MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS

LEGAL ALERT

CYBER RESILIENCE ACT

Framework

The Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act, CRA or the Act)) was published on 20 November 2024.

The Cyber Resilience Act aims to strengthen the cybersecurity of products with digital elements across the board, by mitigating vulnerabilities through the implementation of uniform legal requirements applicable throughout the European Union (EU).

The main objectives of implementing the Act are:

- Mitigate vulnerabilities in connected hardware and software products;
- Ensure greater transparency regarding the security features of products with digital elements available on the European market;
- Promote the responsibility of economic operators at all stages, from the manufacture to the commercialisation of products on the market; and
- Guarantee a high level of protection for users against cybersecurity risks.

Scope of application

The CRA covers a wide range of products with digital elements, including hardware, software, and integrated solutions, which have direct or indirect connectivity with devices or networks. Some examples include:

- Consumer devices (smartphones and other connected devices) – IoT;
- Network and security equipment (firewalls, routers);
- Software solutions (operating systems, SaaS);
- Edge computing devices.

Although the CRA has a broad scope, it does provide for some exceptions: *(i)* this is the case for devices with digital elements that are already regulated on a sectoral basis, such as equipment and software intended for medical diagnosis or treatment, products with software and components related to aviation safety, spare parts intended solely for the replacement of identical components placed on the market before the Act came into force, and *(ii)* products developed specifically for defence or national security purposes.

With regard to open-source code, in cases where it is free software used for research or innovation purposes, provided that *(i)* it is not marketed directly and *(ii)* it is not used as the main component in monetised products, it is excluded from the scope of the Act. However, in cases where it is commercialised or monetised, it will be subject to the provisions of the Act.

Finally, it should be noted that all products with digital elements made available on the market before 11 December 2027, will only be covered by the Act if they undergo substantial changes after that date (*i.e.* changes of purpose or significant security risks).

Classification of products with digital elements

One of the Act's novelties concerns the classification of these products based on the risk of impact in the event of vulnerabilities being identified and exploited. It distinguishes between them as follows:

Important products (Class I)

- By way of example, this includes IoT devices such as smart locks, cameras and connected toys;
- They require robust conformity assessments, but these are generally carried out in-house.

Critical products (Class II)

- These include security systems, such as firewalls, and products that control central network or data functions;
- They are subject to strict conformity assessment processes through rigorous external certification processes.

New conditions and obligations

Evaluation and compliance

- All products covered by the Act must undergo safety checks before being placed on the market;
- If the products are considered general or important, the assessment can be carried out by the manufacturer;
- If they are classified as critical products, assessment by a certified third party is mandatory.

Integration of third-party components

- Manufacturers must provide security updates during the support period in order to minimise any vulnerabilities throughout the product's life cycle;
- Significant changes to products, such as updates that modify the original purposes, may require new conformity assessments.

Updates and lifecycle management

- Suppliers must provide security updates during the support period in order to minimise any vulnerabilities throughout the product's life cycle;
- Significant changes to products, such as updates that modify the original purposes, may require new conformity assessments.

Providing users with clear and accessible information

- Transparency about the product's security features;
- Specification of the support period and the frequency of security updates.

Support to micro, small and medium-sized enterprises

- Implementation of specific support programmes such as financial assistance and cybersecurity training;
- Creating secure environments for compliance testing.

Penalties

The organisations concerned must therefore prepare themselves to incorporate the requirements in question, under penalty of fines for non-compliance, which can be as high as the following amounts:

- Up to EUR 15,000,000 or, if the offender is an undertaking, up to 2.5% of its total worldwide annual turnover for the preceding financial year, whichever is higher, for non-compliance with essential cybersecurity requirements;
- Up to EUR 10,000,000 or, if the offender is an undertaking, up to 2% of its total worldwide annual turnover for the preceding financial year, whichever is higher, for non-compliance or non-compliance with other requirements;
- Up to EUR 5,000,000 or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher, for providing incorrect, incomplete or misleading information to notified bodies and supervisory authorities.

Responsibility for imposing these fines will lie with the national market surveillance authorities, which will additionally have the power to: *(i)* monitor compliance with the rules; *(ii)* order the withdrawal of non-compliant products from the market; and *(iii)* coordinate actions with other entities, such as ENISA, to guarantee the implementation of the regulatory provisions.

Next Steps

For companies that produce or distribute products with digital elements in the EU, it is essential to adopt the following measures:

- **Review product portfolios** to determine which items are covered by the CRA;
- **Implement initial and regular compliance processes**, including internal audits and documentation of cybersecurity features;
- **Preparing external audits and certifications** on critical products;
- **Ensure adequate technical support** for security updates throughout the product lifecycle;
- **Train its internal teams and suppliers** on the requirements of the Act to avoid non-compliance and penalties.

It is important to note that the CRA will be implemented in phases, as follows:

The Act shall be fully applicable as from 11 December 2027, without prejudice to the following:

- Chapter IV, which refers to the notification of conformity assessment bodies, will apply from 11 June 2026; and
- Article 14, which lays down the information obligations to be provided by manufacturers, will apply from 11 September 2026.

For more details on how these changes could impact your organisation, feel free to contact our team.

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS

David Silva Ramalho
Nicole Fortunato
Márcia Tomás Pires
Ana Xavier Nunes