WRITTEN BY

MARTIN BARANIAK
Managing Associate
Kinstellar

LUCIA KORBA
Junior Associate
Kinstellar

KINSTELLAR

EU CYBER-SECURITY UPDATE

In January 2025, Slovakia officially transposed the NIS 2 Directive into its national cybersecurity legislation, introducing a new registration obligation for companies that meet defined size criteria and operate within designated regulated sectors. As expected, this step brought a noticeable level of uncertainty to the market.

Many organizations found themselves unsure about whether they truly qualified as regulated entities under the new rules, particularly given the complexity of sector-specific definitions and the varying interpretations of what constitutes 'essential' or 'important' activities. This ambiguity left numerous companies grappling with the question of whether they were required to register at all which highlighted the need for clearer guidance and more consistent criteria at both national and EU levels.

Now, one year later, the European Union is preparing yet another significant update to the NIS 2 framework, this time presented as part of the ambitious Digital Omnibus initiative. This new legislative package is designed to further streamline, modernize, and harmonize a wide range of processes connected to cybersecurity, artificial intelligence, and data governance across the EU. By bringing these elements together under a more unified regulatory umbrella, the Digital Omnibus aims to reduce fragmentation, simplify compliance obligations, and ensure a more coherent approach to digital resilience throughout the Single Market.

This brings us to the central question: what do the Digital Omnibus and its proposed updates to NIS 2 actually mean for you and your organization? The upcoming changes are set to reshape obligations, clarify responsibilities, and potentially broaden the categories of entities that fall within regulatory scope. Understanding how these adjustments translate into real-world requirements will be essential for preparing your compliance strategy and ensuring that you remain ahead of the evolving EU cybersecurity and digital governance landscape.

The cybersecurity incident-reporting landscape has been increasingly exhausting, with entities required to notify incidents under multiple legal acts such as the General Data Protection Regulation, NIS2, the Digital Operational Resilience Act and others. For this reason, the Digital Omnibus introduces a single-entry point, designed to simplify and streamline these reporting obligations.

How, you may ask? The entity can submit a report which covers all the incident reporting obligations under the multiple legal acts. This will ensure that the reporting obligations under different acts can be fulfilled by simply submitting one report creating an efficient reporting process.

Introduction of the small mid-cap size of enterprises will have a significant impact on the entities falling in scope under NIS 2. Medium-sized enterprises carrying out activities under Annex I of the NIS 2 will no longer need to register, because a new size criterion on the enterprise is being introduced. Small mid-cap size enterprises surpass the criteria for a medium-enterprise but are smaller than large enterprises. This way, many medium sized enterprises will no longer have to register unless they carry out domain name system services.

> **The scope of regulated activities is expanding, with several new categories of entities now being brought under the framework.**

With NIS 2 implementation, many enterprises had questions whether they fall in scope of the regulated activities or not. The NIS 2 amendment clears out some of the issues which have been flagged, such as modernization of sector definitions (in case of hydrogen, healthcare and intelligent transport system), as well as clarification of the activities relating to chemicals manufacture and the removal of chemical distribution as an in-scope activity.

Another sector which has created more questions than we would have liked was the production of electricity. Many producers have produced electricity for their own personal use and had trouble to determine whether they fall in scope or not. This is being cleared out by the amendment, which states that this sector does not apply to producers whose total generation capacity does not exceed one MW. However, the scope of regulated activities is expanding, with several new categories of entities now being brought under the framework. These include providers of European digital identity wallets, providers of European business wallets, as well as operators responsible for submarine data transmission infrastructure.

Overall, the Digital Omnibus package seeks to address a wide range of issues that have been identified since the introduction of the NIS 2 framework. The proposed adjustments go beyond cybersecurity alone, introducing substantial amendments in related fields such as data governance and artificial intelligence. Through this comprehensive approach, the initiative aims to eliminate ambiguities and close regulatory gaps that have caused challenges for organizations across the EU. Ideally, these changes will make it significantly easier for entities to correctly self-identify and assess whether they genuinely fall within the scope of the legislation, ultimately leading to smoother compliance processes and more consistent application of the rules.

Regulatory developments in the digital and technology sectors continue to evolve at a rapid pace, creating ongoing compliance challenges for organizations across the EU. As frameworks such as NIS 2 and the Digital Omnibus develop further, businesses will need to regularly reassess their regulatory exposure, internal processes, and risk management strategies. Staying informed and proactively monitoring legislative changes will be essential to ensuring continued compliance in an increasingly complex digital regulatory environment.