Platis - Anastassiadis
& Associates
the associate law firm of EY Greece

January 2025
Law Alert

Cyber Resilience Act: Horizontal cybersecurity requirements for products with digital elements

The Cyber Resilience Act establishes rules to protect consumers and businesses that purchase or use software or products with digital elements. It introduces cybersecurity requirements for economic operators involved in the production and distribution of these products, extending these requirements throughout the product lifecycle.

On 23 October 2024, Regulation (EU) 2024/2847 of the European Parliament and of the Council, which lays down horizontal cybersecurity requirements for products with digital elements ("Cyber Resilience Act" or "Act"), was published in the Official Journal of the European Union.

The Act establishes uniform cybersecurity requirements for the design, development, production, and distribution of products with digital elements in the EU.

The Act imposes obligations to comply with cybersecurity requirements on manufacturers, importers, distributors, and other persons involved in the manufacture or distribution of products with digital elements within the EU market. The Act was announced in 2020 as part of the EU Cybersecurity Strategy, which aims to protect citizens, businesses, and institutions from cyber threats while promoting international cooperation and a global, open Internet. In this context, the Act complements existing legislation, particularly the NIS2 Directive.

According to the Act, consumers and businesses will now be able to make more informed choices, confident in the cybersecurity credentials of CE-marked products.

1. Scope & subject matter

The Act applies to products with digital elements placed on the market whose purpose or use involves a logical or physical data connection to a device or network.
A product with digital elements is defined in the Act as any software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately. Typical examples of such products are smart home products, individual wearable devices, as well as hardware and software that, although less critical, are considered capable of facilitating the disruption of a device or network.

The material scope of the Act covers manufacturers, distributors, importers, and other economic operators supplying digital products on the EU market.

2. Cybersecurity requirements

The Act provides that products with digital elements shall only be made available on the market if they meet essential cybersecurity requirements and the procedures implemented by their manufacturer comply with these requirements.

Based on a risk assessment by the manufacturer, products must, inter alia, be made available in a secure configuration, protect against unauthorized access, ensure data confidentiality and integrity, protect the availability of essential functions, and minimize negative impacts.

Furthermore, regarding vulnerability handling requirements, manufacturers shall identify and document product vulnerabilities, address them promptly, implement security testing and assessments, and have a policy for vulnerability disclosure and mechanisms for automatic security updates.

Products with digital elements shall only be made available on the market if they comply with the above cybersecurity requirements, as more specifically set out in Annex I, Parts I & II of the Act.

3. Conformity assessment procedure

The Act imposes specific obligations on economic operators for products with digital elements designated as important or critical.

Important products with digital elements are defined in Annex III of the Act and are categorized into Classes I and II, based on their cybersecurity risk level. These products are subject to a more rigorous compliance assessment process due to their higher risk. Class I products follow the conformity assessment procedures outlined in Article 32(2), while Class II products, deemed of higher criticality, are subject to the stricter procedures specified in Article 32(3). For Class II products, this includes assessments by external third parties.

Furthermore, critical products with digital elements are defined as those listed in Annex IV of the Act. These products are subject to more stringent conformity assessment requirements, including the obligation to obtain a European cybersecurity certificate and/or undergo an external third-party assessment.
For products with digital elements that are not classified as important or critical under the Act, a conformity self-assessment procedure applies. This assessment is carried out by the manufacturer under its own responsibility.

4. Obligations of manufacturers

Before placing products with digital elements on the EU market, manufacturers are required to:

- Assess potential risks based on the product's use and lifetime,
- Integrate safe components and exercise due diligence when sourcing them from third parties,
- Implement policies to address and disclose vulnerabilities
- Prepare technical documentation and conduct conformity assessments,
- Issue an EU declaration of conformity and affix the CE marking,
- Include identification and manufacturer information on the product or packaging,
- Provide support for at least five years or for the product's lifetime, and,
- Ensure safety updates remain available for at least ten years or throughout the support period.

In addition, the Act mandates that manufacturers meet the following documentation requirements:

- Technical Documentation: This must include relevant cybersecurity aspects, such as identified vulnerabilities, information provided by third parties, and updates to the product's cybersecurity risk assessment. The technical documentation must be retained for at least 10 years or for the duration of the support period.
- EU Declaration of Conformity: This document demonstrates compliance with the essential requirements of the Regulation and must be kept for at least 10 years or for the duration of the support period.
- Information and User Instructions: These must be provided in an understandable language to enable the safe installation, operation, and use of the product. This information must remain accessible for at least 10 years or for the duration of the support period, either online or in physical form.

Finally, manufacturers are subject to specific reporting obligations and are required to:

- Notify the CSIRT within 24 hours of identifying vulnerabilities in their products,
- Notify the CSIRT within 24 hours of incidents affecting the product's safety,
- Inform users of incidents in a timely manner and provide mitigation measures, and
- Report vulnerabilities in embedded components to the respective maintainers.

5. Obligations of importers, distributors, and other third parties

As regards importers, the Act provides for the obligation to ensure compliance with the essential cybersecurity requirements set out in Annex I of the Act. Importers must check that the manufacturer has carried out a conformity assessment, confirm that technical documentation is available and that the product bears the CE marking, provide the necessary contact details, and include user-friendly instructions and product information.

For the introduction of products with digital elements into the EU market, importers must ensure the availability of technical documentation, CE marking information, instructions for use, contact details of the importer, and the manufacturer's EU declaration of conformity.

If an importer suspects that a product does not comply with the requirements, they must avoid placing it on the market. In cases where a cybersecurity risk is identified, the importer must inform the manufacturer and the market surveillance authorities.

Distributors have similar obligations and must act with due diligence to ensure that products with digital elements bear the CE marking and that manufacturers and importers have fulfilled their compliance obligations. They must also refrain from placing non-compliant products on the market and inform the manufacturer and market surveillance authorities of any cybersecurity risks.

Finally, any natural or legal person who makes a substantial modification to a product with digital elements and places it on the market is considered a manufacturer and is subject to the corresponding obligations.

6. Obligations for software developers

The Act also applies to pluggable software products, imposing obligations on software developers. Software developers must ensure compliance with cybersecurity requirements by implementing up-to-date security measures and best practices to address identified risks. They must provide products with secure default settings and allow users to restore them to a secure state when necessary. Additionally, software developers are required to identify and eliminate vulnerabilities, prevent unauthorized access and report breaches, process only necessary data while ensuring data confidentiality and integrity, ensure that key functions remain active after incidents to mitigate risks such as denial-of-service attacks, and provide secure options for deleting and transferring data between products or systems.

In terms of technical documentation, software developers must maintain a list of software materials and an EU declaration of conformity, which must be accessible to users and include software conformity information. Finally, software developers are required to provide supervisory authorities with the details of any economic operator to whom they have supplied software and retain this information for 10 years.

7. Supervision, fines & enforcement

The Act provides that each Member State shall designate one or more market surveillance authorities to ensure its effective implementation.

In terms of sanctions, penalties ranging from €5,000,000 to €15,000,000, or from 1% to 2.5% of the operator's total worldwide annual turnover, depending on the nature of the breach, are stipulated. It is up to the Member States to define the specific rules on penalties applicable to breaches of the Act's provisions. The Act will enter into force on 11 December 2027. However, the reporting obligations for manufacturers will apply from 11 September 2026, and the provisions on the notification of conformity assessment bodies will apply from 11 June 2026.

The Cyber Resilience Act is available here.

About Platis – Anastassiadis & Associates

Platis - Anastassiadis & Associates is part of the EY Law network operating in 90 countries globally and is comprised of 3,500+ people.

We are an independent law office with a core team of 45 lawyers. Our office provides high quality legal services across the full range of commercial and financial transactions.

Especially in our geographical area, we have established an ongoing cooperation with the respective law firms which are associated with EY, in order to offer seamless and consistent regional services to our clients that have cross country operations.

Our experience allows us to better understand our clients' needs and offer them integrated multidisciplinary solutions in the fields of accounting, tax and financial advisory services. Platis – Anastassiadis & Associates law office is solution focused. We work closely with our clients to seek innovative and practical ways of dealing with their issues. Our priority is to help our clients meet their business objectives. Our expertise, commitment and enthusiasm has resulted in the build up of a client base which includes local and international listed, state and private sector companies and financial institutions.

For more information on digital law issues, please contact:
Eirinikos Platis
Partner
eirinikos.platis@gr.ey.com

Antonios Broumas
Senior Manager
antonios.broumas@gr.ey.com

at the
Platis - Anastassiadis & Associates Law Partnership
Tel.: +30 210 2886 512
legaloffice@gr.ey.com

ey.com

EY EY Greece eygreece @EY_Greece EY Greece

Platis - Anastassiadis & Associates Law Partnership is associated with EY.
Partners: E. Platis, A. Anastassiadis
Partnership is registered with the Athens Bar, registration number 80240
List of our associates upon request.