Cyber Resilience Act

Affected parties and necessary measures to implement the new EU regulation on the cybersecurity of products with digital elements.

The Cyber Resilience Act (CRA) significantly tightens the cyber security requirements for numerous products. The aim of the CRA is to create a uniform security standard for digital products on the European market. The regulation is to directly apply in all EU member states from 2027.

Who is affected?

Manufacturers, importers and distributors of products with digital elements are affected. Products with digital elements are software or hardware products and their backend systems. These include, among others: Networked machines, IoT devices, apps, wearables, software programs, hard drives, firewalls, password managers, microprocessors and much more. Only a few product types are exempt from the CRA.

What needs to be implemented?

The CRA obliges manufacturers of products with digital elements to fulfil certain cyber security and vulnerability management requirements. Manufacturers must design and develop products with digital elements in such a way that an appropriate level of cyber security is guaranteed throughout the entire product life cycle.

Numerous measures must be taken on the basis of a cyber security risk assessment. Among other things, the products covered may only be placed on the market with a secure standard configuration and without known exploitable vulnerabilities. In addition, the CRA requires numerous technical and organisational measures for product resilience.

Manufacturers of products with digital elements must also fulfil far-reaching requirements for the handling of vulnerabilities. Based on continuous monitoring of the products, manufacturers must eliminate known vulnerabilities through free security updates. Actively exploited vulnerabilities must be reported to the market surveillance authority.

What are the consequences of violations?

The market surveillance authorities have extensive powers to investigate, remedy and impose sanctions. Violations of the CRA can result in product warnings and fines of up to 15 million euros or 2.5 per cent of annual global turnover.

Our support

We support your company in implementing the requirements of the Cyber Resilience Act with the following services, among others:

- Examination of the impact
- Requirements catalogue and gap analysis
- Drafting contracts with suppliers and service providers
- Cybersecurity compliance management

Next step: Making contact

We would be happy to explain our detailed approach to you in a personal meeting.

T +49 30 / 2332 895 0
E info@reuschlaw.de