BCLP. Client Intelligent

Insights

THE EU CYBER RESILIENCE ACT'S OBLIGATIONS: WHAT DOES IT MEAN FOR OPEN SOURCE SOFTWARE?

Mar 19, 2026

WHAT IS THE CYBER RESILIENCE ACT AND WHEN DOES IT COME INTO FORCE?

The Cyber Resilience Act (**CRA**) is a European regulation which aims to improve cybersecurity and cyber resilience and provides for common cybersecurity standards for products with digital elements.

Adopted by the EU in October 2024, some of its provisions will be applicable from September 2026 before it comes into full force in December 2027.

WHAT DOES THE CRA MEAN FOR OPEN SOFTWARE?

The CRA broadly defines software as *"the part of an electronic information system which consists of computer code"*. As a result, every piece of code that enables orders to be given to a computer will be software under the CRA, extending its rules to numerous digital services.

1. As open source software (**OSS**) falls within this broad definition, the CRA establishes a separate regime for free OSS, defined as "*software the source code of which is openly shared and which is made available under a free and open-source licence which provides for all rights to make it freely accessible, usable, modifiable and redistributable*". Legal requirements for OSS are tiered, with obligations varying by the role a person plays in the development and distribution of OSS.

I. MANUFACTURER'S OBLIGATIONS

1. **OSS manufacturers**

Manufacturers who distribute products with digital elements on the EU market are within scope of the CRA. Manufacturers are those who develop or have developed products that are sold (i.e. they are monetized and generate profit) by reference to the manufacturer's name or brand name By contrast, OSS manufacturers who accept donations and do not generate economic profit from their

software will fall outside the CRA. And those who who contribute source code to free open source software products that are under someone else's control will also be outside the scope of the CRA.

However, entities who provide OSS for 'free' but who: (i) charge a price for technical support services (where this fee goes beyond reimbursement of the actual costs of providing support); (ii) require that a user's personal data is processed (other than for the purposes of improving the security, compatibility or interoperability of the software); or (iii) accept donations beyond the costs associated with the design, development and provision of a product with digital elements will be within scope of the CRA.

Key obligations on in-scope OSS manufacturers include:

1. **Cybersecurity by design obligations**

- Design, development and production of products containing digital elements so as to ensure an appropriate level of cybersecurity by reference to the risks posed
- Protection of the confidentiality, integrity and availability of data processed, stored or transmitted

2. **Documentation and conformity assessment obligations**

- Requirement for a conformity assessment before the software is placed on the market
- Establishment and maintenance of comprehensive technical documentation demonstrating compliance with the CRA
- Drafting of an EU declaration of conformity and CE marking to be affixed to the product

3. **Obligations relating to vulnerability management**

- Identification and documentation of vulnerabilities and components of the software
- Requirement to address and correct vulnerabilities without undue delay, in particular by providing free security updates
- Report any actively exploited vulnerabilities to ENISA (European Union Agency for Cybersecurity) and the relevant CSIRT (Computer Security Incident Response Team)

4. **Information and transparency obligations towards users**

- Provision of information relating to identification of the manufacturer and of the product
- Provision of information regarding the use of the product and the cybersecurity risk it may cause

- Provision of information on the type of technical security support offered by the manufacturer

5. **Obligations in the event of a non-compliant product**

- Requirement to take immediate corrective action to bring the product into compliance with the CRA or withdraw it from the market if necessary
- Co-operation with market surveillance authorities

2. **Manufacturers integrating OSS components into products with digital elements**

When manufacturers integrate OSS into their own products they must comply with the CRA. In particular, they must exercise due diligence when integrating components sourced from third parties so that those components do not compromise the cybersecurity of the product, including when integrating components of free and OSS that have not been made available on the market in the course of a commercial activity.

If the manufacturer identifies a vulnerability in a component (including in a free and OSS component), it should inform the entity manufacturing or maintaining the component, providing details of any modification the manufacturer has applied to fix the vulnerability.

The EU has powers to establish voluntary security attestation programmes allowing developers or users of products with digital elements qualifying as free and OSS to assess the conformity of such products with the CRA's requirements.

- **Sanctions**

These obligations established by the CRA towards manufacturers are accompanied by deterrent sanctions for negligent manufacturers, such as administrative fines of up to EUR 15,000,000 or, if the offender is an undertaking, up to 2.5% of its total worldwide annual turnover.

II. OBLIGATIONS APPLICABLE TO 'OPEN SOURCE STEWARDS'

The CRA also introduces the novel concept of "open-source software steward" given the cybersecurity concerns posed by free and OSS that are published, but not made available on the market. Stewards are entities other than the manufacturer, who support the development of CRA-in scope products with free and OSS, and do so for commercial purposes. Providing 'support' will include hosting and managing collaborative software development platforms, hosting source code or software, administering or managing products with digital elements that meet the criteria for free and OSS and guiding the development of these products. The CRA's definition of open source steward is broad enough to cover the main OS foundations (including Eclipse Foundation, Linux Foundation, Apache Foundation). Stewards are subject to a specific lighter touch regime, which includes three main obligations:

1. **Requirement to document a cybersecurity policy**

- This should promote the development of a secure product as well as a process for the effective handling of vulnerabilities by the developers of that product. IT remains to be seen how effective this will be in practice in the open source ecosystem, given vulnerability patching it is not mandatory for developers (and non-commercialised OSS is not subject to the CRA). However, the OSS community is usually aware of vulnerabilities that need to be fixed and tend to act quickly (compared with closed code software users who may not detect a vulnerability until it is actively exploited). We therefore anticipate that open software developers and their communities will be involved in the monitoring and the reporting of vulnerabilities.

2. Duty to co-operate with market surveillance authorities

3. **Obligations relating to vulnerability management**

- Open source stewards must report any actively exploited vulnerabilities to ENISA and the relevant CSIRT. The requirement to notify serious incidents will only apply to stewards if the incident has an impact on the security of the products and the network provided by the stewards themselves.

- **Sanctions**

While the obligations of the open source stewards to put in place a cybersecurity policy and to co-operate with the surveillance authorities are not sanctioned, the reporting obligations are sanctioned to the same extent and for the same amounts of administrative fines as for manufacturers (*i.e* up to EUR 15,000,000 or up to 2.5% of its total worldwide annual turnover whichever is higher).

CONCLUSION

The CRA recognizes the particular nature of the ever-evolving OS ecosystem, providing a specific and adapted legal framework for it. It imposes important obligations on OSS manufacturers, manufacturers that integrate OS components into their products and to OSS stewards which should be considered at all stages of the product lifecycle, given the sanctions for non-compliance set out in the CRA.

Thanks to its experience in the digital sector, supporting start-ups and established tech companies, the Paris office of BCLP can help you to decipher and comply with your Cyber Resilience Act obligations. If you would like to discuss anything raised in this briefing, please contact Pierre-Emmanuel Frogé or your usual BCLP contact.

MEET THE TEAM

Pierre-Emmanuel Frogé

Counsel, Paris

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