Published on *The National Law Review* https://natlawreview.com

Council of the European Union Adopts the Cyber Resilience Act

Article By:

Hunton Andrews Kurth's Privacy and Cybersecurity

On October 10, 2024, the Council of the European Union (the "Council") adopted the EU's new regulation on horizontal cybersecurity requirements for products with digital elements (the "Cyber Resilience Act"). The Cyber Resilience Act regulates cybersecurity issues in the design, development, production, manufacturing, and making available on the market, of hardware and software products that are connected, directly or indirectly, to another device or to a network (such as connected home cameras, fridges, TVs, toys and other IoT products).

The Council's adoption is the final stage of the EU legislative process (following earlier approval by the European Parliament). As a next step, the Cyber Resilience Act will be published in the EU's Official Journal and will enter into force 20 days after such publication (the "Effective Date"). The majority of the provisions will become applicable 36 months after the Effective Date, with some exceptions such as the rules on incident reporting which become applicable 21 months after the Effective Date. As a regulation, the Cybersecurity Resilience Act will apply directly in all EU Member States.

The key obligations of the Cyber Resilience Act include:

- **Essential Requirements**: Manufacturers must ensure that products placed on the EU market meet the essential requirements in Annex I of the Cyber Resilience Act, including that the products must be designed to: be free of known vulnerabilities; have secure settings and access controls; protect data confidentiality, integrity and availability; limit data processing and attack surfaces; mitigate exploitation risks; and provide security logs.
- **Risk Assessment**: Prior to placing products on the EU market, manufacturers must conduct a comprehensive cybersecurity risk assessment of their products. This assessment should identify and reduce risks, prevent and mitigate security incidents, and protect the health and safety of the users of the product throughout the product's lifecycle. This risk assessment must be documented and updated as needed.
- **Documentation**: All products must include clear and understandable technical documentation and user instructions, including information about the product's security features, potential risks and instructions for safe use.
- **Support**: Manufacturers must provide ongoing support and provide security updates for a period of at least five years. The end date of the support period should be clearly

communicated to users. The security updates made available during the support period must remain available for download for at least 10 years.

- **Conformity Assessment***:* Prior to placing products on the EU market, manufacturers must carry out a conformity assessment to demonstrate whether the requirements applicable to a specific product are complied with. Depending on the product's risk level, different methods of conformity assessment may be used.
- **Reporting**: Manufacturers must report any actively exploited vulnerability or severe security incident to the Computer Security Incident Response Team and the EU Agency for Cybersecurity ("ENISA") within 24 hours of becoming aware of the issue. They also need to inform impacted users as soon as possible and suggest actions that users can take to mitigate impact.
- **Supply Chain Security**: Manufacturers must ensure that components and software from third-party suppliers meet the Cyber Resilience Act's cybersecurity requirements. This includes conducting due diligence and ongoing monitoring of third-party suppliers.

Non-compliance with the requirements of the Cyber Resilience Act may result in administrative fines of up to €15 million or 2.5% of a company's global annual turnover for the previous fiscal year, whichever is higher.

Read the: Council's Press Release and the Cyber Resilience Act.

National Law Review, Volume XIV, Number 291