9 June 2021

EBF key messages on the proposal for a Revised Directive on Security of Network and Information Systems (NIS2)

The EBF welcomes the European Commission's review of the Directive on Security of Network and Information Systems (NIS2).Ensuring high levels of cybersecurity across the EU currently poses one of the biggest challenges, affecting citizens, customers, and businesses. Cyber threats are by nature not limited to one sector and have the potential to arise from and expand to any field of economic activity, entailing possibly immense repercussions for those affected. As a result, adopting cybersecurity measures which target entities across sectors and ICT service providers is crucial.

Some of the sectors included within the scope of NIS2 are also covered by sector-specific rules, as in the case of the financial sector where, in addition to a number of existing policies (such as the EBA Guidelines on ICT and security risk management), the Commission has already published a proposal for a Regulation on digital operational resilience for the financial sector (DORA[1]). The Regulation includes provisions on ICT risk management, cyber incident reporting, digital operational resilience testing, information-sharing arrangements and managing of ICT third-party risk.

Given the extent of the DORA provisions, we welcome its function as *lex specialis* to NIS2, thereby providing legal certainty to banks in terms of obligations. However, some elements of the current NIS2 text require clarification in order to ensure this certainty.

1) DORA's function as *lex specialis* to NIS2 should be stated clearly and unconditionally

It becomes evident from the text of the NIS2 proposal that it is intended to exclude from its provisions the entities that are already subject to sector-specific cybersecurity legislation. Specifically for the financial sector, DORA is mentioned in the NIS2 explanatory memorandum as a proposal which will be considered as *lex specialis* to NIS2 once both acts have come into force.

Article 2(6) of the proposal stipulates that its **provisions on cybersecurity risk management, incident notification, as well as supervision and enforcement *shall not* apply to entities that are under its scope and already covered by sector-specific legislation**. This indicates a clear intent to address existing overlaps and potential duplication in EU legislation. However, the wording of this Article ("where those requirements are at least equivalent in effect to the obligations laid down in this Directive") **creates uncertainty on which provisions are to be applied for these entities, as**

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

the equivalence in effect of the NIS2 provisions could eventually become a matter of legal interpretation.

As the legal notion of *lex specialis* concerns the relation of the special vis-à-vis the more general with **the equivalence in effect** not being a precondition for its function and, given that the inclusion of this requirement **would only cause legal unclarity on which provisions apply and may impose further obligations to specific entities covered by sector-specific legislation, we recommend that this wording be removed**. This would address all inconsistencies arising from its inclusion, such as:

- Applying to banks the NIS2 enforcement provisions instead of those in DORA in case the latter are not deemed equivalent to the former. In that occasion, the supervision provisions in DORA would still apply, resulting to the paradox of the enforcement authorities being different from the supervision ones.
- Concluding that reporting requirements under DORA are not equivalent to those in NIS2, as only the latter includes provisions on reporting cyber threats. This would lead to entities under the scope of DORA having to also adhere to reporting under NIS2, even though this is not the proposal's intended outcome.

Additionally, the EBF would welcome a **specific in-text mention of DORA as *lex specialis*** legislation to be applied when it comes to provisions about cybersecurity risk management, incident notification, supervision and enforcement, explicitly exempting banks from the obligations set out in NIS2 and overlapping with those in DORA. This would further add to addressing the uncertainty on which requirements and to what extent are to be applied, as explained above.

Proposed amendments:

Recital 12:

"Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents ~~**or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive**~~, those sector-specific provisions, including on supervision and enforcement, should apply.(…)"

Article 2(6):

"Where provisions of sector–specific acts of Union law, **including Regulation (EU) XXXX/XXXX of the European Parliament and of the Council [the DORA Regulation]**, require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents ~~**or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive**~~, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply."

2) The requirement to notify competent authorities and recipients of services on cyber threats creates more problems than those it intends to address

In addition to reporting cyber incidents that have a significant impact on the provision of the entities' services, the proposal includes an **obligation to report on any identified significant cyber threat that could have *potentially* resulted in a significant incident.** Such a requirement **does little to contribute to improving cybersecurity and should be removed**, as in practice it would rather **overwhelm authorities** by the volume of notifications, while creating an **unnecessary compliance burden to entities**.

In addition, given that NIS2 defines "cyber threat" by using the definition provided in the EU Cybersecurity Act[2], it is based on the element of potentiality and is therefore too broad. This will create extensive obligations and a large number of events to be reported, leading to **notifications which would not be necessarily linked to the actual risk that these threats effectively posed**.

At the same time, **the obligation to notify the recipients** of the entities' services of the existence of a threat that can potentially affect them and of measures or remedies to be taken in response also **seems problematic**, **especially in the case of financial institutions.** Such notification would significantly **undercut the trust of users in EU financial services** and could even lead to a financial stability incident.

Constant negative signals about occurrences that may not materialize distort the perception of the actual safety level provided by the financial entity, entailing a much larger risk of bank runs due to loss of public or market confidence in cybersecurity. Also, it is not clear what information could be provided by financial entities that their users could meaningfully act upon. The only action which a bank client could reasonably take would be to withdraw their funds from the financial entity or to disconnect in the case of a correspondent and both of these are likely to result in a greater risk to financial stability than the identified cyber threat.

Another unwanted result of such notification requirements is that it would deliver an **instrument to threat actors to abuse the process** and could be detrimental to counterintelligence operations that might be underway, shifting the need for achieved impact over to the much easier accomplished threat creation.

Incident reporting and exchanging information on the existence of threats are two distinct procedures in the efforts to ensure high levels of cybersecurity. Cyber threat information sharing arrangements among entities is indeed a useful tool and is supported by the EBF, however this should be facilitated on a voluntary basis among trusted circles, as it is already the case under Chapter V of NIS2.

Proposed amendments:

Article 20 (2) subparagraph 1:

[2] EU Cybersecurity Act, Article 2(8)

"~~**Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident.**~~"

Article 20 (2) subparagraph 2:

"~~**Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.**~~"

3) The EBF calls for enabling the establishment of meaningful and voluntary cyber threat information-sharing arrangements among trusted circles

As described above, NIS2 considers DORA as *lex specialis* vis-à-vis its provisions on cybersecurity risk management, incident reporting, supervision and enforcement. Additionally to the exemption from those requirements explicitly mentioned in Article 2 paragraph 6, recital 13 of the proposal extends the exclusion of financial entities from the NIS2 provisions on information sharing. However, this exemption is not retained in the main text of NIS2. This inconsistency creates **uncertainty on whether financial entities are also exempted from the respective information sharing provisions** of the proposal and it should be addressed.

In principle, the provisions in the proposed Directive for facilitating the establishment of cyber threat information sharing arrangements among essential and important entities are welcome and in line with calls from industry. The banking sector would benefit from the exchange of information with other non-financial entities on a voluntary basis regarding threats that have affected other sectors and could potentially also hit financial entities. Nonetheless, some requirements included in these provisions can hinder the establishment of meaningful info-sharing arrangements.

Specifically, **involving public authorities in cyber threat information-sharing** mechanisms that are meant to be a tool for the industry and for timely exchange of crucial information to efficiently identify, prevent and address threats within trusted circles **does not seem to be opportune**. There is need to clarify the rationale of the public authorities' involvement, as well as the conditions under which this would be realized. Authorities in their capacity as regulators, overseers and/or supervisors should not have access to the info-sharing network. Regulatory reporting on cyber incidents and data breaches should be outside the scope of the intelligence sharing within the European community. The involvement of public authorities could be considered in the form of periodic (quarterly or biannually) meetings as a path to foster collaboration and transparency, maintaining a highly trusted cybersecurity ecosystem and enforcing the Public-Private Partnerships (PPPs) that have been created over the years.

It is not clear what is the objective of introducing an **obligation for essential and important entities to notify competent authorities** of their participation in and withdrawal from information sharing arrangements, and it **creates a new and unnecessary burden**, while also **jeopardizing the voluntary nature** of such schemes. There could be strategic considerations behind the decision to participate in info-sharing schemes, and the arrangements among entities could be large in terms of number, or dynamic in terms of validation/cessation. Therefore, the notification requirement should be removed.

Additionally, the proposal needs to provide for a **clear legal basis in the EU data protection** legislation by including a specific mention that directly links the processing of data under NIS2 with the lawfulness of processing under GDPR. When it comes to establishing such schemes, this is essential in order to lift existing obstacles of legal uncertainty that often impede efficient cyber threat information-sharing, especially when it involves personally identifiable information (PII).

The EBF is of the view that information-sharing should be implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, such as via CERTs or using MISP.

Proposed amendments:

Article 26(3):

"~~Member States shall set out rules specifying the procedure, operational elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. Such rules shall also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).~~"

Article 26(4):
"~~Essential and important entities shall notify the competent authorities of their participation in the information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.~~"

For more information:

Alexandra Maniati
Director of Innovation & Cybersecurity
a.maniati@ebf.eu

Dimos Karalis
Policy Adviser – Innovation & Cybersecurity
d.karalis@ebf.eu

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.1 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu