AWAIS LAW | drt INTERNATIONAL LAW FIRM & ALLIANCE

United States | Latin America | Europe | Asia | Middle East

INSIGHT · OPINION · TECHNOLOGY & REGULATORY

The EU Cyber Resilience Act: Can European Cybersecurity Regulations Affect Pakistani Technology Companies?

Ameer Abdaal, Senior Associate · AwaisLaw DRT · November 2026

Cybersecurity is no longer only a matter of national security or information technology. It is increasingly a question of international trade, product liability and regulatory compliance.

As digital products become central to modern commerce, governments are placing legal obligations on manufacturers to build cybersecurity into products from the design and development stage. One of the most significant examples is the European Union's Cyber Resilience Act (CRA), Regulation (EU) 2024/2847.

WHAT THE ACT COVERS

The CRA entered into force on 10 December 2024. It establishes mandatory cybersecurity requirements for products with digital elements made available on the EU market. Depending on the product, this can include hardware, software, connected devices and components. Certain categories are excluded or governed by other EU rules, for example some medical devices, vehicles and purely online services. Whether a particular product falls within the Act therefore depends on its nature and classification.

The Act applies in phases: 11 June 2026, the rules on the notification of conformity assessment bodies apply; 11 September 2026, manufacturers' vulnerability and incident reporting obligations apply; and 11 December 2027, most other obligations apply, including the main product-security and conformity requirements.

THE REPORTING CLOCK

Since 11 September 2026, manufacturers are required to report actively exploited vulnerabilities and severe incidents affecting their products. Reports are made to the European Union Agency for Cybersecurity (ENISA) and the relevant national computer security incident response team (CSIRT), through the Act's single reporting platform.

The reporting follows a staged process. An early warning is issued within 24 hours of becoming aware of the vulnerability or incident. A fuller notification is given within 72 hours. A final report is published within 14 days after a corrective or mitigating measure is available (for an actively exploited vulnerability), or within one month of the 72-hour notification (for a severe incident).

The Act is not limited to businesses established in the EU.

WHY THIS REACHES PAKISTAN

The Act is not limited to businesses established in the EU. A manufacturer based in Pakistan may fall within its scope if it places a product with digital elements on the EU market. The Act also places obligations on importers and other operators in the supply chain, so compliance is relevant across the international supply chain.

Pakistan's information technology and software export sector is expanding, and many Pakistani software houses, hardware manufacturers and technology exporters supply customers in Europe. Where their products fall within the CRA, compliance may become a condition of accessing that market. Companies in this position may need to review their security practices, vulnerability-management processes, incident-response procedures and product documentation. Failure to comply may carry regulatory consequences, including restrictions on market access and financial penalties.

A POLICY IS NOT A PRODUCT-SECURITY REGIME

Pakistan's federal cabinet approved the National Cyber Security Policy in July 2021, recognising the need to strengthen the security of digital infrastructure, promote information security standards and build mechanisms for responding to cyber threats. A national policy, however, is not the same as a statutory product-security and conformity regime like the CRA. To date, Pakistan does not appear to have a comprehensive equivalent. This raises a practical question as to whether Pakistan's current framework adequately prepares its technology industry for increasingly demanding international cybersecurity requirements.

The CRA shows how regulation in a major market can affect businesses far beyond its borders. For Pakistan, the task is not only to strengthen cybersecurity for national protection, but also to keep local technology companies competitive in global markets. Compatible standards, effective vulnerability-disclosure mechanisms and stronger regulatory capacity may all help sustain Pakistan's digital exports. Cybersecurity compliance is increasingly a legal and commercial requirement for taking part in the global digital economy, not just an internal technical matter.

AwaisLaw DRT · International Law Firm & Alliance
United States | Latin America | Europe | Asia | Middle East
awaislaw.com

This opinion piece is published for general information on developments in technology and regulatory law affecting Pakistan. It is not legal advice and should not be relied upon as such. It does not comment on any particular product, company or proceeding. For advice on a specific matter, please contact the firm.