Council of the European Union
General Secretariat

Interinstitutional files:
2020/0359(COD)

Brussels, 19 May 2021

WK 6380/2021 ADD 2

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
CSC
CSCI
PROCIV

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
N° Cion doc.:	14150/20 [COM (2020) 823 final]
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: interaction with sectoral legislation - Comments by CY and MT delegations

Delegations will find in Annex comments by CY and MT delegations on the above-mentioned subject.

TABLE OF CONTENT

CYPRUS

Article 2: We believe that the criteria set in Article 2(1,2) are not taking the different needs of Member States into consideration. In Cyprus, we have a significant proportion of micro and small enterprises, and therefore the size criterion of Article 2(1) may lead to a considerable number of entities that will be excluded from the scope of the Directive, or included in the scope of the Directive based on the provisions of Article 2(2). Thus, we believe that a national risk assessment would be a better approach to determine essential and important entities since it ensures proportionality. An alternative approach would be to alter the provisions of Article 2(1) by setting a relative threshold proportionate to the population of each Member State. This approach would help bigger Member States to limit the number of entities that fall under the scope of the directive and smaller Member States to include entities that are considered critical, regardless of their size.

Additionally, Article 2(2) declares that the Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission. We would like to ask how the Commission intends to use this data and whether there will be any feedback provided back to the Member States.

Article 11: We would like to have a more detailed interpretation of the term "near misses". We have considered the definition provided in Paragraph 39 of the preamble, but we would like to have a more detailed specification. Additionally, we would like to have some more information regarding the management and sharing responsibilities for near misses, for both the competent authority and the essential/important entities.

Article 20(4.a): While we can accept the maximum period of 24 hours provided to essential and important entities to submit the initial incident notification, we believe that the period could be shortened.

Article 20(4.b): We believe that the intermediate report should be submitted whenever the essential or important entities consider that a significant change has emerged since the previous submission, and not only upon request of the competent authority.

Article 20(9): We would like to have a clarification regarding the monthly summary report of anonymized and aggregated data on incidents, significant cyber threats and near misses, which will be provided to ENISA. Specifically, we would like to ask whether it would be acceptable to use software tools to prepare the report in an automated way.

Article 20(11): Article 20(11) states that the Commission may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted, and the cases in which an incident shall be considered significant. We would like to ask under which circumstances and for which reasons the Commission may alter the specific provisions, considering the extra overhead to transfer individual changes to national legislation and operational processes.

Article 23: We would like to express our agreement concerning the provisions of the specific article. We agree that TLD registries and the entities providing domain name registration services for the TLD should be able to maintain accurate and complete registration data and guarantee their integrity and availability.

Article 24: Article 24(2) states that entities referred to in Article 24(1) shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. We would like to ask which entity will evaluate the validity of the information provided by the entities regarding the declaration of their main establishment, and based on which criteria the evaluation will be conducted. We believe that it would be beneficial to establish a specific procedure for the evaluation. Moreover, we believe that cooperation between the Member States should be ensured, to guarantee the effective implementation of this provision.

Article 25: Article 25 states that ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1), and forward the relevant information to the single points of contacts of the Member States. We would like to have some clarifications regarding how this information will be utilized by ENISA and the Member States.

Article 29 & Article 30: According to Article 29(4.h) and Article 30(4.g), competent authorities can order essential and important entities to make public aspects of non-compliance with the obligations laid down in the Directive in a specified manner. We would like to have some clarifications regarding the specific process and the type of information that will be revealed.

Article 29: We agree with the provisions of this article, as they ensure that the competent authorities will have the necessary power to conduct their supervisory responsibilities.

Article 30: Article 30(1) declares that the Member States should ensure that the competent authorities can take action for ensuring the compliance of important entities, through ex-post supervisory measures. We would like to ask why there is not a provision for the enforcement of ex-ante measures to important entities as well, and whether the enforcement of ex-ante measures is in the jurisdiction of the Member States according to the provisions of Article 3 (i.e. whether the Member States can impose ex-ante supervisory measures to important entities, which are considered beneficial for ensuring a higher level of cybersecurity). Moreover, we would like to have a definition of "ex-post", which will determine what would trigger the enforcement of ex-post supervisory measures.

MALTA

The objectives of the security provisions in the Commission Proposal [COM(2020) 823 final] "NIS2" are different from those in Directive (EU) 2018/1972 "EECC" and Regulation (EU) No 910/2014 "eIDAS". The inclusion of security related legal obligations imposed on providers of public electronic communications networks and or services, and trust service providers in relation to NIS2 should only act as a 'safety net' when and if the rules found in the EECC and eIDAS fail to regulate a specific situation. In view of the fact that the primary objectives of NIS2 are meant to implement measures ensuring a high common level of cybersecurity across the Union, aspects of the concurrent development of internal competitive markets in electronic telecommunications are absent and this may be detrimental to respective markets. To that end, the NIS2 must not repeal the rules found in the EECC and eIDAS and these legislative instruments should complement each other to ensure consistency between organisations that provide essential services.

With reference to the EECC

Repealing provisions within the EECC may have a significant impact on the operational aspects for the rest of the provisions within the same legislative tools. This may lead to shortcomings in the implementation and support of legislative articles such as the Emergency Communications and the Single European Emergency Number as well as Public Warning Systems. Further to this, we are concerned that a change in competent authorities will be required to take into account the variances between the objectives of the NIS2 and those of the EECC. As a result of this, the regulation of security of ECS and ECN will function differently.

Adaptation to the EECC security provisions in order to align with the wider scope of application in the NIS2 Directive, can result in significant implementation complexities both for competent authorities as well as network or service providers. An example is the replacement of the terms "electronic communications and services" with the term "security of networks and information systems" in the NIS2 Directive. In addition, the adapted NIS2 proposals may extend the regulatory remits of the measures proposed for both ex-ante and ex-post; the outright implementation of such measures may however be disproportionate towards small scale service providers.

The provisions within the EECC were adopted following lengthy consultation processes that were held within the aim and scope of the respective legislative tools; the primary objectives of the NIS2 Directive were, at the time being, out of scope for such consultations and discussions. Furthermore, the Joint Communication on the EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final) does not show any shortcomings with regard to the implementation of Article 13a which justify the removal of Art 40 from the EECC. This reiterates further that the security approach adopted so far through the concurrent implementation of the current NIS Directive, FRAMEWORK Directive (as adopted in the EECC) and eIDAS appropriately address the security requirements for the relevant markets.

With reference to eIDAS

The eIDAS landscape is different from which the current NIS Directive is addressing. The NIS Directive is more oriented to the underlying network infrastructure and is of a more general nature. In eIDAS, further consideration is given to alternate areas of the Trust Service Provider's (TSP) operation such as customer enrolment procedures and data protection measures. eIDAS delves into person identification - this is not related to cybersecurity per se but is of crucial importance to the overall security posture of a TSP. Specific national regulations allow for remote person identification by QTSPs (Qualified Trust Service Providers) and these regulations include very specific security requirements that go beyond network and information systems security. QTSPs as per Article 19 of eIDAS are expected to manage the "security of the trust services provided" whereas Article 18 of the NIS2 is focused on managing the "security of network and information systems" - this is but a subset of the security obligations of QTSPs under the eIDAS Regulation that are also bound to consider the "softer" elements of security more explicitly.

The NIS2 also includes ex-ante supervision of non-qualified TSPs. This is different from eIDAS whereby non-qualified TSPs may be subjected to ex-post supervision as required. This may put further load on Supervisory Bodies (SBs), particularly in small Member States and also additional load on non-qualified TSPs that tend to be smaller operations when compared to QTSPs.

Splitting the regulation with a Directive is also concerning when it comes to supervision on the ground. Article 24 of eIDAS stipulates the security requirements QTSPs need to adhere to, Article 19 is a feedback mechanism for Supervisory Bodies (SB) to compare the QTSP's claimed position with a real life picture. Repealing Article 19 from eIDAS will result in the elimination of a useful tool for the SB to properly close this feedback mechanism.

With reference to the Commission Proposal on digital operational resilience for the financial sector "DORA"

Both legislative proposals aim to achieve a mutual level of compatibility. DORA has been proposed as a lex specialis vis-a-vie NIS2. There may be instances whereby particular entities falling within the scope of NIS2 will be determined to be critical ICT Third Party Service Providers under DORA. We understand that in this case, while both proposals apply to such entities, DORA will apply in respective instances and in accordance with recital 13 of the NIS2 proposal.

For all the reasons stated above, Malta disagrees with the repealing of security-related provisions in the respective sectoral legislation. Current measures in such legislation should remain unchanged. Nevertheless, Malta would welcome mandatory communication and collaboration between the sectoral competent authorities and NIS2 competent authorities in the Member States to be included within the proposed NIS2 Directive.