The Cyber Resilience Act of the EU

Sara Nesler, Mag. iur. (I), LL.M., Hanover

March 2023

Cyberattacks and cybercrime are continuously on the rise, fuelled by the generally low level of cybersecurity and insufficient understanding and access to information on the part of users. For example, Statista estimates the amount of damage caused by cybercrime in Germany in 2022 at 202.7 billion euros. In response, the EU Commission presented its draft of the "Cyber Resilience Act" (CRA-D) on 15.09.2022. The aim of the new regulations is to increase cyber security in the EU for all manufacturers, importers, and distributors of products with digital elements through horizontally applicable cyber security requirements. The EU Commission's plan is to be welcomed in principle. However, the implementation of the requirements of the CRA-D will be a great challenge for companies due to the high bureaucratic effort and requires early planning.

Addressees

The CRA-D covers market participants along the entire supply chain, i.e. manufacturers as well as importers and traders. The most extensive obligations are imposed on manufacturers. For this reason, the definition of "manufacturer" plays a central role in the application of the new regulation.

A manufacturer within the meaning of the CRA-D is "any natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under his or her name or trademark, whether for payment or free of charge"[1] . This covers not only production in the traditional sense, but also the distribution of so-called *"white label products"* under one's own name or trademark.
Importers, distributors and other persons may also be considered manufacturers and be subject to individual manufacturer obligations if they make substantial changes to a product. Substantial changes are those that extend to the product's compliance with essential cybersecurity requirements or to its intended use. *Refurbishing* and repairs per se shall not normally be considered as substantial changes.

Products with digital elements

The CRA-D applies to all digital content products whose intended or foreseeable use involves a logical or physical data connection to a device or network. This includes both hardware components and software products. Already today, more and more everyday objects have a digital function. Thus, not only

[1] The author's own translation from the original English text.

smartphones or internet routers are products with digital elements, but increasingly also cars, vacuum cleaners, and refrigerators. This trend will increase significantly with the further development of the Internet of Things.
It should be noted that the CRA-D is not limited to consumer contracts. Through the broad definition, the EU Commission wants to cover as many products with digital elements as possible. This is the only way to achieve the goal of a horizontal regulation for the cybersecurity of products that is as gap-free as possible. Exceptions apply only to some product categories that are already strictly regulated in the area of cyber security, such as medical devices and vehicle safety systems.

Three risk levels

The EU Commission recognises, similar to artificial intelligence (see *HP Compact "Artificial Intelligence in Europe", September 2021*), that not all products with digital elements are equally problematic. In addition to "normal" products with digital elements, critical class I products and critical class II products (highly critical products) are identified. Critical systems include browsers, password managers, network monitoring systems and remote access systems.
Operating systems for servers, desktops and mobile devices, routers and modems for Internet access as well as crypto processors, for example, are classified as highly critical. The increasing criticality of the products is associated with higher requirements.

Obligations for manufacturers, Artt. 10-12 CRA-D

In the supply chain, manufacturers are the link with the greatest control over the product. Therefore, they are subject to a whole range of intensive organisational obligations.

Compliance with essential cyber security requirements

First, according to Art. 10 (1) CRA-D, manufacturers must ensure that their products with digital elements are designed, developed and produced in such a way that they guarantee an appropriate level of cyber security, measured against the risks associated with them. To this end, products with digital elements are to be supplied without known exploitable vulnerabilities. These general obligations are specified by a non-exhaustive list of further requirements. For example, products must be supplied with security-friendly (*secure by default*) and privacy-friendly (*privacy by default*) default settings. In addition, each manufacturer must check whether compliance with the listed requirements is sufficient to ensure an appropriate level of cyber security in the specific case; if necessary, they must take further measures.

Vulnerability management

According to Art. 10(6) CRA-D, manufacturers must also ensure effective vulnerability management, including through the identification and documentation of vulnerabilities, their remediation, and the prompt distribution of security updates free of charge.

Other duties

In addition, there are documentation obligations, ongoing checks and adaptation obligations, as well as reporting and notification obligations towards competent authorities and users in the event of exploitations of vulnerabilities and other incidents that have become known.
For the review and adaptation obligations, the Commission foresees a period of up to five years after market introduction. Given the Commission's stated goal of comprehensive cybersecurity, this time limit is puzzling. While it is a relief for manufacturers, many products are designed to operate for a much longer period of time. This could create dangerous cybersecurity vulnerabilities.

Conformity assessment, Artt. 18 et seq. CRA-D

Conformity assessments are carried out to test and demonstrate the conformity of products with digital elements with the CRA-D. The results are documented in a declaration of conformity.

To reduce the effort, the CRA-D grants legal presumptions of conformity for certain products in Art. 18. For example, if the product complies with existing European harmonisation standards. The EU Commission is also empowered to issue general specifications for products. If these are met, the requirements of Annex I CRA-D are also deemed to be met.
For the conformity assessment, manufacturers can choose between the different procedures of Annex VI CRA-D, depending on the risk class of the products. While internal control procedures are sufficient for "normal" products, external verification is required for "critical" and "highly critical" products, either as an EU type examination or in the form of full quality assurance.
Based on the results of the assessment, an EU declaration of conformity must be drawn up. If several EU declarations of conformity are required by different laws, a single declaration of conformity is sufficient as long as it fulfils all the requirements of all applicable laws.
In addition, products with digital elements must also bear the CE marking. The general provisions are applicable to this. However, Art. 22 CRA-D contains provisions on the correct affixing of the marking.

Obligations for importers, Art. 13 CRA-D

EU-based importers who import a product with digital elements into the single market are required to verify compliance with essential cybersecurity requirements. This requirement, similar to the EU Supply Chain Act, involves a high additional expenditure (see *HP Compact "The EU approach to supply chains", February 2022*).
If vulnerabilities become known, the importer must inform the manufacturer, and if the cybersecurity risk is significant (from the importer's point of view), also the market surveillance authorities.

Obligations for traders, Art. 14 CRA-D

Compared to manufacturers and importers, distributors have much lighter obligations. They do not have to verify themselves that a product complies with the cybersecurity requirements, but only check that it bears the CE marking and that the user information according to Annex II CRA-D, the declaration of conformity and the contact information of the importer are available.

Public surveillance and powers of intervention

The EU Commission, the European Cyber Security Agency (ENISA) and the market surveillance authorities of the Member States are responsible for monitoring compliance with the CRA-D. The market surveillance authorities will be the main point of contact for companies.
Powers of investigation and intervention exist not only in the case of non-compliance, but also in the case of CRA-D compliant products that nevertheless pose a risk to certain goods and rights (including the health and safety of persons or compliance with obligations under Union law). In both cases, the market surveillance authority can order all necessary measures in each case, including the recall of the products. The authorities are also authorised to carry out so-called *sweeps*, i.e., coordinated cross-border control actions (simulated cyber-attacks), in order to check certain products or product groups. This intensive possibility to intervene in the rights of market participants and users is criticised in part, especially since the prerequisites for such a "control action" are not specifically regulated. It remains to be seen whether the final version of the regulation will contain stricter requirements in this regard.

Fines

In the event of non-compliance with the provisions of the CRA-D, the draft provides for fines of up to 15 million euros or 2.5% of the total annual turnover. As with the GDPR, the concrete amount of the fines will gradually emerge. Due to a lack of empirical values, a high degree of uncertainty is expected, at least at the beginning. In order to prevent this and to promote a certain uniformity between the Member States, the EU Commission could, similar to the GDPR, issue non-binding guidelines on the calculation of fines. It is currently not foreseeable whether and when this will happen.

Outlook

The draft law still has to be approved by the EU Parliament and Council. In case of amendments, the legislative process will be protracted. If the regulation is adopted, the provisions will apply 24 months after entry into force, except for the obligation to report safety incidents according to Art. 11, which will already apply 12 months after entry into force. Due to the high effort required to implement the regulations and the high fines, companies, and especially manufacturers, should start familiarising themselves with the new requirements in good time.

+ + +

The Alliuris Group

The Alliuris Group consists of 20 law firms and 400 business lawyers within Europe, Asia and America.

Contact	Alisha Daley-Stehr Alliuris Communication
Web	www.alliuris.law
Mail	info@alliuris.org
Fon	+49-511-307 56-20
Fax	+49-511-307 56-21

Alliuris in Germany

Firm	Herfurth & Partner Luisentraße 5, D-30159 Hanover
Web	www.herfurth.de
Fon	+ 49 511 30756 0
Fax	+ 49 511 30756 10
Mob	
Contact	Ulrich Herfurth, Partner
Language	German, English, French, Spanish, Portuguese, Russian, Mandarin, Czech, Polish
Mail	info@herfurth.de

IMPRINT

EDITORS: ALLIURIS A.S.B.L. ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS | BRUSSELS

MANAGEMENT: Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-20, Fax +49-511-307 56-21

BRUSSELS · PARIS · LONDON · AMERSFOORT · UTRECHT · KNOKKE · LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HANOVER · ZUG · VIENNA · SALZBURG · MOSCOW MINSK · ATHENS · ISTANBUL · BEIJING · SHANGHAI · GUANGZHOU NEW DELHI · MUMBAY · NEW YORK · MEXICO CITY SAO PAULO · RIO DE JANEIRO · BRASILIA · BUENOS AIRES · LIMA

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt