The European Commission's proposal for the Cyber Resilience Act

20 September 2022
Par: Jan Pohle | Yannick Aaron Zirnstein

The proposed Cyber Resilience Act seeks to establish fundamental requirements for all products with digital elements and thereby ensure greater cybersecurity.


In the following article we summarise the essential contents of the Draft CRA.

Background

In September 2021, the European Commission announced the proposed legislation. The rationale behind the proposal was that the increasingly frequent occurrence of cyber-attacks is causing immense financial damage as well as compromising the security of both companies and citizens based in the European Union.

The Draft CRA sets out certain conditions that apply to products with digital elements and requires such products to meet cybersecurity requirements throughout the product lifecycle. In addition, increased transparency requirements are intended to ensure that user groups take cybersecurity characteristics into account when selecting and using products and therefore be better protected against cyberattacks.

Scope of the Draft CRA

The material scope of the Draft CRA is quite broad and covers all products with digital elements whose intended or foreseeable use is to establish a direct and/or indirect link of any kind to a device and/or network. According to the proposed definition, all software and hardware products and their related data processing operations are covered.

The products in scope are also divided into two categories, with the relevant category being applied based on predicted levels of risk to the cybersecurity of the product in question. Stricter requirements apply to products that are deemed more critical.

The Draft CRA does not explicitly stipulate a territorial scope of application, and the recitals do not provide any information in this regard either. This creates a fair degree of uncertainty as to whether or not companies outside the European Union would be required to comply with its provisions and, if so, which ones. Nevertheless, the Draft CRA appears to indicate that extraterritorial applicability is intended, although this will have to be explicitly stipulated to ensure legal certainty.
In addition, products that are already the subject of other European legislation, such as medical devices, are explicitly excluded from the scope of the Draft CRA. With regard to those products, the European Commission assumes that the requirements of the Draft CRA are already sufficiently included in the specific legislation applicable to them.

Obligations of economic operators

The Draft CRA lays out different obligations for entities depending on their classification as either a manufacturer, importer or distributor.

However, the fundamental objective remains that the relevant products comply with the "essential cybersecurity requirements and obligations", which are primarily set forth in Annex 1 of the Draft CRA. These include, in particular, the development, production and placing on the market of the products concerned in accordance with certain legal and technical parameters, as well as effective vulnerability handling mechanisms. For the most part, the obligations are not only to be complied with on a one-off basis, but regularly over a period of up to five years, starting with the placing on the market of a product.

For the implementation of these requirements, the Draft CRA provides for a transition period of 24 months (and in some parts of just 12 months), which would commence when the finalised Cyber Resilience Act comes into force. This is likely to present significant challenges for many companies. In principle, product development and manufacturing cycles are planned for a significantly longer period of time; the adjustment of these plans would therefore be accompanied by significant operational upheaval and would be likely to cause a considerable additional economic burden as a result.

Conformity of the products with digital elements

Products subject to the Draft CRA are required to meet certain cybersecurity characteristics. However, in line with the harmonisation efforts of European legislation, there may be the possibility of being able to rely on existing European standards for this purpose. If the products meet the characteristics specified in such existing standards, it is presumed that they also meet the characteristics of the Draft CRA, although presumptions of this kind may be disputed at any time. In the absence of such standards, the European Commission may elect to adopt such standards itself.

To demonstrate compliance with their obligations, manufacturers are required to conduct a so-called conformity assessment. Depending on the risk classification of the product in question there are different procedures and methods that may be applied, with products considered to be of particular high risk being subject to stricter requirements. The procedures range from internal control measures to full quality assurance. For each of these procedures, the Draft CRA contains checklists with specifications that must all be met in order to successfully pass.

Competent bodies and regulatory powers

The Draft CRA also provides for extensive participation by public authorities. Accordingly, the European Commission, ENISA (European Union Agency for Cybersecurity) and national authorities are granted comprehensive market monitoring, investigative and regulatory powers. For cross-border matters, the Draft CRA also addresses the different procedures and principles for these authorities to cooperate with each other if disagreements arise in the interpretation and application of the law.

Authorities are also provided with the power to carry out so-called "sweeps", which appear to be particularly striking and drastic. Sweeps are unannounced and coordinated, involving area-wide monitoring and control measures that are intended to provide information as to whether or not the requirements of the Draft CRA are being complied with. It is particularly important to note that sweeps may apparently be carried out simultaneously by several authorities in close coordination, thus enabling the investigation of cross-border matters. It is unclear how the rights and freedoms of citizens who own products that are the subject of a sweep and are actively using them will be protected in the process.

In particular: Risks of administrative fines

The Draft CRA provides for a phased concept of administrative fines for non-compliance with certain legal requirements, which follows the model of recent European legislation and is intended primarily as a deterrent. Administrative fines for violations of the Draft CRA can reach a maximum amount of either EUR15 million or 2.5 % of the total worldwide annual turnover for the preceding financial year - whichever is higher.
In this context, significant legal uncertainties are likely to arise, mainly because the methods for imposing administrative fines will be left to Member States to implement. Although the Draft CRA specifies certain parameters, in particular criteria for the calculation of administrative fines, the proposed regulation raises considerable concerns with regard to the uniform interpretation and application of the rules on administrative fines throughout the EU.

Summary

The Draft CRA is a part of a series of previously enacted European legislation and future proposed legislation that follows on from the European Commission's digitalisation strategy.

Due to the recognised and steadily growing importance of cybersecurity and increasing public attention being given to this topic, the regulatory approach set out in the Draft CRA is certainly to be welcomed. Nevertheless, the Draft CRA in its current version presents considerable challenges to numerous market stakeholders and has the potential to cause uncertainties should it become law in its current version. A large number of provisions are simply too vague or interfere too intensely with the rights of market stakeholders.

It will be exciting to follow further developments as the legislative process progresses. In the meantime, companies are urged to keep a close eye on the draft legislation and to prepare for the implementation of possible measures arising from it.

AUTHORS

Jan Pohle
Partner
Cologne | T: +49 221 277 277 0
jan.pohle@dlapiper.com

Yannick Aaron Zirnstein
Senior Associate
Cologne | T: +49 221 277 277 0
yannickaaron.zirnstein@dlapiper.com