NEW LEGAL FRAMEWORK FOR CYBERSECURITY

Decree-Law No. 125/2025, of December 4

Decree-Law No. 125/2025, of December 4, transposes Directive (EU) 2022/2555 into Portuguese law, introducing a set of measures aimed at strengthening and harmonizing the cybersecurity framework within the European Union.

COVERED ENTITIES

To respond to the worsening cyber threats, capable of compromising the national security of various entities in multiple sectors, the new regime expands the set of entities covered, adjusting obligations to their size and relevance.

In fact, the regime applies to:

- **Public administration entities,** including agencies and services dependent on the State, except those with functions specifically excluded in the law (national security, defense and intelligence services, criminal investigation, and criminal police agencies)
- **Private entities considered essential or relevant to cyberspace security**, namely:
  - essential service operators,
  - critical infrastructure operators,
  - digital service providers,
  - entities whose size or nature of activity determines a high risk to the

Caldeira Pires - Sociedade Multidisciplinar de Advogados e Consultores, SP, S.A.
Av. da República, 45, 8.º Dto. 1050 -187 Lisboa E info@caldeirapires.pt T +351 210 991 736
www.caldeirapires.pt

continuity of essential services or to national security.

- **Other entities covered by specific sectoral criteria**, to be defined by the competent authorities within the National Cybersecurity Reference Framework.

MEASURES

On the other hand, **the regime also reinforces three central instruments of public cybersecurity policy:**

- **the National Cyberspace Security Strategy,** which sets strategic priorities and objectives;
- **the National Plan for Responding to Large-Scale Crises and Incidents**, which improves the management of these events; and,
- **the National Reference Framework for Cybersecurity**, which systematizes and disseminates norms, standards, and best practices.

This regime **also extends the existing institutional framework, strengthening the role of the National Cybersecurity Center as the national authority and creating sectoral and special supervisory authorities**, which contribute to a more balanced distribution of supervisory functions.

At the same time, a model of cooperation and interoperability is established between public entities with responsibilities in cybersecurity and internal and external security, promoting the effective circulation of information and coordination in the prevention, detection, and response to incidents.

Among the **main measures**, the following stand out:

- Definition of criteria for identifying entities covered by the regime and expansion of the set of entities covered by it;
- Differentiation between essential entities, important entities, and relevant public entities, for the purposes of applying the approved cybersecurity legal regime;
- Definition of the structural instruments for cyberspace security, such as the National Cyberspace Security Strategy, the National Plan for responding to large-scale cybersecurity crises and incidents, the National Reference Framework for Cybersecurity, the National Cyber Defense Strategy, and the Strategic Concept of National Defense;
- Regulation of ethical hacking, more specifically, activities aimed at identifying vulnerabilities inherent in company systems for reporting purposes;
- Strengthening of oversight, with the National Cybersecurity Center achieving the status of national cybersecurity authority;

- Cooperation between entities that are part of the institutional framework for cyberspace security and the private sector for the purposes of sharing information, adopting best practices, developing and/or improving classification systems for cybersecurity risk management measures, risk exposure or cyber threat indicators, incident handling procedures, crisis management, and vulnerability disclosure;
- Obligation for essential and important entities to prepare an annual report summarizing the main activities carried out in the field of network and information system security, including quarterly statistics on incidents and an aggregate analysis of significant incidents — covering affected users, duration, geographical distribution, and any cross-border impact;
- Mandatory notification of any significant incident by essential, important, and public entities to the competent cybersecurity authority;
- Provision for very serious, serious, and minor administrative offenses in the event of non-compliance with certain provisions set forth in the Decree-Law.

ENTRY INTO FORCE

This decree-law shall enter into force 120 days after its publication.

Inês Ferreira Lourenço
ines.fl@caldeirapires.pt