Portugal

Your local contact

Tiago Silva Abade
Head of Public Law & Data Protection
Partner, PwC Legal Portugal
+35 1913463267
tiago.s.abade@pwc.com

Status	In Portugal, the process of transposing the NIS-2-Directive is still ongoing. On February 6, 2025, the draft law was approved by the Council of Ministers, after which it proceeds to Parliament for approval, following a period during which the document was subject to public consultation, from November 22 until the end of December 2024. It was expected that this approval in Parliament would take place on March 20, 2025, the date for which it was scheduled. After the new Government takes office in June 2025, it is expected that approval will occur soon.
Name of National Law	Cybersecurity Legal Regime
Entered into force	Estimated October 2025
Link to current draft or equivalent	https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=314833b
Scope (deviating from NIS-2-Directive)	To be evaluated after the Law has been approved.
Registration	All regulated entities must self-identify via an electronic platform provided by the CNCS within one month of starting operations. Entities already active on the market when the Decree enters into force need to register within 60 days of the platform's availability.
Information Security Standards referenced	Although the public consultation document represents a solid foundation for what may become the national law, the current text stipulates that the implementation and regulation will only occur through technical instructions to be issued by the CNCS, with no date of issuance foreseen. This uncertainty brings with it several concerns and difficulties faced by companies and organizations covered by NIS-2, such as: • Difficulty in planning and implementing security measures and/or technological investments in relation to the specific legal requirements to be transposed; • Non-compliance with the required security standards, which may lead to penalties; • Loss of competitive advantage compared to other companies in the same market located in EU countries where NIS-2 is already a legal reality; • Increased exposure to cybersecurity attacks due to the lack of adoption of minimum-security practices and requirements; and • Decreased reputation/customer trust due to a lack of alignment with best practices in cybersecurity and information security. In addition to these concerns, there has been a growing apprehension among organizations regarding the fact that members of management, executive, and administrative bodies may be held liable, by action or omission, for violations set out in the transposition of NIS-2, as provided for in Article 25 of the Directive.
Incident reporting	National Cybersecurity Center, as stipulated by Article 7, paragraph 1 of Law no. 46/2018, which establishes the Legal Framework for Cyberspace Security.

Portugal

Your local contact

Tiago Silva Abade
Head of Public Law & Data Protection
Partner, PwC Legal Portugal
+35 1913463267
tiago.s.abade@pwc.com

Authority / CSIRT	National Cybersecurity Center (CNCS)
Fines (deviating from NIS-2-Directive)	In the case of essential entities, fines may reach EUR 10.000.000 or 2% of the entity's total global turnover, whichever is higher. For important entities, fines may reach EUR 7.000.000 or 1.4% of the total global turnover, whichever is higher. The following additional sanctions may also be applied: • The publication, at the offender's expense, of an excerpt from the conviction decision or at least the operative part of the conviction decision, in the Official Gazette (Diário da República) and in one of the newspapers with the largest national, regional, or local circulation, depending on the relevant geographic market, after the decision becomes final; • Prohibition from participating in public procurement procedures, when applicable; • The adoption and implementation of a cybersecurity training plan, to be carried out within 6 months; • The adoption or amendment of a security plan, to be carried out within 6 months; • Suspension of the provision of the service until the omitted obligations are fulfilled; • Temporary disqualification of the members of the management, executive, and administrative bodies from exercising their respective functions.
Worth mentioning	Entities subject to the Decree-Law must classify themselves as essential, important, or relevant public entities (self-identification obligation).