April 2021

DOT Europe position paper

Directive on measures for high common level of cybersecurity across the Union (NIS 2)

Introduction

In December 2020, the European Commission released a proposal for a Directive on Security of Network and Information Systems ("**NIS 2**")[1], that would repeal the existing Network and Information Security ("**NIS**")[2] Directive, currently in force.

DOT Europe – the voice of leading digital, online and tech companies in Europe – welcomes the objective of **harmonising and reducing the fragmentation of cybersecurity legislation** across the European Union ("**EU**") Member States.

However, it is important to note that other pieces of legislation are already in force in this area, and that other instruments will come into force in the near future. Indeed, the General Data Protection Regulation ("**GDPR**")[3], the European Union Electronic Communications Code ("**EECC**")[4], the draft Digital Operational Resilience Regulation ("**DORA**")[5] and the draft Critical Entities Directive ("**CED**")[6] are among the tools that (will) cover this policy area and should be considered, in order to avoid confusion and legal duplication.

The proposed NIS 2 is a departure from the initial NIS Directive, which was focused on the cybersecurity of operators of essential services. The difference in terms of risk profile of the operators of essential services and online service providers was taken into account and a proportionate system put in place to accommodate this difference. It is essential that the distinction between risk profiles is continued in the new NIS 2. The relevant obligations must be tailored accordingly to appropriately reflect the relevant risk profile for the services in question. Below, DOT Europe summarises key points to consider in order to achieve a proportionate and future-proof legislation.

[1] Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166
[2] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[3] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC https://eur-lex.europa.eu/eli/reg/2016/679/oj
[4] Directive (EU) 2018/1972 establishing the European Electronic Communications Code https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN
[5] Proposal for a Regulation on digital operational resilience for the financial sector https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN
[6] Proposal for a Directive on the resilience of critical entities https://eur-lex.europa.eu/resource.html?uri=cellar:74d1acf7-3f94-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF

Rue du Trône, 60, 1050
Brussels, Belgium
Tel: +32 (0) 2 626 1990

WWW.DOTEUROPE.EU
Transparency Register: 53905947933-43
DOT Europe was formerly known as EDiMA

Scope

The scope of the draft NIS 2 has been considerably widened compared to the 2016 NIS Directive. "Cloud computing service providers" and "data centre service providers" are now considered as essential entities, whereas "providers of social networking service platforms" and "providers of online search engines" would now be in scope of the draft Directive. Every one of the scope categories is complex and requires careful consideration. We would appreciate more clarity on the inclusion of "manufacturers" in the health space under "essential" entities and other manufacturing entities in the "important" entities category. **Clear and unambiguous definitions are needed in the proposal** to avoid confusion as to what services have to comply with the requirements set out. For example, one entity could provide services that are in the scope of the draft NIS 2 together with services that are not. We would consider it disproportionate to apply draft NIS 2 requirements to the whole entity in that situation. Similarly, one entity could provide several services that are in-scope (e.g. cloud provider, operator of data centres and manufacturers) with a risk of duplicating the compliance efforts. Another example, is where an entity could provide "cloud computing" or "data centre" services solely for its own purposes or the purposes of its own group of companies. We would again consider it unnecessary and disproportionate for the entity to be in scope of the draft NIS 2 on that basis.

More clarity would also be welcome on the designation of "important" and "essential" entities including where the dividing line lies. Otherwise, the risk arises that many digital platforms and services could be considered simultaneously "essential" and "important". This could lead to regulatory uncertainty as to the correct framework under which they should be assessed along with the legal consequences that could arise from such a situation. Regulatory uncertainty and/or imposition of unduly burdensome obligations could ultimately create an unnecessary investment disincentive in the EU digital ecosystem, particularly for SMEs.

Security obligations

For DOT Europe members, delivering their services with the highest level of security possible is of utmost importance. The wide variety of online services captured by the proposed NIS 2 makes it **challenging for online service providers to be able to comply with a 'one-size-fits-all' approach** to security. All services do not have the same way of securing their offerings and already have different methods in place that are tailor-made to suit the service they provide and comply with existing legislation at European and at national level. The draft NIS 2 should not interfere with valid business/commercial decisions that providers have made as to how to structure the provision of their services. As recognised, for example, in Recital 54, providers should be able to determine what technical and organisational measures are required to provide 'appropriate' security and remain free to choose to adopt encryption – including end-to-end encryption ("**E2EE**") – consistent with their own business decisions.

Entities should be responsible for ensuring their in-scope services are delivered with an appropriate level of security, consistent with the framework under the draft NIS 2. However, we strongly recommend an approach that recognises *how* the relevant standard is met and assured. This is best determined by the entity itself, with the entity then being held accountable for those determinations.

It is challenging for any security standard to, on the one hand, be suitable in the vast majority of "normal" cases, and simultaneously take into account the specific challenges that arise when providing specific "essential" or "important" services. This is particularly true, when operating a pan-European, or global infrastructure.

The presence or absence of specific controls should not automatically be taken to mean that one organisation is less or more secure than another. The outcome is what is important. The security measures put in place by an entity should be tailored to the risks an organisation can potentially face. There are a lot of different ways to check whether the appropriate security level is in place. For example, in addition to validation of specific controls, the use of metrics of security-effectiveness can also demonstrate that appropriate measures are in place and operating effectively. DOT Europe encourages the co-legislator to adopt an approach which is based on appropriate outcomes, rather than focusing on prescriptive adherence to fixed standards.

End-to-end encryption

We welcome that the draft NIS 2 recognises the important role that encryption (including E2EE) can play in keeping services secure. In particular for communication services, it often represents the best practice in securing the confidentiality of the service. However, the draft **NIS 2 should refrain from referring to specific cybersecurity risk management measures**, such as encryption, without being more clear on the ability for relevant entities to determine what are appropriate measures. DOT Europe urges the co-legislator to clarify that security measures should be risk-based (taking into account the state of the art) and that no single security measures (such as encryption or E2EE) should necessarily be seen as a "silver bullet" solution applicable to all situations and risk postures. However, at the same time, nothing in the draft NIS 2 should undermine or prevent relevant entities from choosing to adopt E2EE, should they wish to do so. The Recitals should be careful not to undermine the core requirement of Article 18, that 'appropriate' measures are implemented.

In addition, the draft NIS 2 should be careful not to inadvertently undermine the effectiveness of security measures – such as encryption. DOT Europe observes that the draft NIS 2 appears to indicate that the obligation to use encryption, including E2EE, in order to safeguard the security of electronic communications services must be balanced by the fact that law enforcement may need 'lawful access'; and if 'lawful access' is allowed, it should not undermine the security benefits of E2EE (Article 18(2)(g), Recitals 53 and 54). These premises are contradictory and unworkable in practice. We therefore encourage the European Commission to clarify its intent and note that **lawful intercept of content for E2EE – even if expressed as being pursuant to a 'lawful' basis – will inherently undermine security**. Further, we note that such a provision will operate to the detriment of the competitiveness and innovation of EU SMEs and we encourage that such purported 'balancing' to allow for 'lawful access' is deleted.

Reporting obligations

In the draft NIS 2, "essential" and "important" entities are subject to expanded technically and operationally challenging notification and reporting obligations. Bearing in mind that this is a new set of regulatory obligations for online service providers to comply with and that there are current and future legal instruments that require online service providers to provide reports on various parts of their operations, DOT Europe sees room for improvement regarding three aspects.

First, the definitions need to be clarified further to avoid confusion. We regret that **provisions on reporting are often ambiguous** and do not consider the practical reality of the matter. For instance, the difficulty of interpreting a requirement to provide the relevance of information relating to something 'that could have happened'. The definition of a 'significant' incident in Article 20(3) requires interpretation and the difference in definition between an 'incident' in the draft NIS 2 compared with a 'security incident' under the EECC could create confusion and place a significant burden on the entities as well as on the competent authorities if they are not clarified. This is particularly concerning if, contrary to the stated objective in Recital 48, the draft NIS 2 and EECC continue to operate alongside each other. Finally, the end goal of these reporting obligations is not clear, and more details would be welcome regarding what is expected from the entities' services in scope. Overall, this is a departure from incident reporting towards threat reporting which will create a burden for regulators to handle and on companies to produce. In addition, entities will need to decide for themselves when to notify, so clear thresholds are of utmost importance.

Second, the draft NIS 2 envisages notification to competent authorities/computer security incident response teams ("**CSIRTs**") "*without undue delay and in any event within 24 hours after having become aware of the incident*". This **reporting timeframe is likely to be challenging** for the services in scope, given that entities will in most cases need more than 24 hours to gather and analyse enough information to understand whether an incident was "caused by an unlawful or malicious actor". This will lead to the sharing of inaccurate information to the competent authorities in order to respect this strict and unworkable timeline. It also runs the risk of drawing attention away from efforts to remediate the issue at hand in order to meet a notification deadline. We recommend **aligning the notification timeline with the GDPR** and requiring notification "without undue delay and where feasible" no later than 72 hours after having become aware of the incident.[7] This allows service providers the time to undertake necessary investigation into the matter before burdening the competent authority.

Third, the new mandatory requirement to disclose vulnerabilities in order for the European Network and Information Security Agency ("**ENISA**") to compile a centralised vulnerability registry requires further justification, consideration, and explanation of how this will operate in practice. Considering existing global mechanisms and structures in place, **ENISA could play a stronger role in these initiatives rather than creating a regional structure** with additional obligations for businesses. It is also not clear what value such a registry would provide, beyond the value provided by similar initiatives such as the Common Vulnerabilities and Exposures ("**CVE**")[8] or National Vulnerabilities Database ("**NVD**")[9] databases. Reporting vulnerabilities before patching is also a major security risk and not aligned with security industry best-practice on responsible disclosure of vulnerabilities. Such

[7] See Article 33(1) GDPR
[8] https://cve.mitre.org/
[9] https://nvd.nist.gov

disclosure should take place on a voluntary basis. Further clarity on the use of the registry is needed including: (1) who/what entities will have access to the registry, (2) under what conditions and, (3) to what end, to avoid the misuse of the information compiled.

Regulatory inconsistency and confusion

The draft NIS 2 creates regulatory inconsistency and confusion regarding definitions, obligations, and supervision under other overlapping legislations (GDPR, DORA, ePrivacy Directive ("**ePD**")[10], ePrivacy Regulation ("**ePR**")[11], EECC). We encourage policymakers to ensure harmonisation between at least NIS 2, DORA, the ePD, the EECC, and the GDPR. They all have related but inconsistent reporting requirements (e.g. timeframes, level of information and detail, and potential non-compliance penalties). This needs to be streamlined to avoid overlapping and/or conflicting obligations.

- **DORA:**
  - We recommend introducing a clear hierarchy between the draft NIS 2 and the draft DORA to avoid fragmentation and conflicting obligations for cloud providers. There is a high risk of conflicting recommendations coming out of the two separate supervisory and oversight processes from different regulators if no single mechanism for the competent authorities to share information and coordinate their practices is established. In case of conflict, despite the coordination mechanism, the draft NIS 2 should prevail as it is sector-agnostic.
  - On definitions, the draft NIS 2 mentions "incident", while the draft DORA refers to "ICT-related incident." We recommend the alignment of the draft DORA with the draft NIS 2.
  - On reporting, the draft DORA is concerned with "major ICT-related incidents" while the draft NIS 2 with "incidents that are significant". This could be better aligned.
  - On timeframes, there are inconsistencies in relation to the point at which the timeframes for incident notification begin. It would be preferable if timeframes for initial notifications and status updates were consistent and to consider that some entities may have requirements to report under both the draft DORA and the draft NIS 2 (whether directly or indirectly through contractual requirements). This may allow for a more systematic and consistent approach to be taken to incident reporting.
  - On templates, the incident reporting template requirements set out in the draft DORA should be consistent with the notification content requirements of the draft NIS 2. The description of the content to be included in notifications is not consistent between the two proposals. It would be preferable if the notification templates for both initial and status updates do not diverge.

[10] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

[11] Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

- The draft DORA also enables the Joint Committee to issue regulatory technical standards with further criteria, which may cause further non-alignment at a later stage. These inconsistencies may increase the administrative burden and cost in reporting. We recommend that the various supervisory authorities coordinate amongst themselves before making decisions and acting.

- **EECC:**
  - In the event that the reporting obligations under the EECC are to be repealed for public electronic communications networks ("**PECN**") and publicly available electronic communications services ("**PECS**"), we suggest that these are replaced by the obligations listed out in the draft NIS 2.
  - In the interest of legal certainty and regulatory predictability, DOT Europe urges the co-legislator to avoid a situation whereby there would be two regimes that would continue to apply alongside each other with respect to security incident and reporting obligations. Such a situation risks creating confusion and uncertainty, as well as potentially significant additional regulatory burdens on companies without any objective justification.
  - In principle, DOT Europe considers that only those incidents that have had an actual security implication (as envisaged under Article 40 EECC), as opposed to unsubstantiated threats that may or may not materialise or incidents that have the 'potential' to give rise to the causes/effects under Article 20(3), should be reportable.
  - Further, DOT Europe considers it is necessary to ensure that reporting obligations only apply to the relevant services in scope, in respect of which an impact which has actual security implications has occurred, rather than being extended out more broadly to the activities on the entity in question, as could be the case under the draft NIS 2.

- **GDPR:**
  - The draft NIS 2 should align with the GDPR's definitions, concepts (e.g. main establishment), incident reporting thresholds, and templates.

Certification schemes

The proposal introduces the use of potentially mandatory European certification schemes for certain ICT products, services, and processes (Article 21). **DOT Europe does not support mandatory certification**, especially as both "essential" and "important" entities will be covered. This is also in direct conflict with the voluntary certification regime in the Cybersecurity Act ("**CSA**")[12]. The introduction of a mandatory certification regime will lead to legal uncertainty while also creating an additional layer of obligations for the entities in scope, ultimately hindering innovation in cybersecurity as entities will fear non-compliance.

[12] Regulation (EU) 2019/881 on information and communications technology cybersecurity certification and repealing Regulation (EU) No526/2013 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

If the text upholds the mandatory nature of the certification schemes, it could create market entry barriers for small(er) service providers which often do not benefit from substantial compliance teams and resources. In addition, a mandatory obligation to implement security in a 'particular way' would negate the differences that exist between the wide range of services captured by the draft Directive and how they are structured and risk stifling innovation in the fast-moving information security industry. Instead, we would support a principles-based approach implemented in the most appropriate way for that service.

In accordance with Article 57 of the CSA, national schemes should cease to produce effects once EU cybersecurity certification schemes are adopted. There are today numerous national certification schemes with contradictory requirements that jeopardize companies' compliance efforts, hamper innovation and as a result, increase the security risks as companies are resigned to not investing in these costly and burdensome certifications. Furthermore, focusing on EU certification schemes only would affect the interest of companies likely to grow their business outside of Europe of adopting certifications that do not scale and that ultimately, would not be recognised outside of Europe. **Alignment with international standards and at least mutual recognition with international cybersecurity schemes should be encouraged.**

Jurisdiction and application of One-Stop-Shop

We welcome the principle of the main establishment as was already the case in the original NIS Directive, but to achieve a more harmonised approach in the area of network and services security under the draft NIS 2 we recommend to **refer to the "main establishment" notion under the GDPR** and not to create an additional specific NIS-main-establishment-regime. We strongly recommend extending the one-stop-shop ("**OSS**") mechanism in Article 24 to all digital infrastructure service providers, PECN and PECS. This will allow for a more harmonised approach to jurisdiction in this provision. Failure to ensure that these services are included would create a disproportionate regulatory burden. Applying the OSS principle in the draft NIS 2 to PECN and PECS would further streamline the security and notification obligations.

The proposal should also consider the **cross-border nature of some services in scope**. While the draft recognises that some services that are inherently offered across borders should benefit from falling under the jurisdiction of the main establishment of the provider, this is not the case for all services. For example, trust services would fall under the jurisdiction of each Member State. We therefore suggest that trust services fall under the jurisdiction of the main establishment of the provider as well, which is in line with the stated goal of the draft NIS 2, i.e. the further harmonisation of the digital single market for these types of services.

Finally, we consider that the designation of the Member State of the main establishment if cybersecurity decisions are not taken in the EU (Article 24(2)) should not be based on the number of employees in a specific establishment. This is an arbitrary criterion which does not consider the internal organisation of the provider. It should be up to the individual company to decide which Member State should be its main establishment within the EU for the purposes of this draft Directive.

Enforcement and fines

It is generally recognised in the security industry that collaborative, engagement on security matters leads to better security outcomes. DOT Europe is therefore concerned with the rather **broad and punitive approach** foreseen in the draft Directive when it comes to enforcement and fines, and whether this is the most effective means of encouraging engagement with the principles of the draft Directive.

We are also worried that the kind of information competent authorities can request based on Article 29 and 30, as part of their supervisory power, is too broad and unspecific. For instance, it is unclear what "evidence" means with regard to the implementation of cybersecurity policies. We recommend a clarification of this provision to bring legal certainty to entities concerned. Furthermore, on-site audits and inspections might be costly and laborious for companies. It is necessary to tighten the parameters under Article 29(2) to avoid disproportionate burdens on companies and additional or unjustified costs. In addition, as online services generally use very complex technologies, it would be recommended, to limit the security risk and ensure the reliability of the verifications and findings, that any supervisory audits will be subject to specific and internationally recognised auditing standards (e.g. Service Organisational Controls).

While personal data may be exposed due to a cybersecurity incident, it is important that there is clarity regarding the reporting obligations and timelines. The proposed Directive should make clear that the OSS principle of the GDPR is not undermined through Article 32.

We would also like to underline the **importance of proportionality** in this proposal. This area is a new one for entities which may now come into scope of the proposal. They need time to adapt to these new requirements. The fines appear to be similar to the GDPR framework and these prohibitive levels will not foster the type of collaborative engagement between the public and private sectors that is necessary for improved overall cybersecurity. Furthermore, too high sanctions combined with low reporting thresholds might lead to a flood of irrelevant data.

Finally, we regret the lack of harmonisation of administrative penalties in this draft Directive. The European Commission should have the power to comment, and possibly veto, national rules relating to penalties and the measures to implement them, in order to avoid a patchwork of national legislations and fragmentation at EU level.

Conclusion

We welcome the intention behind the revision of the NIS directive. However, several issues remain. The scope of the draft NIS 2 needs to be clarified in light of its wider applicability. The different obligations should take into account that a wide variety of services are now captured by the proposal. Flexibility is required if we want the text to work in practice, especially since different services will have different approaches to providing appropriate security and complex compliance obligations, in particularly on small entities designated as in scope under Member State law (pursuant to Article 2(2)), could stifle growth. Many definitions also need to be clarified in that regard. Finally, we recommend avoiding a blanket fining system in order to reflect the wide range of entities in scope and the specificities of online services. The draft NIS 2 should be proportionate and reasonable to reach the best level of cybersecurity possible in the Single Market.