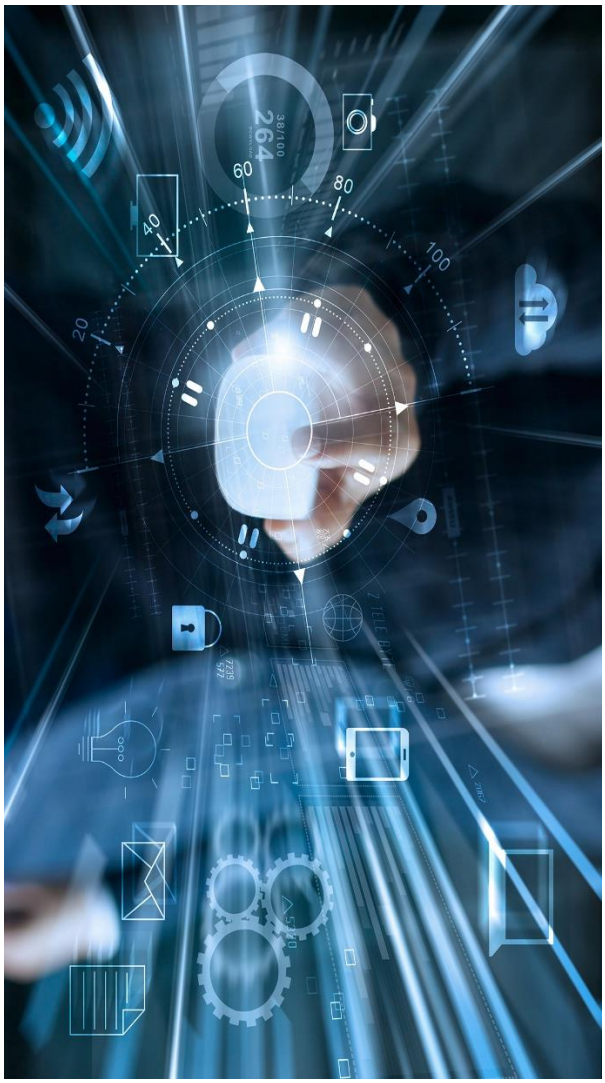
CUATRECASAS

Cyber Resilience Act

Published the Cyber Resilience Act, setting unified cybersecurity standards for digital products across the EU Market

Legal Flash

November 20, 2024



Key aspects

The Cyber Resilience Regulation (Regulation (EU) 2024/2847 of the European Parliament and of the Council) was published today in the Official Journal of the EU, thereby concluding the legislative process for approving this regulation, which has been ongoing since mid-2022 following the European Commission's proposal. These are some of its key aspects:

- Manufacturers must integrate **security measures** from the design phase and ensure CE marking;
- Importers and distributors are responsible for verifying **product cybersecurity standards**;
- Timely reporting of **vulnerabilities and incidents** is mandatory for manufacturers;
- Significant penalties are imposed for noncompliance, with exemptions for small enterprises.

Cyber Resilience Act

The Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (hereinafter, "**CRA**") introduces comprehensive cybersecurity requirements for hardware and software products with digital elements placed in the European Union ("**EU**"). Among other products with digital elements covered under the scope of the CRA, the regulation applies to network management, operating or password systems, smart home general purpose virtual assistants, smartcards or similar devices, alongside hardware devices with security boxes.

Before the CRA was approved, various national and EU-level initiatives addressed cybersecurity challenges in a fragmented way, creating an inconsistent regulatory framework across the internal market. Specifically, while existing EU legislation (e.g., Directive (EU) 2022/2555 [NIS2 Directive] and Regulation (EU) 2019/881 [Cybersecurity Act]) addresses various aspects of cybersecurity from different perspectives, none currently impose mandatory security requirements specifically for products with digital elements.

The CRA is particularly important due to the cross-border nature of cybersecurity risks. Products developed in one country are frequently used by businesses and consumers throughout the entire EU, underscoring the need for a unified regulatory framework.

Following the above, economic operators (i.e. manufacturers, importers, distributors, and authorized representatives) have specific roles in ensuring that products with digital elements are secure and compliant with the CRA before they are placed within the EU. The requirements differ between manufacturers and importers or distributors, and depending on whether the products with digital elements are defined as important products (Annex III of the CRA) or critical products (Annex IV of the CRA).

Manufacturers, importers and distributors

Manufacturers[1] are required to incorporate cybersecurity measures from the outset, ensuring that products are designed, developed, and produced securely. These measures include:

- promoting rigorous evaluations for each product to identify and mitigate any cybersecurity risks during design and development;

[1] Defined in Article 3.13 of the CRA as the "*natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge*".

- maintaining detailed records showing how cybersecurity risks were addressed, making this information available to regulatory bodies if necessary;

- keeping the information and instructions to the user set out in Annex II at the disposal of users and market surveillance authorities for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer[2];

- ensuring that products display a CE mark, indicating they comply with the necessary standards and can be safely sold across the EU; and

- setting up processes for handling potential cybersecurity issues that arise after the product is released, such as providing security updates and advising users on how to manage vulnerabilities.

The CRA introduces the role of the authorized representative which shall be appointed and authorized by the manufacturer to perform the tasks specified in the written mandate received from the manufacturer which shall allow the authorized representative to (i) keep the EU declaration of conformity and the technical documentation at the disposal of the market surveillance authorities for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer; (ii) provide that authority with all the information and documentation necessary to demonstrate the conformity of the product with digital elements, and; (iii) cooperate with the market surveillance authorities, at their request.

As for importers[3] and distributors[4], the accountability lies on the need to verify, assess, and guarantee that the products that are being sold are safe and comply with cybersecurity standards. For example, importers must verify that products meet all cybersecurity requirements before they are marketed, including checking the CE marking and proper documentation. Distributors must stay alert to any emerging security issues and ensure that the products they handle remain compliant over time.

The CRA identifies a set of cybersecurity measures that must be applied by manufacturers and verified by importers and distributors, including the following:

- **Security by design**: Products must be developed with security in mind from the outset. This includes incorporating protective measures to prevent unauthorized access and ensuring the integrity and confidentiality of any data processed.

[2] Where such information and instructions are provided online, manufacturers shall ensure that they are accessible, user-friendly and available online for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.
[3] Defined in Article 3.16 of the CRA as the "*natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the EU*".
[4] Defined in Article 3.17 of the CRA as the "*natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties*".

- **Protection of critical products**: Products that perform essential cybersecurity functions or pose an elevated risk if compromised – such as firewalls or intrusion prevention systems – face stricter security requirements. These products must undergo more thorough assessments to ensure their robustness.

- **Vulnerability management**: All products must have a plan for managing vulnerabilities during their entire lifecycle. Manufacturers are expected to provide security updates, patches, and instructions to mitigate risks as they arise. This is especially important for critical products (listed in Annex IV of the CRA), where timely updates are essential to maintain security.

- **Supply chain security**: Economic operators must carefully manage the cybersecurity risks associated with third-party components used in their products, including open-source software. The level of scrutiny depends on the nature of the component and its associated risks. Manufacturers should ensure that any third-party components, including software, are secure, regularly updated, and free from known vulnerabilities.

- **Security updates and support**: Modifications to a product, whether through software updates or hardware changes, can affect its cybersecurity status. For instance, a feature update that introduces new functionalities could increase the product's potential exposure to cyber threats, requiring a new risk assessment. However, not all updates are considered substantial. Minor patches, such as bug fixes or interface improvements, typically do not change a product's overall security risk. However, more significant changes, especially those that affect core functionalities, require closer scrutiny to ensure they do not introduce new vulnerabilities. In situations where a product's modification significantly alters its intended purpose or risk profile, it may need to go through a new conformity assessment. This ensures that the product continues to meet the required security standards after major updates or changes.

When it comes to **open-source software**, economic operators must take special consideration when integrating this type of software into commercial products. While open-source projects not intended for commercial use may be exempt from certain obligations, any product that incorporates open-source components in a commercial context must ensure those components meet cybersecurity standards. For open-source software stewards—organizations that provide long-term support for such projects—a more flexible approach is applied. However, commercial products that incorporate these components must still meet the full security requirements.

In addition to the above, it is worthy saying the CRA introduces some cases in which manufacturers obligations apply to importers and distributors. Specifically, when the importer or distributor places a product with digital elements on the market under its name or trademark or carries out a substantial

modification of a product with digital elements already placed on the market. In such cases, under the CRA, the importer or the distributor will be subject to the manufacturers' obligations set forth in the CRA.

Incident response and notifications

The notification requirements within the CRA aim to ensure transparency, rapid response, and collaborative efforts among manufacturers, the European Union Agency for Cybersecurity ("**ENISA**"), and the Computer Security Incident Response Teams ("**CSIRTs**") network. The CRA mandates that manufacturers of products with digital elements must notify the pertinent entities about **actively exploited vulnerabilities** and **cybersecurity incidents classified as severe**. Incidents will be classified as severe if they negatively affect the product's ability to protect sensitive data or functions, or if they lead to the introduction or execution of malicious code into a system, causing cybersecurity risks to the product with digital elements.

The process and timelines for notifying both exploited vulnerabilities and severe incidents follow the current modus operandi of most of the cybersecurity legislation—namely, through the following main notifications:

- An **early warning notification** must be submitted **within 24 hours of becoming aware** of the vulnerability or incident, specifying relevant information such as whether the incident resulted from unlawful or malicious acts.
- An **interim** and more detailed incident notification must follow **within 72 hours**, providing broader context, including the nature of the vulnerability or incident, corrective measures already taken, and potential mitigation steps users can adopt.
- A **final report** is due within **one month**, detailing the severity of the vulnerability, potential malicious actors involved, and comprehensive mitigation steps.

Under exceptional circumstances, manufacturers may request an extension for providing a notification, particularly if a vulnerability is subject to ongoing coordinated vulnerability disclosure. However, this extension is strictly time-bound and dependent on cybersecurity-related grounds.

Manufacturers must notify the **CSIRT** designated as coordinator and **ENISA** simultaneously. This notification must be submitted via a **single reporting platform** managed by ENISA, facilitating streamlined communication with all CSIRTs across the EU.

In cases of actively exploited vulnerabilities or severe incidents, manufacturers are required to inform impacted users, providing details on risks and mitigation actions. If the manufacturer fails to inform users, the notified CSIRTs can take over the communication responsibility, ensuring crucial security information is disseminated.

Also, following other cybersecurity legislation and reference frameworks, the voluntary sharing of cybersecurity threats, vulnerabilities and incidents is to be maintained in the CRA. Therefore, manufacturers and other stakeholders can voluntarily notify vulnerabilities or incidents to ENISA or the CSIRTs network. This voluntary approach encourages a collaborative cybersecurity environment, enhancing transparency and resilience across the industry.

Notification of conformity assessment bodies

Member States are specifically mandated to designate and inform the European Commission and the other Member States of the conformity assessment bodies they recognize as competent to carry out assessments for compliance with the CRA.

These bodies are entrusted with evaluating whether products with digital elements meet the cybersecurity criteria required by the CRA. This notification process aims to create a standardized approach across the EU, ensuring that all designated bodies adhere to the same high standards of assessment.

To qualify for notification, conformity assessment bodies must meet certain stringent criteria, which include the following:

- **Independence and impartiality**: These bodies must operate independently from manufacturers, thereby avoiding any conflicts of interest and ensuring unbiased assessments.

- **Technical competence**: They must possess the necessary expertise and resources to accurately evaluate products against the requirements set out in the CRA.

- **Quality management**: Designated bodies are expected to implement robust quality management systems that guarantee consistency and reliability in their assessments.

Compliance and market surveillance

In a similar vein, Member States are required to appoint market surveillance authorities responsible for monitoring compliance with CRA—currently, Portuguese governmental bodies have not yet designated any authorities. These authorities are instrumental in ensuring that products placed on the market consistently meet the required cybersecurity standards.

Their responsibilities include **actively monitoring the market** to ensure compliance with cybersecurity regulations, which involves regular inspections, testing, and evaluations of products available for sale.

These authorities also have the **power to investigate products** suspected of noncompliance, conduct audits, review technical documentation, and assess the CE marking along with the EU declaration of conformity.

If noncompliance is identified, market surveillance authorities have the authority to take **corrective actions**. This may necessitate manufacturers ceasing the sale of noncompliant products, withdrawing them from the market, or recalling them from consumers altogether.

To systematically identify and address noncompliance, market surveillance authorities are encouraged to conduct coordinated control actions, commonly referred to as **sweeps**. These predominantly involve simultaneous inspections of specific products or categories across multiple Member States, with the results being aggregated and made publicly available.

Confidentiality and penalties

Note that CRA places significant emphasis on confidentiality and the enforcement of penalties. The primary objectives of these confidentiality provisions are to safeguard sensitive information while ensuring the regulatory framework operates effectively without compromising intellectual property rights or national security.

In terms of enforcement, CRA requires that Member States establish effective and proportionate penalties for infringements, namely:

- **Infringements of essential cybersecurity requirements**: Up to €15 million or 2.5% of the offender's total worldwide annual turnover, whichever is higher.
- **Infringements of general obligations**: Up to €10 million or 2% of the offender's total worldwide annual turnover, whichever is higher.

- **Providing misleading information**: Up to €5 million or 1% of the offender's total worldwide annual turnover, whichever is higher.

Naturally, when determining the administrative fine amount, relevant circumstances such as the nature, seriousness and duration of the infringement must be carefully considered. Specific provisions also exempt certain entities from penalties. For example, manufacturers classified as microenterprises or small enterprises may be exempt from penalties for certain noncompliance issues related to deadlines. This same exemption also applies to open-source software stewards for any infringements of the CRA.

Next steps for businesses

To help implement the CRA, the European Commission will provide guidance, especially aimed at small and medium-sized enterprises (**SMEs**). This support will help economic operators understand how to implement the necessary cybersecurity measures effectively. Companies are also given a transitional period to adapt products already on the market to the new cybersecurity requirements, allowing them to continue operating without immediate disruption while they make the necessary adjustments.

The next steps for economic operators, particularly manufacturers, will be to perform a gap analysis on the existing cybersecurity measures in place, not only on an organizational level, but also for the manufacturing of their products with digital elements. This gap analysis must be focused on a risk-based approach, including supply chain risk, and on the manufacturers' capabilities to detect and respond to arising vulnerabilities.

The Regulation will be applicable from December 11, 2027, although Article 14, concerning the information obligations of manufacturers, will be applicable from September 11, 2026; and Chapter IV, concerning the notification of conformity assessment bodies, will be applicable from June 11, 2026.

For additional information please contact your regular contact at *Cuatrecasas.*