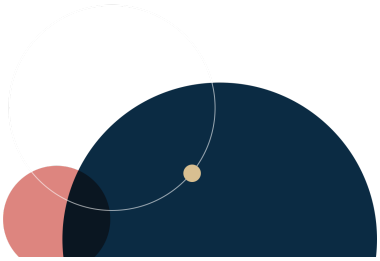
Steptoe

STEPTECHTOE | DECEMBER 16, 2024

The EU Cyber Resilience Act Has Entered into Force

10 THINGS YOU NEED TO KNOW ABOUT IT

Authors
Anne-Gabrielle Haie, Maria Avramidou



Overview

The EU Regulation on horizontal cybersecurity requirements for Products with Digital Elements (Cyber Resilience Act) entered into force on December 10, 2024. The Cyber Resilience Act introduces **harmonized rules for the placing on the market of connected hardware and software products, mandatory cybersecurity requirements for such products** and **corresponding obligations for all actors across the value chain.** It will have an important impact on companies that **design, develop, produce and make available such products on the EU market**. Below, we elaborate on 10 things that organizations need to know about the Cyber Resilience Act.

1. What Is the Purpose of the Cyber Resilience Act?

The Cyber Resilience Act aims to **complement and make the existing EU cybersecurity legislative framework more coherent**, **ensuring that Products with Digital Elements**, for example "Internet of Things" products, **are secure throughout their lifecycle**. Accordingly, it aims to ensure that Products with Digital Elements made available on the EU market have fewer vulnerabilities and that actors across the value chain remain responsible for their cybersecurity. Moreover, the Cyber Resilience Act envisions to enable users to take cybersecurity into account when selecting and using Products with Digital Elements, for example by improving transparency with regard to the support period for Products with Digital Elements made available on the EU market.

2. Who Does the Cyber Resilience Act Apply to?

The Cyber Resilience Act notably applies to:

- **Manufacturers** of Products with Digital Elements;

- **Importers** of Products with Digital Elements;
- **Distributors** of Products with Digital Elements; and
- **Open-source software stewards.**

It must be noted that the Cyber Resilience Act has an **extraterritorial effect** and it applies to any company that manufactures, imports or distributes on the EU market Products with Digital Elements, irrespective of its location or establishment.

3. What Does the term "Product with Digital Elements" mean?

"Product with digital elements" is defined as a **software or hardware product and its remote data processing solutions,** including software or hardware components being placed on the market separately. Overall, the Cyber Resilience Act applies to a broad range of products that are connected directly or indirectly to a device or network, including hardware and software. This includes connected home cameras, connected home appliances, connected toys, smartphones, laptops, modems, firewalls, and smart meters, etc.

The Cyber Resilience Act **excludes from its scope** the following Products with Digital Elements:

- Products with Digital Elements subject to **Medical Devices** Regulation; **In vitro Diagnostic Medical Devices** Regulation; and Regulation on **type-approval requirements for motor vehicles and their trailers;**
- Products with Digital Elements that have been certified in accordance with Regulation related to **civil aviation**;
- Equipment subject to Directive related to **marine equipment;**
- **Spare parts** that are made available on the market to replace identical components in Products with Digital Elements and that are **manufactured according to the same specifications as the components that they are intended to replace**;
- Products with Digital Elements developed or modified exclusively for **national security or defense purposes** or to products specifically **designed to process classified information**.

4. Which Obligations Does the Cyber Resilience Act Impose?

The Cyber Resilience Act imposes a series of cybersecurity obligations for manufacturers, importers, distributors and authorized representatives of Products with Digital Elements as well as for open-source software stewards, based on their roles and responsibilities along the value chain. Below we examine the **main obligations that these actors have to comply with**.

4.1 Manufacturers

Manufacturers are natural or legal persons who develop or manufacture Products with Digital Elements or have Products with Digital Elements designed, developed or manufactured, and market them under their name or trademark, whether for payment, monetization or free of charge. They must notably:

- Undertake an **assessment of the cybersecurity risks** associated with their products;
- **Design, develop, and produce products in accordance with the essential cybersecurity requirements**set out in Annex I, Part I (e.g., to ensure an appropriate level of cybersecurity of those products based on the risks at hand; etc.);
- Draw up **technical documentation**, which must include the cybersecurity risk assessment;

- Draw up **information and instructions** set out in Annex II;
- For certain Products with Digital Elements, carry out a **conformity assessment** procedure;
- Draw up an **EU declaration of conformity** and affix a **CE marking**;
- Conduct **due diligence when integrating components sourced from third parties** in Products with Digital Elements;
- **Document relevant cybersecurity aspects concerning the product** (incl. vulnerabilities), and, where applicable, **update the risk assessment of the product**;
- Ensure that **vulnerabilities** of the product **are handled effectively** and in accordance with the essential requirements set out in Part II of Annex I;
- Keep **technical documentation and EU declaration of conformity at the disposal of the market surveillance authorities** for at least 10 years after the product has been placed on the EU market;
- Put in place **procedures for products that are part of a series of production** to remain in conformity with the Cyber Resilience Act;
- Where it knows or has reason to believe that the product or processes put in place are not in conformity with the Cyber Resilience Act, take appropriate **corrective measures;**
- Upon request from a market surveillance authority, provide all **information to demonstrate the conformity** of the product;
- **Before ceasing its operations, inform the relevant market surveillance authorities** and, to the extent possible, the **users** of the concerned Products with Digital Elements placed on the market;
- Within 24 hours, **notify both CSIRT and ENISA** simultaneously of **any actively exploited vulnerability** or **severe incident**.
- **Without undue delay, inform users** about an **actively exploited vulnerability** or a **severe incident** and **possible corrective measures**;
- Appoint **authorized representative**.

4.2 Importers

Importers are natural or legal persons established in the Union who place on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union. They must notably:

- Only **place on the EU market products that comply with the essential cybersecurity requirements;**
- **verify that the manufacturer has complied with its obligations** related to conformity assessment, technical documentation, CE marking and attestation of conformity, and information and instructions for use, product identification, contact details, and support period information;
- Indicate **contact details and registered trade name / trademark on the product's packaging or accompanying documentation**;
- Where an Importer knows / has reason to believe that the product or processes put in place are not in conformity with the Cyber Resilience Act, take appropriate **corrective measures;**
- **When identifying a vulnerability, inform manufacturer and market surveillance authority** in case of a significant cybersecurity risk;
- For 10 years, keep a copy of **EU declaration of conformity and technical documentation;**

- Upon request from a market surveillance authority, provide all **information to demonstrate the conformity of the product;**
- Where it becomes aware that the **manufacturer has ceased its operations, inform market surveillance authorities and**, to extent possible, **users**.

4.3 Distributors

Distributors are natural or legal persons in the supply chain, other than the manufacturer or the importer, that make a product with digital elements available on the Union market without affecting its properties. They must notably:

- **Verify that manufacturers and importers have complied with certain of their obligations;**
- Only **make available on the EU market products that comply with the essential cybersecurity requirements;**
- Where a product poses a **significant cybersecurity risk**, **inform the manufacturer and the market surveillance authority**;
- Where they know / have reason to believe that the products or processes are not in conformity, make sure that the appropriate **corrective measures** are taken;
- When identifying a **vulnerability, inform manufacturer**;
- Upon request from a market surveillance authority, provide all **information to demonstrate** the **conformity** of the product;
- Where it becomes aware that the **manufacturer has ceased its operations, inform market surveillance authorities and**, to extent possible,

4.4 *Open-source Software Stewards*

Open-source software stewards are legal persons, other than a manufacturer, that have the purpose or objective of systematically providing support on a sustained basis for the development of specific Products with Digital Elements, qualifying as free and open-source software and intended for commercial activities, and that ensure the viability of those products. They must notably:

- Put in place and document a **cybersecurity policy** to foster the secure development of a product with digital elements and effective handling of vulnerabilities by the developers of that product and share it with market surveillance authorities, upon their reasoned request, and
- **Cooperate with the market surveillance authorities** with a view **to mitigating the cybersecurity risks** posed by a product with digital elements qualifying as free and open-source software.

5. How are Products with Digital Elements classified under the Cyber Resilience Act?

The Cyber Resilience Act classifies Products with Digital Elements into three main categories depending on their risks:

- **Default Products with Digital Elements:** These are basically products that are not explicitly listed as either important or critical. For these products, compliance with the Cyber Resilience Act is done through a self-assessment;

- **Important Products with Digital Elements:** These products present a higher cybersecurity risk by performing a function which carries a significant risk of adverse effects in terms of its intensity and ability to damage the health, security or safety of users of such products. It includes notably smart home products with security functionalities, baby monitoring systems and alarm systems, connected toys and personal wearable health technology. Important Products with Digital Elements are divided into two classes. These products need to undergo a stricter conformity assessment procedure.
- **Critical Products with Digital Elements:** These products have a cybersecurity-related functionality and perform a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or damage many other Products with Digital Elements through direct manipulation. It includes notably hardware devices with Security Boxes; Smart meter gateways within smart metering systems and other devices for advanced security purposes; Smartcards or similar devices. These products will need to undergo a stricter conformity assessment procedure or will be required to obtain a European cybersecurity certificate.

6. How does the Cyber Resilience Act Interplay With the NIS2 Directive?

The Cyber Resilience Act will complement the NIS2 Directive, which establishes cybersecurity requirements, including supply chain cybersecurity measures and incident reporting obligations for essential and important entities, with the objective to increase the resilience of the services they provide. Thus, the enhanced level of cybersecurity of Products with Digital Elements established by the Cyber Resilience Act could facilitate compliance of the entities that fall within the scope of the NIS2 Directive and could strengthen the cybersecurity of the entire supply chain.

7. What Do Manufacturers Subject to Cyber Resilience Act Need to Do?

Manufacturers notably need to:

- Perform a **comprehensive risk assessment** for their Products with Digital Elements to identify vulnerabilities and potential threats, and implement mitigation measures to address risks;
- Ensure that **Products with Digital Elements are designed, developed, and produced in accordance with the essential cybersecurity requirements** set in the Cyber Resilience Act;
- Update **internal procedures and processes to appropriately report risks and vulnerabilities** of their products and overall **to comply with obligations** set in the Cyber Resilience Act;
- Prepare and keep up to date **documentation demonstrating conformity with their obligations;**
- Provide **training to their product design/development teams** on the Cyber Resilience Act.

8. By When Do Organizations Need to Comply With the Cyber Resilience Act?

Subject to particular provisions, companies that fall within the scope of the Cyber Resilience Act will need to comply with their respective obligations by December 11, 2027. Certain of the obligations enshrined therein will need to be complied with at an earlier date.

9. Who Will Supervise and Monitor Compliance With the Cyber Resilience Act?

Each EU Member State must designate one or more competent authority(ies) responsible for supervising and monitoring compliance with the Cyber Resilience Act. In case of designation of multiple competent authorities in an EU Member State their coordinated position will be represented and their cooperation will be facilitated by a single liaison office.

In certain instances market surveillance authorities will cooperate, among others, with national cybersecurity certification authorities designated pursuant the Cybersecurity Act, Computer Security Incident Response Teams (CSIRTs) designated as coordinators pursuant to the NIS2 Directive, the European Union Agency for Cybersecurity (ENISA) and national data protection authorities.

10. What Are the Risks in Case of Non-compliance?

EU Member States will lay down the rules on penalties applicable to infringements of the Cyber Resilience Act. Non-compliance with the Cyber Resilience Act can lead to fines up to €15,000,000 or 2,5% of the undertaking's total worldwide annual turnover, whichever is higher.