CLIFFORD

CHANCE

THE EU CYBER RESILIENCE ACT IS NOW A REALITY

DECEMBER 2024

THE EU CYBER RESILIENCE ACT IS NOW A REALITY
KEY TAKEAWAYS

The EU Cyber Resilience Act (CRA) was published in the Official Journal of the EU on 20 November 2024, establishing mandatory cybersecurity requirements for products with digital elements (PDEs) within the EU market. The CRA aims to harmonise the cybersecurity framework applicable to connected products across the EU, and to promote a safe and resilient digital ecosystem.

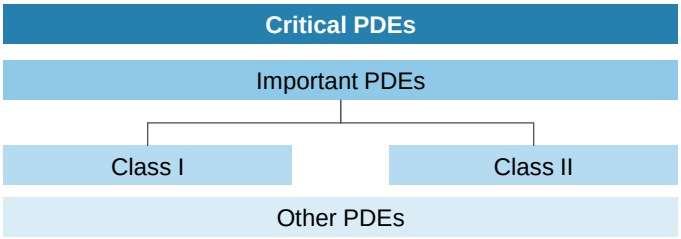
1. Key objectives

- Securing a high level of cybersecurity of PDEs and their integrated remote data processing solutions throughout PDEs lifecycles.
- Ensuring a coherent and harmonised cybersecurity framework for PDEs, including through essential cybersecurity requirements to be complied with.
- Enhancing transparency including as regards the security properties of PDEs.
- Enabling secure use by businesses and consumers, and providing users and businesses with greater legal certainty.

2. Scope

- Governs PDEs (including software, hardware, or components thereof) made available on the EU market.
- Imposes obligations on economic operators along the value chain, including manufacturers, authorised representatives, importers and distributors.
- Also imposes obligations on "open-source software stewards", i.e. legal persons other than manufacturers that systematically provide support for the development of specific PDEs qualifying as free and open-source software and that ensure their viability.
- Examples of PDEs include mobile devices, mobile applications, and smart home devices.
- Certain products are excluded, including medical devices and in vitro diagnostic medical devices, motor vehicles, certain marine equipment as well as PDEs certified under the EU Regulation on civil aviation.
- As regards "remote data processing solutions", only remote data processing (e.g., functions allowing to process / store at a distance) for which the software is designed and developed by or on behalf of the PDE manufacturer and which is basically necessary for the PDE to perform its functions is captured.

3. Risk categorisation



- PDEs are classified according to their criticality and risk level. And the greater the risk level, the stronger the requirements.
- For instance, "Critical PDEs" include PDEs which carry a significant risk of adverse effects in terms of ability to disrupt, control or damage a large number of other PDEs through direct manipulation.
- "Important PDEs" are categorised according to two different classes. They include such things as smart home products with security functionalities (e.g. smart door locks or baby monitoring systems), Internet connected toys with social interactive or location tracking features, and personal wearable products intended for children.

4. Application

- Directly applicable across all EU Member States.
- For matters covered by the CRA, Member States should generally not impose additional cybersecurity requirements for making PDEs available on the market. There are exceptions, however.

5. Enforcement and penalties

- Enforcement involves designated national authorities and an EU-level supervisory structure.
- Measures in the event of non-conformity include product withdrawals / recalls as well as fines up to €15 million or 2.5% of total worldwide annual turnover.

THE EU CYBER RESILIENCE ACT IS NOW A REALITY

KEY TAKEAWAYS (CONTINUED)

6. Key obligations

PDEs must notably meet essential cybersecurity requirements laid down in Annex I to the CRA. There are also requirements that apply specifically to Important PDEs and Critical PDEs respectively, and there are varying obligations for operators across the value chain depending on their role.

Manufacturers:

- Key cybersecurity standards for PDEs
- Conformity assessments
- Risk assessments
- EU declarations of conformity
- Vulnerability handling requirements
- Vulnerability and incident reporting
- Technical documentation / instructions for users

Importers and distributors:

- Due diligence obligations of PDEs' manufacturers to ensure conformity
- Vulnerability reporting

Open-source software stewards:

- Cybersecurity policies
- Cooperation with market surveillance authorities

Looking forward

Businesses should prepare for compliance, including by:

- Identifying products in scope (noting the broad definition of PDEs)
- Integrating CRA requirements into product lifecycles
- Updating internal processes
- Preparing and maintaining required documentation
- Implementing a reporting process for incidents and vulnerabilities

Key dates

- Certain manufacturer reporting obligations applicable from **11 September 2026**
- Fully applicable from **11 December 2027**

Transition periods

- Relevant EU type-examination certificates and cybersecurity approval decisions already in place will remain valid until **11 June 2028** (unless they expire earlier and unless otherwise specified in the relevant EU legislation)
- If new product categories are added or an existing product is reclassified from Class I to Class II, companies can typically expect a **12-month** transition period save urgency

For more information on the Cyber Resilience Act, you can read our more detailed Client Briefing: "The EU Cyber Resilience Act – Towards a safe and secure digital market in Europe". Please click here.

CLIFFORD

CHANCE

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ