. 19 eIDAS. There will be a legal loophole. Could the CLS present it's opinion in this respect?

8) The NIS2 negotiations should take into consideration the results of eIDAS review, to be presented in the following months.

9) We would strongly encourage the EC to present a working document explaining all the concerns, including presented above, on the consequences of including the TSPs to NIS2. This should also be discussed with experts in the art. 19 eIDAS group and FESA.

10) We would encourage EC to present a working document explaining possibility to consolidate incident reporting from all regimes while respecting different scope, identifying relevant reporting entities and presenting timeframe.

**Art. 40**

1) There is also need for thorough analysis concerning the deletion of art. 41 and 41 of directive 2018/1972. We would also encourage the EC to present a working document on that. The new framework should take into account the best practises and experience gathered in the telecommunication sector. For example it is necessary to clarify if ENISA will still publish the recommendations on technical measures.

**SLOVENIA**

**Article 40**

We ask for further information about the relation between NIS 2 and EECC? Can you please share again the findings of the impact assessment of the NIS 2 for the current EECC regime in relation to the Articles 40 and 41 of Directive (EU) 2018/1972 (EECC)? While welcoming NIS 2 as the horizontal legislation for cyber security, there is a concern about a possible fragmentation of the regulation of the electronic communications market.

**SPAIN**

| ARTICLE | JUSTIFICATION FOR THE SPANISH PROPOSAL |
|---|---|
| **Article 35**<br>Review | The present Directive is in many ways an experiment in uncharted territory. The current article states that the report on the review of the functioning of this Directive "*shall in particular assess the relevance of sectors, subsectors, size and type of entities*". We believe this report and review should be far more ambitious, and concentrate on five more aspects: level of effectiveness in attaining cybersecurity (estimated in euros saved), level of compliance, level of supervision attained, costs of supervision on supervising bodies and costs on the supervised entities. |
| **Article 36**<br>**Exercise of the delegation** | |
| **Article 37**<br>**Committee procedure** | |
| **Article 38**<br>**Transposition** | Although this NIS 2 is an update of NIS 1, the 18-month deadline for transposition may be short, considering the precedents in Spain of NIS1, and the delay, for example, in approving the regulations, in the processing of the law or modification of the current ones, etc. We request a period of 24 months |
| **Article 39**<br>**Amendment of Regulation (EU) No 910/2014** | **We request the elimination of this Article**<br>**Trust services should be eliminated as a subsector of essential entities in application of the principle of lex specialis, as in the current Directive**.<br>The current proposal seeks to repeal the entire supervisory mechanism instituted by Regulation (EU) No 910/2014 on trust services (eIDAS Regulation), including these as a subsector of "important entities". This raises three serious problems.<br>First, the scope of assets to be supervised in the eIDAS Regulation is broader than that of the proposed Directive NIS2. The proposal is limited to the security of the information systems and networks that the entities use in the provision of services. The eIDAS Regulation supervises all dangers with an impact on the security of the trust service, from the Registration Authority (normally its network infrastructure will be from another company) to the procedures executed in the user environment and the user environment and its communications. For example, it also supervises the provision of the service itself (eg issuance of the certificate), as well as the use of the products (eg that certificate) that would be within the scope of the user. This derogation implies a removal of this security supervision.<br>The proposal refers only to ""the security of network and information systems which those entities use in the provision of their services"". It does not cover the security of issued certificates |

| | |
|---|---|
| | or smart cards, which do fall within the objective of article 19 eIDAS. ""Qualified and non-qualified trust service providers shall take appropriate technical and organizational measures to manage the risks posed to the security of the trust services they provide."". The security imposed by art. 19 of the eIDAS Regulation to trust services has a greater scope than the physical and logical infrastructures of the provider, to which the NIS2 proposal is limited. Under the proposal, an incident as serious as ROCA would not be reported.<br><br>Second, the inclusion of the sector in the proposal gives the Member States the possibility to demand different technical security measures, when the eIDAS Regulation and its implementing acts impose common ones. It is precisely this fragmentation that motivated the conversion of the Electronic Signature Directive into the current eIDAS Regulation. The NIS2 proposal, in its article 18 (Cybersecurity risk management measures) places in the hands of the MS the cybersecurity measures that essential and important entities must take to ensure a level of security of their networks and information systems. The NIS2 only imposes very vague general guidelines on EMMs in this regard (""The measures referred to in paragraph 1 shall include at least the following: ..."""). This is not the case in the eIDAS Regulation. Article 24 2 of eIDAS says, for example, in section e) that suppliers must use reliable systems and products that are protected against any alteration and that guarantee the security and technical reliability of the processes they support. And section f) says that they have to use reliable systems to store data.<br><br>Third, the proposal applies the toughest supervisory regime to all companies in the sector, even small and micro-companies. The eIDAS Regulation has an ex ante supervision regime, similar to that of ""essential entities"", for qualified trust service providers and an ex post, similar to that of ""important entities"", for non-qualified ones. This follows the unanimous criterion of the supervisory authorities of the MS, who judge this level of supervision adequate to the relative importance of each provider. This tightening would have a pernicious effect on companies in the sector, undermining their already diminished competitiveness vis-à-vis suppliers from outside the EU." |
| **Article 40**<br><br>**Amendment of Directive (EU) 2018/1972** | **This article only may stand if Micro and small companies of communications infrastructure and communications services operators should be categorized as ""Important Entities"" instead of ""Essential Entities" (article 2).**<br><br>Article 2, paragraph 2, letter (a), (i) establishes that all operators of networks and services and electronic communications will fall within the scope of the Directive regardless of their size and therefore a supervisory regime will be applied to them. ex ante since they are considered Essential Entities according to point 8 of Annex I.<br><br>In relation to this point, the following provisions should be |

| | |
|---|---|
| | highlighted:<br><br>• The general principle of exclusion in Article 2, section 1 leaves micro and small companies (less than 50 employees or € 10 million in turnover) out of the scope of the regulation. The objective of this article, as detailed in the impact analysis, is to reduce the administrative burdens and the costs of complying with the obligations imposed by the Directive.<br><br>• On the other hand, article 30 of the directive, establishes an ex post supervision regime applicable to Major Entities, lighter and more proportional, differentiating itself from the ex ante supervision regime that applies to Essential Entities, which is more exhaustive and of routine character. In this way, as argued in Recital (70), a more proportionate and lighter balance is achieved in the supervision of important Entities, so that they do not have to systematically document compliance with respect to risk management. of cybersecurity and a reactive mechanism (ex post) is implemented in its place by the Competent Authorities once the breach of the directive is evidenced without, therefore, having the general obligation to supervise this type of entity.<br><br>In our opinion, a balance can be achieved between both provisions (articles 2.1 and 30) that would be applicable to the case of small telecommunications operators. In this way, micro and small telecommunications companies would remain within the scope of the Directive, taking into account their importance as a basic constituent element of the Digital Infrastructure, although they would be included in the ex post supervision regime that would guarantee a overall compliance with the directive while minimizing administrative burdens.<br><br>The increased burdens that the approval of the proposal would entail would be especially burdensome in the case of Spain, where there are more than 400 registered small local telecommunications operators, which barely have the material, administrative, economic or personal means to carry out the exhaustive ex ante requirements imposed by the directive in its article 29.<br><br>Considering all the foregoing, we propose that micro and small companies of communications infrastructure and services operators as defined in article 2, paragraph 2, letter (a), (i), remain within the scope of application of the directive, but not under the ex ante supervision regime, but rather under the ex post supervision regime, hereinafter categorized as Major Entities instead of Essential Entities. |

| | |
|---|---|
| **Article 41**<br>**Repeal** | |
| **Article 42**<br>**Entry into force** | |
| **Article 43**<br>**Addressees** | |

**SWEDEN**

**Article 36**

SE would like the Commission to explain the need to adopt delegated acts and to elaborate on the reasoning for choosing delegated acts instead of implementing acts.

In Article 36 (4) it is stated that the Commission shall consult experts designated by each Member States – what status and significance will these consultations have? Will Member States have an actual impact in the development of delegated act?

**Article 38**

SE considers that 18 months to adopt and publish the laws, regulations and administrative provisions necessary to comply with this Directive is too short a time. This proposal is comprehensive and affects significantly more sectors than the current NIS Directive why more time will be needed.