EUROPEAN
RENTAL
ASSOCIATION

March 17, 2023

The Cyber Resilience Act

What is the Cyber Resilience Act?

On September 15, 2022, the European Commission presented a proposal for a European Cyber Resilience Act (CRA). This proposal for a regulation aims to ensure stronger cybersecurity for products with digital elements. It lays down a set of essential cybersecurity requirements that every connected device and almost every piece of software distributed in Europe must comply with to face today's diverse and sophisticated cyber-attacks.

The aim of the proposal is to introduce a harmonized and horizontal regulatory framework to empower consumers, stimulate the internal market, and bring legal certainty to consumers and producers.

The CRA will complement the existing EU legislative framework, which includes the 2016 Directive on the security of Network and Information Systems (NIS Directive) and the 2019 Cybersecurity Act, as well as the Directive on measures for a high common level of cybersecurity across the Union (NIS 2), which entered into force last January.

Main objectives

The CRA aims to establish common standards for cybersecurity, applicable to "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately."

In general, the two main objectives of the regulation include:

- Creating 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 ensuring that manufacturers take security seriously throughout a product's life cycle;
- Creating conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

Additionally, the four specific objectives that were set out in the CRA include:

- Ensuring that manufacturers improve the security of products with digital elements from the design and development phase onwards and throughout the whole life cycle;
- Ensuring a single and coherent cybersecurity framework, facilitating compliance for hardware and software producers;

- Increasing the transparency of cybersecurity practices and properties of products and their manufacturers;
- Enabling businesses and consumers to use products with digital elements securely.

Position of equipment manufacturers

In its position paper on the proposal for the CRA, CECE stated to be committed to cybersecurity and welcomes the proposal. However, it has several concerns regarding the scope and timeline of the regulation. The main concerns include the following:

- The definition of in-scope products is too broad and leaves too much room for interpretation. CECE believes the CRA should only apply to connected digital products that communicate data directly or indirectly via a publicly available electronic communications service.
- The implementation timeframe is too short. Considering the practical timeframe needed for the development and assessment of the provisions of the CRA, the time necessary for manufacturers to implement these provisions, and the time required to set up sufficient accredited notified bodies for cybersecurity, CECE asks for a longer transition period of five years instead of two years after the entry into force.

Although CECE generally favors the CRA, it stressed that the construction equipment sector and its manufacturers are already committed to ensuring the highest possible level of cybersecurity.

Impact on rental companies

In the CRA proposal, rental companies would fall under the category of distributors. The regulation aims to ensure that all stakeholders, including distributors of digital products, are held accountable for cybersecurity risks. It, therefore, creates the following obligation for distributors:

- When making a digital product available, distributors must verify that it meets the essential requirements, including CE marking, and inform the manufacturer of any identified vulnerabilities;
- If a product poses a significant cybersecurity risk, the distributor must immediately inform the manufacturer and relevant national authorities and cooperate with them to eliminate the risk;
- Distributors must provide all necessary information and documentation to demonstrate conformity with regulations and inform users if the manufacturer is unable to comply.

Tentative timeline

The Swedish Presidency of the European Union Council appears to prioritize the act as digitalization has proved to be essential, for example, during the COVID-19 pandemic. The legislative negotiations are not

EUROPEAN RENTAL ASSOCIATION

expected to conclude earlier than by end of 2023. The regulation is foreseen to enter into force 24 months after its publication.

Useful links

- Cyber Resilience Act | Shaping Europe's digital future (Europa.eu)
- Commission proposal for the European Cyber Resilience Act (text)
- European Cyber Resilience Act (CRA) (European-cyber-resilience-act.com)
- An Overview of the EU's Cyber Resilience Act – Center for Data Innovation
- CECE comments on the Cyber Resilience Act proposal