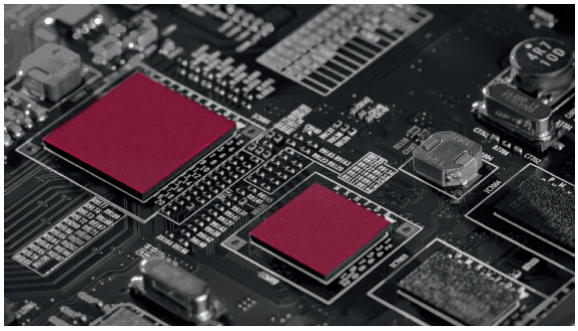
ADVANT Beiten

Tech Law Briefing

April 2024



The Cyber Resilience Act

Dear Reader,

In this issue, we present the most important aspects of the Cyber Resilience Act ("CRA"), which was recently passed by the European Parliament. The CRA introduces extensive security requirements for manufacturers, importers, and distributors of hardware and software products intended for the European market.

Learn more about the coverage of the CRA, essential cybersecurity requirements, conformity assessment and CE marking, point of contact, reporting obligations, monitoring and enforcement, and the timeline.

Please find below our Tech Law Briefing.

Your Contacts:

Dr Andreas Lober

vCard

Daniel Trunk

vCard

Tech Law Briefing:

The Cyber Resilience Act

Almost unnoticed in the shadow of the AI Regulation, the so-called Cyber Resilience Act ("CRA") was passed by the European Parliament on March 12, 2024. This comprehensive Act introduces extensive security requirements for manufacturers, importers, and distributors of hardware and software products intended for the European Union market. The goal of the CRA is to improve cybersecurity and combat widespread vulnerabilities that can have far-reaching consequences due to, among other things, inconsistent provision of security updates and lack of user understanding. In this way, the Act complements the NIS-2 Directive, which focuses primarily on corporate cybersecurity.

I. What does the Cyber Resilience Act cover?

The scope of the CRA is very broad, covering all types of hardware and software, from low to high risk. The CRA initially distinguishes three product categories:

- "Basic" products with digital elements
- Class I and II important products with digital elements, and
- Critical products with digital elements.

The requirements for the products vary depending on the category.

Class I important products include:

- Identity management systems
- Stand-alone and embedded browsers
- Password managers
- Anti-malware
- Network management systems
- Security information and event management systems
- Boot managers

- Public key infrastructures and digital certificates issuance software
- Physical and virtual network interfaces
- Operating systems
- Routers, modems, and switches
- Microprocessors
- Microcontrollers
- Application-specific integrated circuits and field-programmable gate arrays
- Smart home general purpose virtual assistants
- Smart home products with security features
- Internet connected toys
- Wearables for health monitoring

Class II important products include:

- Hypervisors
- Container runtime systems
- Firewalls
- Intrusion detection and/or prevention systems
- Tamper-resistant microprocessors and microcontrollers

The annex of critical products currently includes hardware devices with security boxes, smart meter gateways in intelligent metering systems, and smartcards or similar devices. Both lists are to be expanded and specified by the EU Commission through delegated acts in the future.

II. Essential Cybersecurity Requirements

In order to make a product with digital elements available in the EU, it must meet some essential requirements. First, the manufacturer must assess and document the cybersecurity risks of the product, taking into account the results during planning, production, and the expected lifetime of the product. Based on this assessment, the products must, in particular

- be free of known exploitable vulnerabilities,
- have secure configurations enabled by default, and
- enable free security updates automatically.

They must

- protect against unauthorised access,
- maintain the confidentiality and integrity of data,
- minimise data processing, and
- ensure core functionality even after disruptions.

Product design must minimise attacks, limit impact, and provide transparent security information. This includes an obligation to identify and document exploitable vulnerabilities, regularly review product security, and take precautionary measures, including a coordinated vulnerability disclosure policy. The support period for products with digital elements, during which security updates must be provided and technical documentation must be produced, shall generally be at least five years. The end of the support period shall be clearly and conspicuously disclosed at the time of purchase.

Importers and distributors of products are also required to ensure that the products comply with the requirements of the Regulation.

III. Conformity Assessment and CE Marking

For products with digital components, an EU declaration of conformity from the manufacturer is required, ensuring compliance with the requirements set out in the CRA or further regulations. The corresponding CE Marking must be visibly, legibly, and permanently affixed to the product. For software products, the software must be indicated either on the conformity declaration or on the accompanying website.

The intended conformity assessment procedure can be conducted by the manufacturer on their own responsibility for products not classified as important or critical. The involvement of an independent notified body is voluntary for important products of Class I but mandatory for Class II.

VI. Point of Contact

Manufacturers shall designate a single point of contact where users can report vulnerabilities and obtain information. The single point of contact should not only be automated but also enable contact with a human employee.

V. Reporting Obligations

Manufacturers must report security breaches by malicious actors and cybersecurity incidents that pose an increased risk to users or other individuals. The European Union Agency for Cybersecurity (ENISA) will set up a uniform reporting platform for these reports, which must generally be made immediately but can be delayed for a necessary period for security reasons in individual cases. Addressed vulnerabilities will be recorded in a European vulnerability database in agreement with the manufacturer.

VI. Monitoring and Enforcement

Monitoring and enforcement are primarily carried out by market surveillance authorities, which must now be designated in each Member State. These can also demand access to internal data from manufacturers to assess product conformity.

In case of violations, as with other EU legislation, depending on the nature and severity, substantial fines can be imposed. In the case of the Cyber Resilience Act, they can amount to up to 15 million euros or 2.5% of the company's total worldwide annual turnover in the preceding financial year. The specific rules are left to the EU Member States.

VII. Timeline

The CRA must now be formally adopted by the Council of the European Union. This is expected to take place in April 2024. In line with other EU legislation, the CRA will then enter into force on the twentieth day following its publication in the Official Journal of the European Union. The Regulation will be fully applicable 36 months after its entry into force, although some aspects, including the obligation to report security incidents, will apply earlier.

Products with digital elements placed on the market before the full entry into force of the Regulation will not be subject to the requirements, provided they are not significantly modified after that date. However, this does not apply to the obligation to report security incidents.

VIII. Conclusion

The Cyber Resilience Act obliges economic operators to exercise particular care in the context of cybersecurity. On the one hand, this leads to considerable additional efforts, but on the other hand, it provides a certain degree of legal certainty, as the CRA applies throughout the European Union. Thus, products that comply with the requirements of the Regulation can, in principle, be marketed in any other EU Member State without stricter cybersecurity requirements hindering economic activity. Although the requirements of the Cyber Resilience Act will not be fully applicable for approximately 36 months, they need to be considered early for products with long development cycles and long-term contracts.

From a legal perspective, in addition to compliance with mandatory disclosures, new aspects will play a critical role in the negotiation of IT contracts. For example, manufacturers who obtain components for their products from third parties should require assurances that these components are compliant with the CRA.

EDITOR IN CHARGE:
Dr Andreas Lober | Rechtsanwalt
©Beiten Burkhardt
Rechtsanwaltsgesellschaft mbH

Update Preferences | Forward

Please note

This publication cannot replace consultation with a trained legal professional. If you no longer wish to receive information, you can unsubscribe at any time.

Imprint

This publication is issued by Beiten Burkhardt Rechtsanwaltsgesellschaft mbH
Ganghoferstrasse 33, 80339 Munich, Germany
Registered under HR B 155350 at the Regional Court Munich / VAT Reg. No.: DE811218811
For more information see:
www.advant-beiten.com/en/imprint

Beiten Burkhardt Rechtsanwaltsgesellschaft mbH is a member of ADVANT, an association of independent law firms. Each Member Firm is a separate and legally distinct entity, and is liable only for its own acts or omissions.