NATIONAL IMPLEMENTATION OF THE NIS 2 REQUIREMENTS

THE NEW PORTUGUESE CYBERSECURITY LAW

João Vitorino, Pedro Ramalho de Almeida e Bernardo Pedro Santana

SUMMARY

The new Cybersecurity Law transposes the NIS 2 Directive to the Portuguese internal law and significantly expands the range of entities subject to cybersecurity obligations. It introduces stronger responsibilities for management bodies, more detailed and harmonised risk management obligations, and new rules on identification, reporting and oversight. It also creates separate supervisory models for Essential Entities and Important Entities, replacing the previous NIS 1 structure, and establishes a significantly stricter sanctioning regime. The new Cybersecurity Law becomes effective on April 4, 2026, and its practical implementation will depend on further technical instructions from the CNCS and sectoral authorities.

A NEW LEGAL FRAMEWORK

The new Cybersecurity Law marks a significant evolution from the previous NIS 1 regime, which imposed less detailed duties and applied to a more limited group of entities. The scope is now substantially broadened to include sectors and subsectors that were not covered under NIS 1. It strengthens the obligations of public and private entities that perform essential or important functions for the economy and society.

Scope and Covered Entities

By contrast with the previous NIS 1 regime applied, only to specific public bodies within narrowly defined critical sectors, the new Cybersecurity Law divides covered entities into three categories:

(1) Essential Entities, comprising entities from critical sectors that exceed the thresholds for medium-sized enterprises, medium-sized electronic communications providers, qualified trust service providers, TLD registries and DNS providers. The classification also depends on the entity's level of exposure to risk and its potential impact;
(2) Important Entities, which are entities operating in the same critical sectors that do not meet the criteria for Essential Entities; and
(3) Relevant Public Entities, covering public bodies not included in the first two categories and distributed across Groups A and B depending on their size.

But, as under NIS 1, public entities operating in the fields of national security, public security, defence and intelligence services, are excluded.

New Obligations for Companies

Covered entities must register on the CNCS (National Centre for Cybersecurity) electronic platform within 30 days of starting their activity or, for existing entities, within 60 days of the platform becoming available.

The new Cybersecurity Law assigns direct responsibility for cybersecurity risk management to management bodies, whereas the previous regime imposed less explicit and less enforceable duties. Failure to ensure adequate oversight may lead to liability and sanctions for directors.

Management bodies of Essential Entities and of Important Entities now have reinforced obligations to approve and monitor cybersecurity measures, including ensuring regular training.

Risk Management Obligations

Essential Entities and Important Entities must implement technical and organisational measures proportional to their risk exposure and adopt a risk management system covering all assets and systems necessary for service continuity. Such measures must follow CNCS guidelines and risk matrices and reflect relevant technological developments.

For this purpose, the new Cybersecurity Law:

- sets minimum security requirements, including risk management policies, business continuity measures, access controls and multifactor authentication;
- requires the assessment and documentation of residual risk and the prompt adoption of corrective measures;
- imposes upon each entity the obligations to prepare an annual report, to appoint a cybersecurity officer and to maintain a permanent contact point with continuous availability.

The new Cybersecurity Law establishes a national cybersecurity certification system for ICT products and services, allowing entities to demonstrate compliance and streamline conformity processes.

Incident Notification

The new Cybersecurity Law sets shorter deadlines for reporting significant incidents and security breaches. Entities must submit an initial notification within 24 hours, an update within 72 hours and a final report within 30 business days after the impact ends. Under NIS 1, notifications had to be made "without undue delay", with no fixed deadlines, giving competent authorities considerable discretion.

Role of the National Cybersecurity Centre (CNCS)

The CNCS continues to act as the national coordinator for cybersecurity but now assumes additional supervisory, auditing, inspection and technical guidance functions, substantially expanding the role foreseen under NIS 1.

Supervisory intensity varies according to whether an entity is classified as essential or important. Essential Entities are subject to continuous supervision, including audits, inspections and testing, whereas Important Entities are generally subject to reactive supervision, primarily after incidents or indications of non-compliance.

Significantly higher penalties for serious or very serious infringements will be in place, setting limits of up to €10 million or 2 percent of turnover for Essential Entities and up to €7 million or 1.4 percent for Important Entities.

Entry into Force and Transitional Period

The new Cybersecurity Law enters into force 120 days after publication, which occurred on December 4, 2025. The CNCS and sectoral authorities are currently preparing technical instructions and complementary rules that will operationalise the new obligations.

ABOUT MACEDO VITORINO

MACEDO VITORINO is a leading Portuguese law firm. We advise domestic and foreign clients in a wide range of business sectors, including banking, distribution, industry and projects. We are known for our professional and client-oriented approach to complex and difficult matters.

Since the incorporation of the firm in 1996, we have been involved in several high-profile transactions in all of the firm's fields of practice, including banking and finance, capital markets, corporate and M&A, energy, real estate, project finance, complex disputes and restructurings.

IMPORTANT INFORMATION

The opinions expressed in this article are of a general nature and should not be considered professional advice. Should you require legal advice on these matters, you should contact a lawyer. If you are a client of MACEDO VITORINO, you may contact us by email at mv@macedovitorino.com.