BCLP. Client Intelligent

Insights

KEY INSIGHTS ON THE EU CYBER RESILIENCE ACT – WHAT BUSINESSES NEED TO KNOW

DIGITAL SPEAKS SERIES

Nov 25, 2024

SUMMARY

The Cyber Resilience Act (CRA) is a groundbreaking piece of legislation designed to enhance the cybersecurity of digital products and services made available in the EU. Published last week in the Official Journal of the European Union, it marks the start of a phased 3 year implementation period. The CRA aims to strengthen the resilience of the EU's digital economy by imposing stricter requirements on manufacturers, importers, and distributors of products or software with a digital component and will therefore have significant compliance consequences for businesses.

WHO WILL BE AFFECTED?

- manufacturers;
- importers; and
- distributors of products with a 'digital element' whose use requires a direct or indirect logical or physical data connection to a device or network.

The CRA defines a "*product with digital element*" as either software or hardware (or a product combining both). This definition covers numerous goods we all use in our daily life and therefore brings many everyday products (from smart watches to digital assistants to baby monitors) within the CRA's scope.

WHAT IS THE TERRITORIAL SCOPE OF THE CRA?

This regulation applies to those manufacturers, importers and distributors of products and services who are located in the European Union.

Importantly, like many newly enacted EU regulations, it has also an extraterritorial effect: all manufacturers, whether based in the EU or not, will have to comply with the CRA requirements in order to place their products or services on the European market.

WHAT STEPS SHOULD COMPANIES TAKE TO ENSURE COMPLIANCE WITH THIS REGULATION?

Obligations are tiered depending on the role occupied by a company in the product supply chain.

MANUFACTURER OBLIGATIONS

The regulation sets out two sets of requirements for manufacturers of products with a digital component. For those requirements concerning **product properties**, the manufacturer must:

- carry out a product risk assessment, which must be documented and updated to minimize cyber risk at the development stage and during product maintenance;
- comply with the essential cybersecurity requirements set out in Annex of the regulation, and prepare the EU declaration of to certify this;
- provide users with information concerning: (i) product identification (batch or serial number); (ii) manufacturer's contact details; and (iii) the end date of any support period; and
- affix a CE marking and a pictogram or other marking to the product, indicating the cyber , to enable users to make an informed choice.

With regard to **vulnerability management**, the manufacturer must:

- correct vulnerabilities for a period of at least 5 years from the date the product is placed on the market; and
- notify, via a reporting platform specifically established by the European Cybersecurity Agency (ENISA), the competent national and ENISA of any actively exploited vulnerability as soon as it is discovered, first in the form of an alert, then in the form of a . Notification by the manufacturer must be made promptly:
  - an early warning notification must be issued without undue delay and in any event within 24 hours of learning of the vulnerability;
  - a vulnerability notification must then be issued within 72 hours of learning of the vulnerability (providing information about the nature of the incident as well as any corrective or mitigating measures taken or that users can take);

- lastly, the manufacturer must issue a final report listing the corrective actions being taken and information concerning any malicious actor that has exploited or that is exploiting the vulnerability, no later than 14 days after a corrective or mitigating measure is available.

IMPORTER OBLIGATIONS

Importers must verify, before placing the product on the market, that the product complies with essential CRA cybersecurity requirements and that the manufacturer has put in place sufficient vulnerability management processes. It must also: (i) obtain from the manufacturer a set of documents evidencing compliance with the CRA requirements and (ii) include its on the product or on its packaging or in a document accompanying the product.

DISTRIBUTOR OBLIGATIONS

Distributors must check that the product bears the CE mark, and that the manufacturer and importer have complied with their obligations under the CRA.

If there is a risk a product does not conform with the CRA requirements, **importers and distributors** must not place the product on the EU market and must inform, without undue delay, the product manufacturer and the market surveillance competent authorities of the Member States in which they have made the product available.

Importantly, an importer or distributor will also be considered a manufacturer (for the purposes of CRA compliance) when it places a product with digital elements on the market under its name or trade mark or carries out a substantial modification of a product already placed on the market.

WHO ARE THE RELEVANT REGULATORS?

- A Computer Security Incident Response Team (CSIRT) designated by each Member State will coordinate vulnerability disclosures. It will facilitate, where necessary, the interaction between the person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable products or services. It will also receive any notifications of severe incident having an impact on the security of a product with digital elements.
- The European Union Agency for Cybersecurity (ENISA) is the competent authority, at the EU level to receive any notifications of severe incidents having an impact on the security of the product with digital elements.
- Member States will also designate market surveillance authorities to monitor product sales in each Member State. This authority can request the operators to take all appropriate corrective

actions to bring the product into compliance, to withdraw it from the market, or to recall it within a reasonable period.

PENALTIES

Businesses who fail to comply with the CRA risk the imposition of very significant fines:

- Manufacturers can be fined up to 15,000,000 euros or 2.5% of total worldwide annual turnover for the preceding financial year (whichever is higher)
- Importers and distributors can be fined up to 10,000,000 euros or 2% of total worldwide annual turnover for the preceding financial year (whichever is higher)
- Fines of up to 5,000,000 euros or 1% of total worldwide annual turnover for the preceding financial year (whichever is higher) for the provision of inaccurate information to the conformity assessment bodies and/or supervisory authorities.

NEXT STEPS AND ENTRY INTO FORCE

The CRA will enter into force on December 10th, 2024, and will apply 36 months after its entry into force, on **December 11th, 2027**. However, certain provisions will nevertheless apply earlier, including the manufacturer's obligation to report any actively exploited vulnerabilities to the CSIRT and ENISA, which will apply 21 months after the CRA comes into force, on **September 11th, 2026**.

RELATED PRACTICE AREAS

- Data Privacy & Security
- Technology Transactions

MEET THE TEAM

Pierre-Emmanuel Froge

Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21
