Japan Business Council in Europe

18 March 2021

Revised Directive on Security of Network and Information Systems (NIS2)

JBCE's position

Japan Business Council in Europe (JBCE) welcomes the proposal for the Revised Directive on Security of Network and Information Systems (NIS2). It supports the Commission's efforts to address new challenges in the cybersecurity threat landscape in Europe. To contribute to a more resilient Europe, JBCE members would like the European Commission to consider the following recommendations:

Harmonisation

JBCE encourages the co-legislators to work towards a maximum harmonisation framework to provide legal certainty and to lower implementation costs[1]. This is particularly important for entities operating in several Member States. Full harmonisation would ensure that incident notification thresholds and approaches to mandating certification are the same across EU Member States and that entities are not fined for the same breach under both NIS2 and the GDPR.

It is particularly important that full harmonisation applies to the following articles: Article 5 (national cybersecurity strategy), Article 18 (risk management measures), Article 20 (reporting obligations), Article 21 (use of European cybersecurity certification schemes), Article 31 (administrative fines) and Article 32 (infringements entailing a personal data breach).

Alignment with EU law and other initiatives

JBCE believes that the relationship between NIS2 and the wider legal framework (Cybersecurity Act) needs to be further explained. The relationship between the EU Cybersecurity Strategy and the national cybersecurity strategies that Member States are obligated to adopt under Article 5 should be clearly articulated to avoid overlaps and conflicts.

Scope

Greater clarity is needed on the scope of the proposed NIS2. The newly created list of essential entities includes the category '*Digital infrastructure*', which comprises '*content delivery network providers*', '*cloud computing service providers*' and '*data centre service providers*'.

Moreover, it is difficult to understand the justification for including different types of manufacturers under the *'important entities'* category. If the aim is to ensure the continuous supply of devices, components and services to essential entities, then this is covered already under the supply chain security obligation in Article 18(2)(d). It is unclear why manufacturers of – for instance – wearables or TVs should fall under the extensive risk management and notification obligations enshrined in Articles 18 and 20. Therefore, JBCE suggests removing manufacturers from the list of important entities provided in Annex II to the proposed Directive.

The NIS2 proposal and its Annex II also do not provide details on the classification of economic activities. The NACE classification could lead to fragmentation between Member States in how economic activity

[1] NIS 2 impact assessment expects to be significant as to lead to 22% increase of IT security spending over the 1st years of its implementation

classification is defined; therefore it is essential to have a unified classification and to avoid unnecessary confusion.

JBCE also suggests that the Directive should provide clear guidance on its geographical jurisdiction, regardless of whether entities are included in scope only under the essential entities list or under the important entities list. The Directive should establish a one-stop-shop system for entities which operate in more than one Member State.

Cybersecurity risk management measures

According to the proposal, essential and important entities shall take appropriate and proportionate technical and organisational measures to manage cybersecurity risks. It is important that existing international standards (e.g. ISO 27001) would be the basis for the technical and methodological specifications of the risk management measures that entities must take under Article 18(2).

Definitions

When defining '*cybersecurity*' the proposal refers to the definition given under the Cybersecurity Act. Still, this definition doesn't clarify which processes and services exactly fall under the scope of the Directive.

Certification

Article 21(1) provides the possibility for Member States to compel essential and important entities to certify certain ICT products, services and processes under specific European cybersecurity certification schemes adopted through the Cybersecurity Act. This provision may create discrepancies if Member States rule differently on the lists for certification and would impose significant confusion and administrative burden for the operators which provide services in several Member States. JBCE believes it is too early to introduce mandatory requirements for schemes that are still being developed and that are meant to be voluntary, and while there is not a unified EU approach on which ICT products, services and processes need to be certified.

Supply chain security

Article 18(2)(d) requires essential and important entities to emplace supply chain security measures, including aspects concerning relationships between each entity and its suppliers or service providers (such as providers of data storage and processing services or managed security services). JBCE suggests there is clarification that these measures should only apply to tier 1 suppliers, providers and recipients, and not to the entire supply chain.

Article 20 paragraph 2 foresees that entities shall notify, without undue delay, the recipients of their services potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. It should be clarified that these requirements are for tier 1 providers and recipients, rather than the whole supply chain. The extension of notification requirements (e.g. to include potential vulnerabilities) will generate uncertainty on criteria for notification and cause an overload of existing notification mechanisms on both sides (emitting and receiving), to the point that they would become non-operational. JBCE believes this should be replaced by a more effective threat information exchange system, and discussed in consultation with industry.

Reporting

It is important to ensure that clear procedures are adopted so as to avoid multiple reporting of incidents (whether to multiple bodies, in multiple jurisdictions, or in multiple formats). More specifically, JBCE suggests:

- **Refining the scope of threats that need to be notified**. The proposal obligates reporting any cyber threat that could have potentially resulted in a significant incident, but it does not

provide any indication as to how to assess whether a threat could 'potentially' result in a significant incident. As such, the current wording in Article 20(2) is too broad and implies that nearly all threats are to be notified. JBCE calls for a clearer and narrower scope for threat reporting.

- **Aligning reporting and notification provisions with GDPR Article 33.** The proposal envisages three reports for the same security incident, the first of which must take place within 24 hours from when the entity becomes aware of the incident. This would be excessively burdensome and force entities to divert resources from establishing the facts of the incident and taking mitigation measures to filing notifications. Additionally, the 24-hour deadline for the first notification would often not allow entities sufficient time to provide authorities with accurate information regarding the incident. JBCE therefore thinks that Article 20(3) should be aligned with Article 33 GDPR. Competent authorities and, where appropriate, recipients of the notifying entity's services, should be notified only once, and not later than 72 hours from having become aware of the security incident.
- **Obliging Member States to establish a 'single entry point' for all notifications** required under NIS2, GDPR and the ePrivacy Directive. ENISA should also develop common notification templates to be used under these Directives. This is foreseen in recital 56 of the NIS2 proposal, but should also be reflected in the body of the legal text.

Penalties

According to Article 31(4), Member States may impose administrative fines of up to 10 000 000 EUR or 2% of the total worldwide annual turnover of the parent company of the entity which has infringed upon the Directive. This provision is clearly inspired by fines that may be imposed under the GDPR. JBCE believes that NIS2 should envisage an upper limit for fines which is lower than the upper limits envisaged in the GDPR: security breaches do not merit penalties as severe as those imposed for personal data breaches.

International standardisation

JBCE welcomes the recognition of implementing international standards. **When drawing up advice and guidelines for technical areas**, international standards or commonly used guidelines (NIST CSF, IEC62443 etc.) should be considered as a basis. They should be set at an appropriate level for mutual understanding, and in consideration of companies' capabilities - so as not to put excessive burdens on some companies.

Implementation

Important entities which are newly covered under NIS2 will need time to examine and prepare for their new obligations as assigned under the directive. JBCE suggests there should be a longer grace period for newly covered entities, particularly considering actions to amend NIS2-related laws in each Member State, as is now taking place.

About JBCE

Founded in 1999, the Japan Business Council in Europe (JBCE) is a leading European organization representing the interests of about 90 multinational companies of Japanese parentage active in Europe. Our members operate across a wide range of sectors, including information and communication technology, electronics, chemicals, automotive, machinery, wholesale trade, precision instruments, pharmaceutical, textiles and glass products.

For more information: https://www.jbce.org/ / E-mail: info@jbce.org

EU Transparency Register: 68368571120-55