NIS2 transposition

Verizon's position

Introduction

1. Verizon is a global player. Outside of the U.S., Verizon provides a broad range of global communication products and enterprise solutions, predominantly to large business and government customers. We are established in most European Union ("**EU**") Member States ("**MSs**" and singular "**MS**"), and provide services in over 150 countries worldwide. As a pan-European business provider, we generally welcome any initiative which aims to bring further harmonisation and legal certainty, and reduce administrative burden at EU and national levels.

Verizon's main concerns

Harmonisation and consistency

2. Verizon's concerns are twofold: (1) The objective of the Network and Information Systems ("**NIS2**") Directive is to provide legal measures to boost the overall level of cybersecurity in the EU. Therefore, the need for harmonisation is paramount, serving as the main objective of the NIS2 implementation at both EU and MS levels. This encompasses uniformity in security measures and reporting obligations. (2) Integrating and aligning the Directive's complexity with other regulations, like the Digital Operational Resilience Act ("**DORA**") & the Resilience of Critical Entities Directive ("**CRE**"). The European Commission ("**EC**") has a leading role to play in ensuring consistency through Implementing Acts and Delegated Acts. The benefits include reducing complexity for (multinational/pan-European) companies and preventing a mix of differing national requirements that may conflict. Simplifying cybersecurity obligations, eliminating overlapping duties and unnecessary expenses would help achieve this objective. Below we explain these concerns in more detail.

NIS2 security practices should align with existing practices of EECC Arts. 40 & 41

3. With NIS2, NIS related articles 40 & 41 of the European Electronic Communications Code ("**EECC**") will be repealed. Telecom providers have been subject to security and resilience regulation since 2013. As such they already have substantial and robust security policies in place, and extensive experience in implementing NIS requirements. That also includes an efficient working relationship with the national telecoms regulatory authorities ("**NRAs**") at operational level that should be maintained. Verizon strongly believes that telecom providers should not be expected to make changes to their existing

security practices to meet NIS2 when the outcome is the same.

4. We call upon MSs to harmonise technical, organisational and operational measures and align them with the EECC NIS articles. Furthermore, measures should be principles based so as to allow each entity to apply appropriate measures to its level of risks. Under recital 65, the Cooperation Group could map national requirements against each other. This could help ensure consistency and compatibility across the Union and reduce burden for entities operating in multiple MSs.

Standards and cost of implementation

5. We encourage the use and/or reference to international standards. MSs should refrain from specifying the use of certain technologies; this will mean that entities can pick technology that fits with their business models and systems better, and will ensure that regulations do not risk becoming out of date as technology changes and improves.

6. MSs should carefully consider Article 21(1) since it mentions that the cost of implementation must be taken into account when setting technical, operational and organisational measures.

The transposition of NIS2 into national law should seek for the right balance between clarity and flexibility allowing companies optimal compliance efforts.

7. MSs should have flexibility and recognise that such multi-national, multi-service entities will have corporate level controls rather than national and service specific ones. The use of the criterion of 'main establishment' should be the standard for entities with complex business models and cross-border presence. The main establishment is one that has operational and managerial capabilities to implement cybersecurity measures. The implementation of the Directive needs to avoid that subsidiaries of a pan-European group fall under the separate and concurrent jurisdiction of respective MSs where they operate. Verizon suggests MSs to request or follow the guidance that should be provided by the Commission as per recital 21. In addition, this guidance is paramount for the supervision of entities with complex business models that may be classified as both an essential and important operator.

8. Verizon recommends that Entities should have the flexibility to define "Management body" in a manner appropriate to their business. Business models can be complex and there can be no one-size-fits-all approach to management structures. MSs should allow entities to decide where "management" responsibility and liability lies, even if that is outside the EU.

9. Recital 124 sets out that MSs can set their prioritisation for supervision using various criteria or benchmarks. Verizon strongly believes that MS should avoid prioritising services to large enterprise customers in their enforcement actions. Large enterprises typically possess stronger bargaining power and a deeper understanding of security risks, often reflected in stringent contractual commitments. This manifests itself in strong contractual commitments including

SLAs, audit rights and documentation requirements. As such, entities who provide services to those enterprise customers already have an additional incentive to ensure strong security practices.

One stop shop for incident reporting

10. Verizon is strongly in favour of implementing a centralised One-Stop-Shop for Security Incident Reporting. This would lessen the burden on entities and increase authority efficiency, incident reporting under various regulations (GDPR, NIS2, E-privacy, CER). We also believe that reporting delays should be aligned and realistic across the rules listed above.

11. We strongly believe in order to avoid overloading competent authorities with reports that reporting on significant incidents should be targeted and that thresholds for incident notification should be set at appropriate levels. We recommend the use of absolute thresholds (e.g. 1 million users impacted) instead of qualitative type criteria as these are harder to build into automated reporting systems and lead to overreporting of non-significant incidents.

12. We call upon MSs to exempt B2B Providers from public reporting requirements of cybersecurity threats or incidents since B2B providers don't have direct consumer relationships, and reporting between B2B providers and their customers is governed by their contractual relationships.

November 2023

verizon