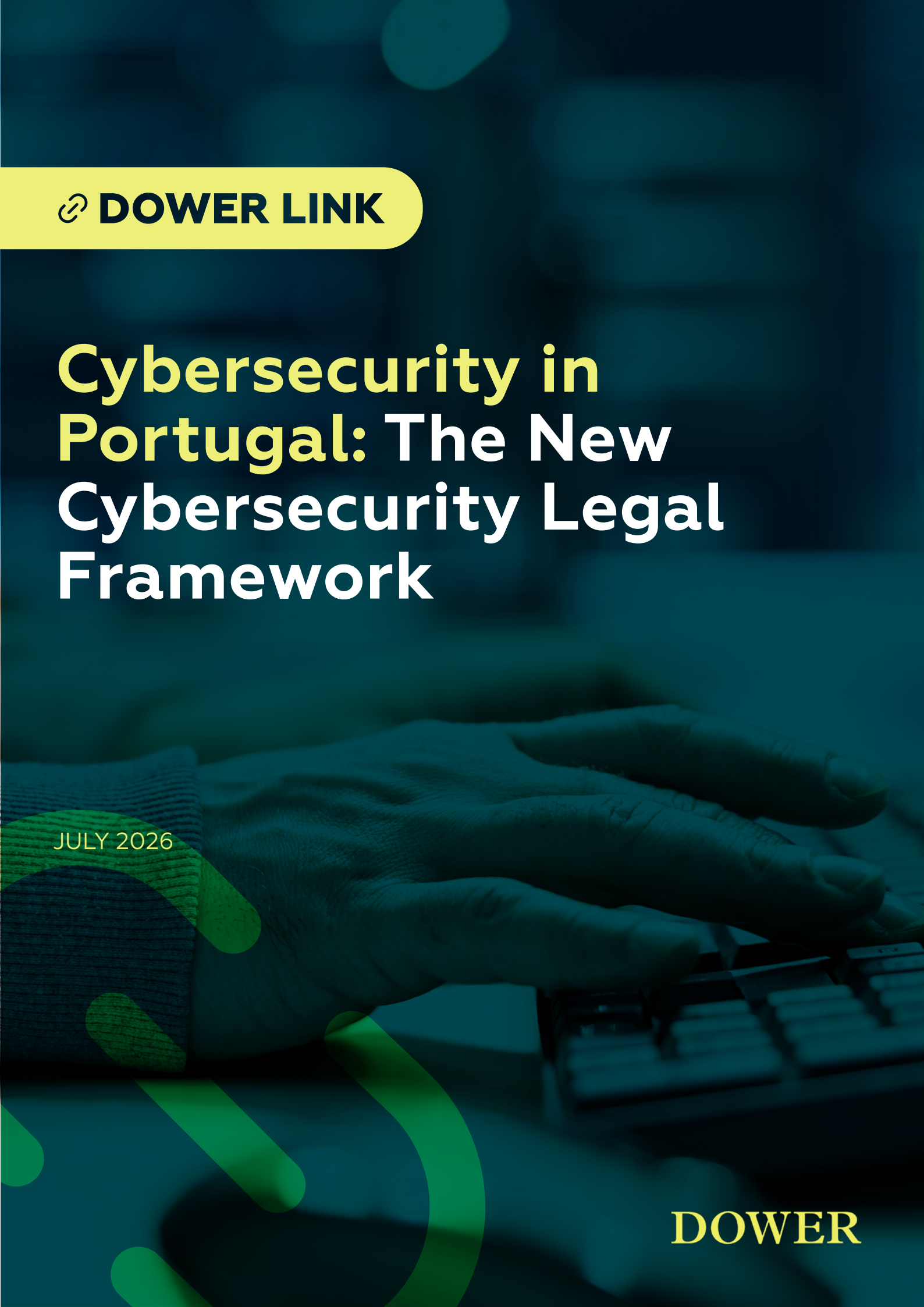
DOWER LINK

Cybersecurity in Portugal: The New Cybersecurity Legal Framework



JULY 2026

DOWER

Decree-Law No. 125/2025, which transposes the NIS2 Directive into Portuguese law and establishes the new Legal Framework for Cybersecurity, entered into force last April.

The NIS2 Directive was introduced to strengthen cybersecurity across the European Union.

Its main objectives are to:

i. Increase the digital resilience of organisations;
ii. Harmonise rules across Member States;
iii. Strengthen the response to cybersecurity incidents.

Who is covered by the Cybersecurity Legal Framework?

Essential entities: Entities operating in sectors of high criticality to society and the economy, such as energy, transport, healthcare, digital infrastructure, electronic communications, banking and certain financial services, among others provided for by law.

Important entities: Entities covered by the Cybersecurity Legal Framework that are not classified as essential. Their classification depends on the activity carried out in critical sectors, the size of the entity and the other criteria laid down by law.

Relevant public entities: Entities which, although not classified as essential or important, meet the specific requirements set out in the Cybersecurity Legal Framework, taking into account, in particular, the scope of the functions they perform or their size.

Although the legal framework generally applies to **medium-sized and large organisations**, it may also extend to **smaller entities where they meet the specific criteria** laid down by law, particularly having regard to the critical nature or significance of the services they provide.

So, what changes for organizations?

1. New responsibilities for senior management

Senior management is now expected to play an active role in cybersecurity. They must:

i. Approve cybersecurity risk management measures;
ii. Oversee their implementation;
iii. Ensure appropriate training;
iv. Ensure compliance with legal obligations.

2. Risk management is no longer optional

Essential and important entities must implement cybersecurity measures covering, among other areas:

i. Incident handling;
ii. Business continuity;
iii. Supply chain security;
iv. Basic cyber hygiene practices and cybersecurity awareness training;
v. Human resources security;
vi. Other appropriate cybersecurity measures.

Relevant public entities must implement the cybersecurity measures established by the National Cybersecurity Centre (CNCS) under Regulation No. 756/2026 of 22 June.

3. Cybersecurity Officer

Essential and important entities must appoint a Cybersecurity Officer, whose responsibilities include:

i. Proposing cybersecurity risk management measures;
ii. Providing information on cybersecurity risk management measures;
iii. Assisting with supervisory and enforcement requirements;

iv. Promoting a cybersecurity culture;
v. Managing residual cybersecurity risk;
vi. Ensuring the preparation of the annual report;
vii. Coordinating the activities of the permanent point of contact.

4. Incident notification

Entities covered by the RJC must notify the competent cybersecurity authority of significant cybersecurity incidents..

The reporting process includes:

i. Initial notification;
ii. Interim reports, where applicable;
iii. Notification that the significant impact has ended;
iv. Final report.

What happens in case of non-compliance?

The new framework provides for administrative fines of up to:

- **€10 million or 2% of the organization's** total worldwide annual turnover, whichever is higher, for legal entities;
- **€200,000** for natural persons.

Additional enforcement measures may also be imposed, including:

i. **Ancillary sanctions, s**uch as restrictions on business activities and the implementation of mandatory cybersecurity action plans; and
ii. **Periodic penalty payments.**

The Decree-Law has been in force since 3 April 2026.

Until 3 April 2027, entities subject to the Cybersecurity Legal Framework (RJC) may, upon submitting a reasoned request, apply for a waiver of imposed administrative fines.

On 23 June 2026, Regulation No. 756/2026 entered into force, establishing the practical implementation of the Cybersecurity Legal Framework in areas such as incident reporting and communication with the competent cybersecurity authority.

Is your organisation prepared?

Identifying the applicable obligations at an early stage and preparing your organisation accordingly are essential to ensuring compliance and strengthening digital resilience.

Privacy and Compliance Team
dower@dower.pt