



POLICY BRIEF

15 09 2025
22

THE NETWORK AND INFORMATION SECURITY DIRECTIVE 2 (NIS2)

From an original text by FEDERICA CASAROSA

Summarized by Arianna Rossi



The Network and Information Security Directive 2 (NIS2)	
BACKGROUND AND FIELD OF APPLICATION	<p>The Network and Information Security Directive (NIS Directive)¹ is widely recognized as a foundational piece of European cybersecurity legislation. It was later revised and replaced by the NIS 2 Directive,² introduced by the European Commission in December 2020 to address the limitations of the original framework. The NIS 2 Directive aims to strengthen cybersecurity across the EU's digital internal market by establishing harmonized standards for risk management and incident reporting. A key feature of the new directive is its expanded scope, which significantly increases the number of entities subject to its obligations and requirements, thereby enhancing the overall resilience of digital infrastructure in the Union.</p>
HIGHLIGHTS	<p>The current structure of the NIS 2 Directive builds directly on the evaluation of its predecessor, the NIS Directive, addressing several of its limitations. One of the initial challenges was defining which entities fell within its scope. NIS 2 introduces a distinction between essential entities (EEs) and important entities (IEs), with largely similar obligations. The primary criterion for inclusion is now enterprise size, excluding small and micro enterprises (Art. 2(1)), although this metric alone may not fully capture an entity's societal or economic relevance. Nonetheless, the Directive outlines several exceptions where size is irrelevant, such as providers of public electronic communications, trust services, domain name systems, sole providers of critical services, entities impacting public safety or health, and public administrations.</p> <p>A second inclusion criterion is whether the entity operates in one of the sectors listed in Annexes I and II, which now include additional domains like telecommunications, social media platforms, and public administration, significantly expanding the Directive's scope.</p> <p>To improve incident reporting, NIS 2 adopts a two-step process: entities must notify the national authority or CSIRT within 24 hours of detecting an incident, followed by a detailed report within 72 hours, and a final recovery report after one month. For enforcement, the Directive sets a minimum list of administrative fines for non-compliance with cybersecurity and notification obligations, and grants national authorities</p>

¹ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, pp. 1–30.

² Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, pp. 80–152.



	powers to issue warnings, binding instructions, and recommendations (Art. 32(4)).
IMPACT	<p>The inclusion of public administration and health-related services within the scope of NIS 2 may bring certain public research institutions under its cybersecurity governance. This regulatory framework, backed by enforcement mechanisms such as administrative fines, encourages these institutions to strengthen their internal cybersecurity policies and infrastructure. However, it also introduces increased compliance obligations that may be challenging for research bodies lacking sufficient resources or tailored guidance. The pressure to avoid sanctions may lead some institutions to adopt cybersecurity measures rapidly, even when their internal capacity to do so is limited, raising concerns about the sustainability and effectiveness of such efforts.</p>