

# New Legal Regime on Cybersecurity

Government approves Decree-Law 125/2025 of December 4, which transposes NIS2, expands the scope of cybersecurity, and strengthens risk management, incident reporting and penalties.

Portugal | Legal Flash | December 2025

## KEY ASPECTS

- Decree-Law 125/2025 of December 4 (“**Decree-Law 125/2025**”) transposes [Directive \(EU\) 2022/2555 of the European Parliament and of the Council of December 14, 2022 \(“NIS2”\)](#) into the Portuguese legal framework and imposes a duty of diligence and oversight with personal liability for intentional misconduct or gross negligence, requiring documented decision-making processes and the integration of cybersecurity into top-level management.
- Essential, important and relevant public entities are required to register on the designated platform and meet deadlines for reporting significant-impact incidents, including (i) an alert within 24 hours of verifying the incident, (ii) an update within 72 hours, (iii) an end-of-impact notification within 24 hours, and (iv) a final report within 30 business days of the end-of-impact notification, supported by tested processes, trained teams and clear reporting lines.
- A risk management system is mandatory, covering risk analysis, incident response, continuity planning, lifecycle management, and supply chain security. This system must include encryption and multifactor or continuous authentication. Also, an annual report is required, along with certification, where applicable, issued by an accredited body or under a scheme recognized by the Portuguese National Cybersecurity Centre (“**CNCS**”). The CNCS may mandate this certification.
- Classification of an entity as essential or important dictates specific obligations and fines of up to €10 million or 2% of the preceding financial year’s annual worldwide turnover for essential entities, and up to €7 million or 1.4% of the preceding financial year’s annual worldwide turnover for important entities. Negligence is also subject to penalties.
- Decree-Law 125/2025 enters into force 120 days after its publication. Certain provisions will take effect 24 months after the CNCS approves and publishes applicable regulations that will trigger this transition period.





The publication of **Decree-Law 125/2025**, which transposes the **NIS2 Directive** and establishes the New Legal Regime on Cybersecurity, represents a significant milestone in the national regulatory landscape. Far from being merely a compliance exercise, the new regime imposes a concrete obligation of resilience and requires the integration of cybersecurity into top-level management. This shift directly impacts strategy and risk management, thereby reinforcing the accountability of management and governing bodies.

**Note:** Unless expressly stated otherwise, references to articles in this Legal Flash pertain to the annex containing the Legal Regime on Cybersecurity, as referred to in article 2 of Decree-Law 125/2025 (“**Annex**”).

---

## Origin and purpose: NIS2 Directive

The new national framework arises from the transposition of the NIS2 Directive, which revokes the previous **Directive (EU) 2016/1148 of the European Parliament and of the Council (“NIS Directive”)**. This update aims to address the limitations of the original NIS Directive.

Experience since 2016 has demonstrated that the NIS Directive was insufficient in the face of the increasing number, sophistication and impact of cyberattacks. Also, it did not account for the increasing interdependence of digital services or the vulnerabilities within supply chains. Significant regulatory fragmentation persisted among Member States, with varying levels of requirements and an absence of harmonized minimum requirements.

It was within this context that, in 2022, the European Union (“**EU**”) approved the NIS2 Directive. Articles 1 through 4 of the NIS2 Directive define the subject matter, scope and structural principles of the new regime. The NIS2 Directive broadens the range of covered entities, strengthens risk management obligations (Article 21), establishes uniform rules for incident notification (Article 23), and introduces a substantially more stringent enforcement and penalty regime.

---

## Scope of application and sectoral coverage

Decree-Law 125/2025 fully transposes the EU framework by distinguishing between essential entities and important entities. This distinction reflects Annexes I and II, and Article 3 of the NIS2, imposing distinct and stricter obligations and penalty regimes on essential entities.

**Entities from the following sectors**, as outlined in Annex I of the Annex, **qualify as essential entities** (article 6):

1. **Energy:** Electricity, district heating and cooling systems, oil, gas, and hydrogen
2. **Transport:** Air, rail, water, and road
3. **Banking:** Credit institutions
4. **Financial market infrastructures:** Trading venue operators and central counterparties (CCPs)
5. **Health:** Healthcare providers, EU reference laboratories, and entities carrying out research and development (R&D) activities of medicinal products
6. **Drinking water:** Suppliers and distributors of water intended for human consumption
7. **Waste water:** Wastewater management
8. **Digital infrastructure:** Internet Exchange Point providers; DNS (Domain Name System) service providers, excluding operators of root name servers; TLD (Top Level Domain) name registries; cloud computing service providers; data center service providers; content delivery



network providers; trust service providers; providers of public electronic communications networks; and providers of publicly available electronic communications services

9. **Information and communication technologies (ICT) service management (B2B):** Managed service providers and managed security service providers
10. **Space:** Operators of ground-based infrastructure that support the provision of space-based services

**Note:** The qualification as an “essential entity” is determined by the cumulative application of the criteria in Article 6. According to these criteria, an entity must belong to a sector listed in Annex I of the Annex, and it must meet the size criterion defined in Annex III, as specified in articles 3.1.a), 6.1.a), 6.1.c), 7.2.f), and 12.2.i).

Beyond this rule, article 6 provides for inclusions regardless of an entity’s size, and the possibility of risk-based qualification by the CNCS, which also determines the classification as an “essential” entity.

The Public Administration is not, in itself, categorized as a macro “sector” in the Annexes. Instead, certain entities qualify as essential under article 6.1.d).

### **Entities in Annex II sectors that qualify as important entities (article 6)**

Under article 6, entities from the following sectors, as a rule, qualify as important entities:

1. **Postal and courier services:** Postal service providers
2. **Waste management**
3. **Manufacture, production and distribution of chemicals**
4. **Production, processing and distribution of food:**
5. **Manufacturing:** Entities involved in the manufacture of:
  - a) medical devices and in vitro diagnostic medical devices;
  - b) computer, communications, electronics, and optical products;
  - c) electrical equipment;
  - d) machinery and equipment (unspecified);
  - e) motor vehicles, trailers and semi-trailers; and
  - f) other transport equipment.
6. **Digital providers:** Providers of online marketplace, online search engines and social networking services platforms
7. **Research**

**Note:** The qualification as an “important entity” is determined by the cumulative application of the criteria outlined in article 6. An entity must belong to a sector listed in Annex II of the Annex and meet the size criterion defined in Annex III, as specified in articles 3.1.a), 6.1.a), 6.1.c), 7.2.f), and 12.2.i).

Beyond this rule, article 6 provides for inclusions regardless of an entity’s size and the possibility of risk-based qualification by the CNCS, which also determines the classification as an “important” entity.

Compliance within the supply chain extends beyond the entity itself. Whether classified as essential or important, an entity must assess and monitor the risks associated with critical suppliers and



service providers (article 28). It must also comply with public decisions imposing the restriction or cessation of the use of high-risk ICT (article 18.3).

---

## Preparation phases for covered organizations

Preparation should be phased as follows:

1. **Post-publication of Decree-Law 125/2025 (until entry into force – 120 days) (analysis and design phase):** Organizations should carry out a gap analysis, mapping existing gaps against the requirements set out in Decree-Law 125/2025, and assessing the legal framework. Formal appointments include the Cybersecurity Officer (article 31) and the Permanent Point of Contact (article 32).
2. **Before full application (implementation and testing phase):** Organizations should develop and test incident management and business continuity plans. Formalizing risk management in the supply chain (article 28) is essential, as is compliance with the duty to register on the designated electronic platform (articles 8.1 and 35).
3. **Oversight and continuous improvement (operationalization phase):** Upon entry into force of Decree-Law 125/2025, organizations must fulfill their obligations, subject to supervision by the competent authority (CNCS). Preparation of the annual report, where applicable (article 30), is required. Also, if required by the CNCS, organizations must obtain cybersecurity certification under article 34.

---

## Decree-Law 125/2025 radar: What management and governing bodies cannot ignore

The publication of Decree-Law 125/2025 creates a new ecosystem of accountability. For business development purposes, management must shift its approach from simply asking, “What does the law say?” to evaluating, “What is the risk of inaction?” The key topics identified in the decree-law, as outlined below, must be treated as priorities for oversight and immediate action.

### The game changer: Immediate risk and personal liability of management and governing body members

- **Risk for members of management and governing bodies:** The most significant risk is personal liability of management board members for acts or omissions carried out through “intentional misconduct or gross negligence” (article 25.2). To mitigate accusations of gross negligence, management and governing bodies must ensure the existence of documented evidence demonstrating due diligence and oversight. Cybersecurity, as a fiduciary responsibility, can no longer be delegated. Rather, it requires active supervision, well-documented decision making, and a continuous demonstration of diligence by board members.
- **Financial threat (penalty regime):** The fines outlined in articles 61 through 64 represent a substantial financial threat. For essential entities, fines may reach up to €10 million or 2% of the preceding financial year’s annual worldwide turnover, whichever is higher. For important entities, fines may reach €7 million or 1.4% of the preceding financial year’s annual worldwide turnover, whichever is higher (article 61.2.b.i)). Given these severe penalties, organizations must treat compliance as a priority for mitigating financial risks, especially because negligence is also penalized under article 64.



---

## Framework and timeline (oversight action)

- **Subjective scope of application:** The initial classification of an entity as an essential entity or important entity is critical for compliance. This classification determines the obligations to be met, the type of minimum measures required, and the applicable penalty regime (articles 3–8). For this reason, management and governing bodies must ensure the entity is properly identified and registered on the designated electronic platform.
- **Timeline (applicability and entry into force):** The 120-day period for the decree-law to enter into force (article 11) and the 24-month timeline for certain provisions to take effect (article 10) are not an “excuse” to delay the implementation of the statute (where applicable), but rather the maximum deadline for its preparation. Management and governing bodies must closely monitor regulations issued by the CNCS, especially those that will govern the designated electronic platform, the national reference framework, the minimum measures to be adopted by covered entities, and certification.

---

## Obligations of management and governing bodies (duty of diligence)

- **Risk management system** (article 26): Management and governing bodies must oversee the implementation of a comprehensive and well-documented cybersecurity risk management system. At a minimum, this system must address:
  - risk analysis and management policies;
  - incident management;
  - business continuity;
  - supply chain security;
  - security throughout systems’ lifecycle; and
  - application of measures such as encryption and multifactor or continuous authentication.
- **Supply chain security** (article 28): As responsibility extends to the supply chain, covered entities must ensure that their direct suppliers comply with applicable security requirements. Management and governing bodies are required to enforce minimum security criteria, carry out contractual due diligence and ensure continuous monitoring of critical providers.
- **Residual risk management** (article 29): Entities must identify, document and manage residual risks that remain after implementing the minimum measures. Also, management and governing bodies must demonstrate no gaps were overlooked and ensure that the residual risks were consciously approved at the appropriate level.
- **Incident notification** (article 40): Incident notification applies to significant-impact incidents reported by essential entities, important entities and public entities, as stipulated in article 40. These notifications trigger mandatory legal deadlines defined in articles 42 through 44. Management and governing bodies are responsible for ensuring the existence of prepared plans, teams and operational processes that enable compliance with the following legal deadlines:
  - **24 hours:** Submit a rapid alert within 24 hours of incident verification (article 42.1).
  - **72 hours:** Update the initial notification within 72 hours (article 42.3).
  - **24 hours:** Submit an end-of-impact notification within 24 hours of the issue’s resolution (article 43.1.e)).



- **30 business days:** Provide a final report within 30 business days after the end-of-impact notification (article 44.1).

Fulfilling the above obligations requires robust procedures, clear internal reporting structures, simulations to ensure readiness, multidisciplinary coordination, and continuous documentation of all actions.

---

## Administrative duties and proof of compliance

- **Points of contact and registrations:** The appointment and communication of both the Cybersecurity Officer (article 31) and the Permanent Point of Contact (article 32) are mandatory. Compliance with the duty to register on the designated electronic platform, as required by articles 8.1 and 35, serves as a marker of an entity's maturity and as a communication channel for the purpose of supervision by the CNCS.
- **Annual report** (article 30): The annual report constitutes the primary evidence of the implementation of technical and organizational measures by covered entities. It must be prepared and substantiated by systematically collecting evidence throughout the financial year.
- **Certification** (article 34): Cybersecurity certification provides proof of compliance through an independent third party. Certification is issued by an accredited compliance assessment body or under a CNCS-recognized scheme (article 34). It strengthens the trust of clients, regulators and investors by certifying compliance with cybersecurity standards.

---

## Proof of security (legalization of ethical hacking)

**Proactive validation:** Article 7 of Decree-Law 122/2025 amends the Cybercrime Law by introducing article 8-A, which permits non-punishable acts performed in the public interest of cybersecurity, such as consensual ethical hacking. Management and governing bodies may authorize intrusive security tests to identify vulnerabilities. These actions benefit from a legal framework that exempts auditors and ethical hackers from criminal liability, provided legal requirements are met, thereby enhancing the demonstration of organizational due diligence.

---

## Next steps: Timeline and roadmap

The implementation process will be gradual, even though Decree-Law 125/2025 will enter into force **120 days after its publication** (article 11 of Decree-Law 125/2025). However, the effectiveness of certain provisions will depend on regulations to be issued by the CNCS.

This timeframe established for the decree-law to take effect and enter into force (articles 10 and 11 of Decree-Law 125/2025) should be treated as a preparatory period. Following the prescribed legal procedure, the CNCS is expected to approve and publish the implementation regulations. Specifically, these regulations will address the operation of the designated electronic platform, the National Cybersecurity Reference Framework, and the minimum cybersecurity measures. Once published, the **24-month period for certain provisions under the new regime to take effect** will start running (article 10.2 of Decree-Law 125/2025).

Meanwhile, CNCS launched the **NIS2 Roadmap** on November 27, an initiative offering 60 free training sessions across the country, including in the Madeira and Azores autonomous regions (not mentioned in the decree-law). This initiative seeks to empower and educate stakeholders on their new responsibilities, strengthen individual and organizational capabilities, while promoting a more resilient ecosystem and a true cybersecurity culture.



As noted above, the transition period should be treated as a critical phase for strategic planning and for laying the groundwork for compliance, rather than as a deferral of obligations.

---

## Conclusion

Decree-Law 125/2025, which establishes the new Legal Regime on Cybersecurity, elevates risk management to a core **management responsibility**, with direct implications for top-level leadership. By proactively embracing this framework, organizations move beyond mere compliance, strengthening trust, resilience and credibility to guarantee success in an increasingly complex digital ecosystem.

The Cuatrecasas team stands ready to support organizations in assessing whether they fall within the scope of Decree-Law 125/2025 and, where applicable, in designing and implementing a tailored and effective implementation strategy.



For additional information, please contact our **Knowledge and Innovation Group lawyers** or your regular contact person at Cuatrecasas.

©2025 CUATRECASAS

All rights reserved.

This document is a compilation of legal information prepared by Cuatrecasas. The information or comments included in this document do not constitute legal advice.

The intellectual property rights in this document are owned by Cuatrecasas. Reproduction in any medium, distribution, transfer, and any other use of this document, whether in its entirety or in excerpted form, are prohibited without Cuatrecasas's prior authorization.

