



POLICY BRIEF

15 09 2025

21

THE CYBER RESILIENCE ACT

From an original text by **FEDERICA CASAROSA**

Summarized by Arianna Rossi



The Cyber Resilience Act	
BACKGROUND AND FIELD OF APPLICATION	<p>The growing concern at the European level over security risks linked to the increasing interconnectivity of digital devices led to the adoption of the Cyber Resilience Act.¹ This issue was first highlighted in the EU's Cybersecurity Strategy for the Digital Decade, introduced in 2020, and later translated into legislation aimed at preventing and mitigating the impact of malicious attacks that exploit vulnerabilities in online-connected products.</p>
HIGHLIGHTS	<ul style="list-style-type: none"> ○ The Cyber Resilience Act focuses on products with digital elements available in the EU market, defined broadly to include software, hardware, and remote data processing solutions. However, it excludes medical devices, which remain governed by the Medical Device Regulation (see Policy Brief no. 6). ○ Products with digital components must meet both pre-market and post-market cybersecurity requirements, covering design, development, monitoring, and updates. ○ Manufacturers are responsible for ensuring no known vulnerabilities exist and must implement secure default configurations and protective measures such as encryption and access controls. These requirements are detailed in Annex II, which outlines standards for security, data integrity, resilience, and vulnerability management. ○ Before market release, manufacturers must prepare technical documentation assessing cybersecurity risks and describing mitigation strategies. ○ Products undergo conformity assessments based on their risk classification, with high-risk items (such as central systems or health-monitoring wearables) subject to stricter procedures under Article 32. ○ After certification, manufacturers remain responsible for post-market surveillance and must report security incidents to national CSIRTs within 24 hours. ○ If user cooperation is needed to deploy fixes, users must be informed. ○ Authorities may enforce corrective actions, including product withdrawal or recall, to ensure continued compliance.
IMPACT	<p>There are a few aspects that are relevant for BRIEF researchers working on interconnected digital objects. Ensuring a high level of cybersecurity is</p>

¹ 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 and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024.



	<p>closely aligned with the robustness and security requirements outlined in the AI Act (see Policy Brief 11). Annex II of the Cyber Resilience Act provides essential security measures, such as encryption, data minimization, and resilience, that can serve as practical guidance for researchers developing secure digital products.</p> <p>Moreover, with clearly defined conformity assessment procedures, researchers working on high-risk technologies, including wearable health devices, can anticipate regulatory expectations more effectively. Additionally, the post-market surveillance framework offers a valuable opportunity to study real-world product performance and vulnerabilities, supporting ongoing improvements in cybersecurity and product reliability.</p>
--	--