PAVESIO
STUDIO LEGALE

July 2026

Cyber Resilience Act
Regulatory Updates for products with digital elements

Regulation (EU) 2024/2847 (the **Cyber Resilience Act**) introduces a harmonized European framework on cybersecurity applicable to **products with digital elements**.

The new regulation forms part of the European Union's broader strategy to strengthen the cyber resilience of the internal market. It complements the existing regulatory framework – particularly the NIS 2 Directive, which focuses on security measures for networks and information systems within regulated organizations – with the objective of ensuring a high and consistent level of cybersecurity for products throughout their entire lifecycle.

Scope of Application

The Cyber Resilience Act applies to all **products with digital elements** – namely, any hardware or software product, as well as related remote data-processing solutions – whose intended purpose or reasonably foreseeable use **includes a logical or physical connection** (whether direct or indirect) to a device or network.

Excluded from the scope of the Regulation are products with digital elements that are already governed by equivalent sector-specific legislation, including, by way of example, regulations concerning medical devices and in vitro diagnostic medical devices, motor vehicles subject to automotive type-approval requirements (categories M, N, and O), and aircraft.

Manufacturers' Obligations

As of **11 September 2026**, manufacturers of products with digital elements will be required to:

- notify, through the Single Reporting Platform currently being established, any **actively exploited vulnerabilities**, i.e., vulnerabilities for which there is reliable evidence of exploitation by a third party not authorized by the system owner, as well as any severe incidents affecting the security of the products (Article 14);

- inform **users of the product with digital elements** – whether directly affected or, where appropriate, the wider user community – of the identified vulnerability or incident, providing clear information regarding any **risk mitigation measures and/or corrective actions to be taken**. Such information should also be made available in structured formats suitable for automated processing where appropriate (Article 14).

As of **11 December 2027**, manufacturers of products with digital elements will be subject to a number of specific obligations, including, by way of example, the requirement to:

- ensure that products are **designed, developed, and manufactured in compliance with the applicable essential cybersecurity requirements** set out in the Regulation (Article 13, in conjunction with Annex I, Part I);

Pavesio Studio Legale
info@pavesioassociati.it
www.pavesioassociati.it

Torino
Corso Vittorio Emanuele II, 68
10121 Torino
T. +39 011 51121

Milano
Via Bigli, 2
20121
T. +39 02 303049

- implement **security-by-design and security-by-default principles** and adopt a **structured cybersecurity risk management approach** throughout the entire product lifecycle (Article 13);

- establish and maintain **vulnerability handling processes**, including the timely provision of security updates and patches (Article 13, in conjunction with Article 14 and Annex I, Part II);

- comply with **information obligations** towards users, particularly with regard to cybersecurity risks, secure use instructions, and the availability of security updates (Article 13, in conjunction with Annex II);

- affix the **CE marking** as evidence of conformity with the applicable cybersecurity requirements (Article 30);

- prepare and maintain the **technical documentation demonstrating the conformity** of the product with digital elements, **including a cybersecurity risk assessment** (Article 31, in conjunction with Annex VII);

- carry out, or have carried out, the **applicable conformity assessment procedures** selected for the product (Article 32, in conjunction with Annex VIII).

For products that also qualify as **high-risk AI systems**, the Cyber Resilience Act introduces an important principle of regulatory alignment and integration of requirements. Compliance with the cybersecurity requirements of the Cyber Resilience Act may also serve to demonstrate compliance with the corresponding cybersecurity requirements under the **AI Act**, thereby avoiding unnecessary duplication of obligations. In essence, the cybersecurity requirements set out in the AI Act are deemed to be fulfilled where the product complies with the essential cybersecurity requirements and the related organizational processes established under Annex I of the Cyber Resilience Act.

The Cyber Resilience Act represents a significant paradigm shift, requiring economic operators to **embed cybersecurity as a structural component of digital products**. Cybersecurity is no longer treated merely as a technical requirement but as a strategic market factor and a key element of accountability throughout the entire product lifecycle.

Against this backdrop, organizations should assess whether they place on the market products with digital elements that fall within the scope of the Cyber Resilience Act. Such an assessment is essential to ensure that the necessary measures are implemented in a timely manner to achieve compliance with both the formal and substantive obligations introduced by the Regulation.

Contacts

Turin Corso Vittorio Emanuele II, 68 10121 | T. +39 011 51121
Milan Via Bigli 2, 20121 | T. +39 02 303049

info@pavesioassociati.it – www.pavesioassociati.it

For further information:
AreaCompliance@pavesioassociati.it
AreaLegalTech@pavesioassociati.it

Disclaimer

This document has been prepared in general terms and is intended solely for informational and regulatory update purposes.