Deep dive into the European Cyber Resilience Act

Scope of the analysis

On 15 September 2022, the European Commission published a proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act - CRA). The Cyber Resilience Act introduces cybersecurity rules to ensure more secure hardware and software products.

The scope of the proposed legislation is far reaching as it covers products with digital elements placed on the market. While existing internal market legislation applies to certain products with digital elements, most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity. In particular, the current EU legal framework does not address the cybersecurity of non-embedded software, even if cybersecurity attacks increasingly target vulnerabilities in these products, causing significant societal and economic costs. Hence, through the Cyber Resilience Act, the Commission aims to establish conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle. Additionally, the Commission proposes conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

This analysis offers a deep dive into the content of the proposal by looking at each chapter. If you have any questions or would like to know if and how your organization is going to be impacted by this new legislation, feel free to get in touch with Managing Partner Jasper Nagtegaal at j.nagtegaal@publyon.com.

Details of the proposal

Chapter I - Definitions

Chapter I indicates the scope and definitions of the proposed Regulation. In particular, the CRA proposes cybersecurity rules to ensure more secure hardware and software products by laying down:

- Rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products;
- Essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity;
- Essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes;
- Rules on market surveillance and enforcement of the above-mentioned rules and requirements.

The scope of the CRA is defined in article 2, stating that it shall apply to products with digital elements whose use includes a direct or indirect logical or physical data connection to a device or network. Importantly, this article also lists the products with digital elements that shall not be covered under the CRA, such as those that have already been certified in accordance with other EU Regulations and those developed exclusively for national security or military purposes. Article 3 provides definitions of a product with digital elements which is defined as ‘any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately’. Products with digital elements shall only be made available on the market if they meet the requirements as set out in sections 1 and 2 of Annex I. Articles 6-9 further define critical products with digital elements, general product safety, high-risk AI systems and machinery products.

The proposed CRA explicitly mentions that Member States shall not impede either the access to the market of products with digital elements which comply with the CRA, or the use of products with digital elements which do not comply with the CRA, but which are used at exhibitions or for testing purposes.

Chapter II - Obligations

Chapter II details the obligations of economic operators, namely manufacturers, authorised representatives, importers, and distributors (articles 10 to 17). The two first articles provide an extensive landscape of the responsibilities of manufacturers when placing a product on the market, as well as their reporting obligations. These articles aim to ensure that products with a digital element have been designed, developed, and produced in accordance with the essential cybersecurity requirements set out in this Regulation.

In addition, reporting obligations, to ENISA and consumers, are mandatory under some circumstances. Authorised representatives have less obligations than manufacturers, as they only need to cooperate with the market surveillance authorities, apart from their mandate. Articles 13 and 14 state that the importers and distributors' obligations ensure that only digital elements that comply with the cybersecurity requirements are placed on the market. This must be done by verifying products, take corrective measures if needed and storing products information for 10 years.

Lastly, articles 15 and 16 detail the conditions under which obligations of manufacturers apply to importers, distributors, or others, while article 17 provides economic operators with information to downscale to market surveillance authorities, for 10 years.

Chapter III - Conformity

Chapter III sets out the conformity of products with digital elements and processes. In particular, article 18 gives an overview of which products with digital elements, put in place by the manufacturer, shall be presumed to be in conformity with the essential requirements set out in Annex I. It also details the powers of the Commission to specify the European cybersecurity certification schemes that can be used to demonstrate conformity with the essential requirements or parts thereof as set out in Annex I. Article 19 lists the cases in which the Commission is empowered, by means of implementing acts, to adopt common specifications in respect of the essential requirements set out in Annex I. Article 20 clarifies how the EU declaration of conformity should be drawn up by manufacturers and what such a declaration should entail. Articles 21-23 define the conditions for CE marking, while article 24 lists conformity assessment procedures, which are set out in Annex VI.

Chapter IV – Notification of conformity assessment bodies

Chapter IV introduces the notification procedures of conformity assessment bodies. Article 25 and 26 state that Member States shall notify the Commission and other Member States of conformity assessment bodies authorised to carry out conformity assessments in accordance with the Regulation, and require Member States to designate a responsible notifying authority for setting up and carrying out procedures. The following articles detail the requirements for notifying authorities and conformity assessment bodies in order to be designated as such, as well as how Member States shall inform the Commission of their procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies. The Commission shall make that information publicly available.

Additionally, attention is paid to small and medium sized enterprises (SMEs). Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, in particular taking into account the interests of SMEs in relation to fees.

Article 30 states that a conformity assessment body shall be presumed to comply with the requirements set out in article 29 insofar as the applicable harmonised standards cover those requirements, if said conformity assessment body demonstrates its conformity with the criteria laid down in the relevant harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union.

The responsibility carried by notified bodies for their subsidiaries and subcontractors is explained in article 31, while articles 32-33 stipulate how a conformity assessment body should submit an application for notification to the notifying authority of the Member State in which it is established, as well as the notification procedure which should be followed by notifying authorities. Article 34 states the Commission will assign an identification number to each notified body and will keep an up-to-date list of the bodies notified under the Regulation.

Articles 35-38 detail how a notifying authority should react to a notified body that no longer meets the requirements laid down in article 29, and how the Commission will ascertain challenges to the competence of notified bodies. They also include the operational obligations of notified bodies, as well as when and how a notified body should inform the notifying authority. Article 39 states that the Commission shall provide for the organization of exchange of experience between the Member States' national authorities responsible for notification policy. How the Commission and Member States will help guide the coordination between the differing notified bodies is described in article 40.

Chapter V – Market surveillance and enforcement

Chapter V indicates that each Member State shall designate one or more, existing or new market surveillance authorities for the purpose of ensuring the effective implementation of the CRA. National market surveillance authorities shall carry out market surveillance in the territory of that Member State, in accordance with Regulation (EU) 2019/1020. The Commission shall facilitate the exchange of experience between market surveillance authorities and shall support the authorities when providing guidance and advice to economic operators. In turn, economic operators are asked to fully cooperate with market surveillance authorities and other competent authorities.

While the scope of the CRA is broad, an exception exists for products with digital elements that are classified as high-risk AI systems under the AI Act. Such systems shall be under the responsibility of the designated market surveillance authorities under the AI Act. Article 41 sets out the establishment of a dedicated administrative cooperation group (ADCO) tasked with the uniform application of the CRA and be composed of representatives of the designated market surveillance authorities.

The procedures for both Member States at national level and the Commission with the help of ENISA at EU level, concerning products with digital elements presenting a significant cybersecurity risk, are laid down in articles 43 and 46 respectively. Additionally, where the Member State can take measures against potentially cybersecurity threats, the Commission receives the competence to launch a consultation or evaluate whether such measures are justified. Where products with digital elements are deemed to present a significant risk, the article 46 requires the manufacturer to take all necessary steps to eliminate the risk. Subsequently, national market surveillance authorities may require a manufacturer to take measure. Should the non-compliance persist, the Member State must take appropriate measures to restrict or prohibit the product from being available on the market or recall the product from the market.

While market surveillance authorities are allowed to cooperate to carry out joint activities, conditional to such agreement not leading to unfair competition between economic operators or negative affecting the agreements under article 48. Finally, article 49 outlines the possibility for market surveillance authorities to conduct simultaneous, coordinated, control actions, referred to as ‘sweeps’, to check compliance with or to detect infringements to the CRA.

Chapter VI – Delegated Acts

Chapter VI, in its articles 50 and 51, provides the technical details on the adoption of delegated acts, to ensure that the regulatory framework can be adapted where needed. The Commission holds this power and shall consult experts designated by Member States, before notifying the Parliament and Council. This power may be revoked at any time by both the Parliament and the Council, but this decision shall not affect any delegated act in force. Furthermore, the Commission should be assisted by a committee, for opinion.

Chapter VII – Confidentiality and penalties

This chapter contains the rules on confidentiality of information and data obtained in carrying out their tasks and activities. Hence, article 52 states that all parties involved in the application of the CRA shall respect the confidentiality of information and data to protect property rights and confidential business information, but also to protect the effective implementation of the CRA (especially for inspections, investigations, or audits), public and national security interests, and criminal or administrative proceedings. To ensure effective enforcement article 53 provides market surveillance authorities the competence to impose or request the imposition of administrative fines. However, the CRA also establishes the maximum levels of administrative fines that should be provided in national laws in case of non-compliance with the Regulation.

Chapter VIII – Final provisions

Chapter VIII includes the final provisions of the Regulation, detailing that the Regulation to Annex I of Regulation 2019/1020 on market surveillance and compliance of products, meaning that that Regulation will apply to products with digital elements insofar as there are no specific provisions with the same objective in the CRA. Moreover, article 55 adds transitional provisions for certificates and products with digital elements issued or placed on the market before the date of application of the CRA. Whereas article 56 imposes an obligation on the Commission to review the CRA 3 years after entry into force. Finally, to allow manufacturers, notified bodies and Member States time to adapt to the new requirements, article 57 states that the Regulation will become applicable twenty-four months after its entry into force, except for the reporting obligation on manufacturers which shall apply from 12 months after its entry into force.