ALERT

SEPTEMBER 2022

European Commission Proposes Legislation Imposing New Cybersecurity Requirements on Digital Products

On September 15, 2022, the European Commission published a proposal for a Cyber Resilience Act, the first EU-wide legislation introducing a single set of cybersecurity rules for hardware and software products placed in the EU market applying throughout their entire life cycle.

The proposed regulation aims to safeguard EU businesses and consumers buying or using digital products against the risks resulting from inadequate cybersecurity features. The regulation will apply to 'products with digital elements' connected to a device or network, and it will complement the existing EU cybersecurity framework (i.e., the NIS 1 Directive, soon to be replaced by the NIS 2 Directive, and the Cybersecurity Act).

In a nutshell, the Cyber Resilience Act:

- **Lays down essential requirements for the design, development, production, delivery, and maintenance of products with digital elements** to protect against cyber threats.
- **Sets out obligations for manufacturers**. Before placing a digital product on the market, manufacturers will have to: document all related cybersecurity risks; report vulnerabilities and incidents; document all related cybersecurity risks; report vulnerabilities and incidents; provide for effective vulnerability handling processes for the expected product life cycle or for a period of five years; provide instructions on the use of such products and issue security updates; and notify any exploited vulnerability in the product to the European Union Agency for Cybersecurity, or ENISA, within 24 hours.
- **Sets out cybersecurity obligations for importers and distributors** with respect to products entering the market.
- **Provides for a process of conformity assessment** designed to demonstrate compliance with cybersecurity requirements. For non-critical products, the regulation requires self-assessment. For critical products (e.g., identity management systems software, browsers, password managers, VPN, network management systems, network traffic monitoring systems, MDM software, network interfaces, firewalls, operating systems for servers, PKI infrastructure, microprocessors, smartcards), the regulation requires a third-party conformity assessment.
- **Establishes rules for surveillance and enforcement**. Each member state will have to appoint a market surveillance authority responsible for the enforcement of the regulation. In the event of non-compliance, the authority can require the operator (i.e., the manufacturer, the authorized representative, the importer, the distributor, or any other natural or legal person subject to the obligations laid down by the regulation) to take corrective action, restrict the circulation of the product, or order its withdrawal. The authority will also be able to impose fines (up to 15 million euros or up to 2.5% of an undertaking's total global turnover).

The proposal will now be examined by the European Parliament and the Council of the EU. If adopted, manufacturers, notified entities, and member states will have two years to adapt to the new requirements (except from the obligation to report vulnerabilities and incidents, which will only apply after one year).


Laurent De Muyter
Brussels


Olivier Haas
Paris


Dr. Jörg Hladjk
Brussels


Jonathon Little
London


Mauricio F. Paez
New York


Alexandre G. Verheyden
Brussels


Dr. Undine von Diemar
Munich

Lucie Fournier, associate, and Benedetta Brambati, intern, both in the Brussels Office, contributed to this Alert.
