JUN. 26

INFORMATIVE NOTE

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

Regulation of the Legal Framework for Cybersecurity

Background

The Regulation of the Legal Framework for Cybersecurity (Regulation 756/2026 of 22 June 2026 - the "Regulation") has been published in the Diário da República. It sets out the matters in the Legal Framework for Cybersecurity (Regime Jurídico da Cibersegurança – the "RJC"[1]), approved by Decree-Law 125/2025 of 4 December) that have been placed under the responsibility of the National Cybersecurity Centre (Centro Nacional de Cibersegurança – the "CNCS").

The draft Regulation was put out for public consultation between March and April. This resulted in dozens of contributions, some of which were reflected in the final text.

Scope of application

The Regulation applies to essential, important and relevant public entities as defined in the RJC. In particular, it governs:

The Regulation applies to essential, important and relevant public entities as defined in the RJC.

- The operation of the electronic platform, particularly with regard to the procedure for self-identification and classification of entities.
- Mandatory notifications of cybersecurity incidents and voluntary notifications of relevant information.
- Communications between organisations and the competent cybersecurity authority.
- The National Cybersecurity Reference Framework (QNRCS).
- The establishment of the Risk Matrix.
- The management of residual risk.

Pedro Lomba
Marta Salgado Areias
Mafalda de Brito Fernandes
Technology, Media and Telecommunications team

1 Legislation transposing Directive (EU) 2022/2555 ("NIS 2 Directive") into Portuguese law.

- Compliance levels and minimum mandatory cybersecurity measures for covered entities.
- The rules relating to the appointment of the cybersecurity officer and the permanent point of contact.
- Matters whose application depends on technical instructions or other regulations issued by the competent cybersecurity authority, including technical criteria and operational mechanisms relating to the platform and notifications.

MyCiber online platform

The MyCiber online platform, which is developed and managed by the CNCS and available at MyCiber.gov.pt, centralises registration, classification, mandatory reporting, incident notification and the dissemination of information by the competent authorities.

The platform operates on the principle of a single declaration, with exemption from providing information that is already available. Each entity has a single account, a secure area, delivery receipts and authentication via the Citizen Card, Digital Mobile Key or equivalent mechanisms, including those issued in other EU Member States. Notifications are sent to the secure area with email alerts. This does not affect the posting of summonses and final administrative offence decisions. An indicative simulator is also available, though it is not binding on the CNCS.

Self-identification and classification

Entities already in operation must complete registration within 60 days of the platform becoming available, and entities commencing operations must complete registration within 30 days.

Entities subject to the RJC must identify themselves on the platform by completing an online form. The form requires details such as the entity's name, tax identification number (NIF), the sector(s) and sub-sector(s) in which it operates, its legal status, its address, its up-to-date contact details, the number of its employees, and its CNCS code. The CNCS, together with the relevant authority for the sector where applicable, determines whether the entity falls within the scope of the RJC. The entity has 10 working days to submit comments. If no comments are submitted, a Classification Decision is issued, upon which the RJC's obligations apply, without prejudice to the remedies provided for in the Code of Administrative Procedure.

Entities already in operation must complete registration within 60 days of the platform becoming available, and entities commencing operations must complete registration within 30 days, failing which administrative penalties may be imposed. Each entity is responsible for the data and information submitted via the platform and must keep it permanently up to date.

The classification may be amended at any time by the competent authority depending on changing circumstances.

Communication of the cybersecurity officer and permanent point of contact must be made using the form available in the restricted area of the electronic platform.

If it is concluded that the organisation is not covered by the RJC, its provisional registration will be cancelled within 90 days at most. However, the competent cybersecurity authority will retain the self-identification form and the corresponding notification of exclusion for as long as it deems necessary.

Financial institutions

Following registration and classification, financial institutions that are covered by both the RJC and Regulation (EU) 2022/2554 (DORA) and Law 73/2025 of 23 December, must submit reports and notifications regarding digital operational resilience to the authorities specified in the applicable special legislation. However, they must comply with the RJC's obligations regarding the appointment of a cybersecurity officer, a permanent point of contact, and incident reporting.

Submission of documents

Critical entities must submit the annual report required by Article 30 of the RJC to the relevant cybersecurity authority via the restricted area of the electronic platform each year. Important entities must submit the annual report to the CNCS whenever requested to do so.

Cybersecurity officer and permanent point of contact

Communication of the cybersecurity officer and permanent point of contact must be made using the form available in the restricted area of the electronic platform. For organisations that were already in existence on the date that the RJC came into force, the 20-working-day time limit begins on the date that the organisation is notified of its classification.

Mandatory incident reporting

Mandatory incident reports, as set out in Articles 40 to 44 of the RJC, must be submitted using the form in the restricted area. Automated alerts of upcoming deadlines. 'Significant impact' is defined by Implementing Regulation (EU) 2024/2690 for the entities specified therein, and by a technical instruction from the CNCS for all others. Voluntary notifications of incidents, cyber threats, near incidents or vulnerabilities can be submitted without authentication via the platform.

Pursuant to Article 45 of the RJC, voluntary notifications of incidents, cyber threats, near incidents or vulnerabilities may be submitted by any natural or legal person without the need to log in to the platform.

The National Cybersecurity Reference Framework (QNRCS)

The QNRCS, set out in Annex I, is the national reference framework for cybersecurity management norms, standards, and best practices. It is structured around objectives, categories, and controls. The QNRCS should be applied with a view to continuous improvement. It is updated by the CNCS at least every five years, and its optional use must be combined with the minimum measures set out in Annex III.

Voluntary certification

Public bodies that are essential, important and relevant may benefit from a presumption of compliance with cybersecurity measures by means of a certificate issued by an accredited body. This can include EC QNRCS, ISO/IEC 27001 with full scope covering the relevant systems, or another approved scheme. Any changes affecting the certificate must be reported within 72 hours in the event of revocation or within ten working days in all other cases. In justified cases, the competent authority may also require national, European or international certification.

Compliance levels and minimum cybersecurity measures

The Regulation sets out three compliance levels – basic, substantial, and high – derived from the Risk Matrix (see Annex II). This matrix takes into account factors such as the sector, size, and associated risk. Covered entities must implement the measures set out in Annexes III and IV as a minimum, including those at lower levels if they are subject to substantial or high levels. In the event of overlap, the more stringent level applies. The measures cover areas including assets, identities and access, data, technological infrastructure, monitoring, incidents, training and the supply chain.

Risk management

A risk analysis must be carried out at least once a year or following notification from the CNCS regarding an emerging threat or vulnerability. The analysis must take into account the history of incidents, users affected, duration, geographical distribution and cross-sectoral dependencies. Entities must submit an initial list of relevant publicly accessible assets within six months of being notified of their designation, or by 31 January of the following year, whichever is sooner. They must also update this list annually and treat it as sensitive information.

A risk analysis must be carried out at least once a year or following notification from the CNCS regarding an emerging threat or vulnerability.

Entry into force and application

The Regulation came into force on 23 June 2026. Its provisions apply immediately, unless they are subject to specific transitional arrangements or require technical instructions or supplementary measures. This includes the rules governing the functioning of the electronic platform, self-identification, classification and communications with the competent cybersecurity authority, provided they can be implemented immediately.

PL
MJ

The 24-month transitional period established by the Legal Framework for Cybersecurity (RJC) applies to the following obligations and annexes in particular:

- The minimum cybersecurity measures set out in Annexes III and IV - for essential and important entities at basic, substantial and high levels, and for relevant public entities in Groups A and B respectively - are to be implemented pursuant to Articles 26 and 33 of the RJC.
- The Risk Matrix set out in Annex II is applied as the instrument for determining the applicable compliance levels for essential and important entities.
- This includes the obligation to periodically assess and manage risks and residual risks, as well as the requirement to carry out risk assessments at least annually and to assess residual risk following the implementation of cybersecurity measures.
- Mandatory notification of significant incidents, including initial notification, notification of the end of significant impact, and final or interim reports. This is without prejudice to any obligations arising directly from the RJC or applicable European legislation.
- Submission of the list of publicly accessible assets and its periodic updating depends on the classification of the entity and the operational implementation of the applicable regulatory mechanisms.

Recommended actions

Entities potentially covered by the Regulation are recommended to adopt the following measures in particular:

- Confirm compliance with the RJC and complete the self-identification process on the MyCiber platform, providing the necessary information on the form.
- Identify the obligations that are already enforceable and those covered by the 24-month transition period, including the associated classification deadlines.
- Appoint a cybersecurity officer and a permanent point of contact, and submit the communication on the platform.
- Conduct a gap analysis against the applicable minimum requirements and review incident management and reporting procedures.
- Ensure compliance with data protection regulations and consider obtaining voluntary certification. Monitor technical instructions, guidelines or other regulations issued by the CNCS. ■

This document is intended for general distribution to clients and colleagues, and the information contained in it is provided as a general and abstract overview. It should not be used as a basis on which to make decisions and professional legal advice should be sought for specific cases. The contents of this document may not be reproduced, in whole or in part, without the express consent of the author. If you require any further information on this topic, please contact **Pedro Lomba (pedro.lomba@plmj.pt)** or **Marta Salgado Areias (marta.salgadoareias@plmj.pt).**