Lawyer Insights

Comprehensive EU Cyber Security Law in the Pipeline

By David Dumont
Published in CPO Magazine | November 30, 2022

On September 15, 2022, the European Commission released its proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements – the "EU Cyber Resilience Act". If adopted by the European Parliament and Council, the EU Cyber Resilience Act will introduce a comprehensive framework of cybersecurity requirements for products with digital elements in the EU.

This initiative from the European Commission is not surprising, as the Commission's president, Ursula von der Leyen, announced EU actions in the cybersecurity space in last year's State of the Union address. EU legislators have been focusing on the EU's digital and cybersecurity strategy for the last couple of years, as cybersecurity incidents become more frequent, have a significant impact on the European economy and form a real threat for the safety of European citizens. Similar to the EU's position in the privacy and data protection space, the EU has the intention to become an international point of reference in the field of cybersecurity legislation. This requires **c**ybersecurity requirements in the EU. Instead, the cybersecurity landscape in the EU is a real patchwork of industry and product specific rules at EU and Member State level.

At an EU level, cybersecurity requirements are scattered over different pieces of legislation, for example, with respect to critical infrastructure, medical devices, aviation, and motor vehicles. The fragmented legal framework in the EU creates compliance challenges for companies and raises cybersecurity risks resulting from, amongst others, gaps in legislation with respect to certain key products with digital elements that are often targeted by cyberattacks.

With the EU Cyber Resilience Act, the EU takes an important step towards a more robust harmonized set of cybersecurity rules. Ensuring a minimum standard of security for all products with digital elements on the EU market through a Regulation that will be directly applicable in all EU Member States is a sensible approach, taking into account that products circulate freely and a vulnerability in one product can be an entry point for a cyberattack that affects the entire digital ecosystem.

Key Requirements

The EU Cyber Resilience Act introduces requirements that are aimed at ensuring that products with digital elements that are made available on the EU market have less security vulnerabilities and that such vulnerabilities are addressed if they arise during the product's lifecycle. Furthermore, the EU Cyber Resilience Act imposes transparent labelling obligations that will enable digital product users to take into account a product's cybersecurity features when selecting and using the concerned product.

If adopted in its current form, the EU Cyber Resilience Act will cover all products with digital elements that are integrated in or connected to an electronic information system and will impose obligations on the various actors involved in bringing or keeping these products with digital elements on the EU market.

Comprehensive EU Cyber Security Law in the Pipeline
By David Dumont
Published in CPO Magazine | November 30, 2022

Although most obligations are addressed to manufacturers, other parties such as importers and distributors will also have new responsibilities if they place a product on the market under their name or trademark, or substantially modify the product.

The Act sets forth mandatory cybersecurity requirements that need to be complied with starting from the product's design phase continuing throughout the product's lifecycle. It will require companies in the digital space to have a security-by-design mindset when developing products and bringing them to the market. Furthermore, compliance with the EU Cyber Resilience Act will not be a one-off exercise as the security related obligations continue to exist throughout the product's lifecycle.

The EU Cyber Resilience Act lays down requirements to:

- Design, develop and produce products in such a way that they ensure an appropriate level of cybersecurity;
- Deliver products without any known exploitable vulnerabilities;
- Protect the confidentiality and integrity of data stored, transmitted or otherwise processed in connection with products with digital elements;
- Minimize data processing to data that is adequate, relevant and necessary in relation to the intended use of the product;
- Ensure that security vulnerabilities can be addressed through product updates and are handled in accordance with the respective requirements of the EU Cyber Resilience Act; and
- Report actively exploited vulnerabilities or any incident having impact on the security of the product to the European Union Agency for Cybersecurity within 24 hours after becoming aware of it and also notify the product users in case of an incident, as well as the corrective measures they can take to mitigate the impact of the incident.

Effective Cybersecurity Framework

In its proposal, the European Commission has embedded a number of obligations to ensure the effectiveness of the EU Cyber Resilience Act. The various actors involved in bringing a digital product to the EU market will be under a duty to notify the relevant market surveillance authorities in case the requirements under the EU Cyber Resilience Act have not or are no longer complied with. This duty establishes a form of internal control between the relevant economic actors and supports the compliance monitoring capabilities of the relevant supervisory authorities.

Furthermore, the EU Cyber Resilience Act will require digital product manufacturers to carry out cybersecurity assessments and be able to demonstrate their products' conformity with the mandatory

cybersecurity requirements set forth in the Act. With respect to the conformity assessments, the European Commission proposes to take a risk-based approach where certain "critical products with digital elements," such as Internet browsers, antivirus software, operating systems, industrial automation and control systems, and microprocessors, are subject to stricter conformity assessment procedures. In addition, the European Commission will have the power to create a category of "highly critical products with digital elements" for which manufacturers may be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme.

In addition, the EU Cyber Resilience Act introduces stringent penalties for companies that fail to comply with their obligations under the Act. These penalties include administrative fines of up to €15 million or, in the case of an undertaking, up to 2.5% of its total worldwide annual turnover for the preceding financial year, whichever is higher. In addition, market surveillance authorities (and, in exceptional cases, the European Commission) may order companies to bring non-compliant products into compliance, withdraw them from the market or recall them from users.

In addition to regulatory enforcement, an organization that fails to comply with the Cyber Resilience Act may face significant reputational damage. The Cyber Resilience Act introduces transparency obligations vis-à-vis users of the products with digital elements and the Act likely will further increase consumers' awareness around the importance of cybersecurity features of the products with digital elements they are using. Indirectly, this may also create a competitive pressure for companies to ensure that their products meet or even exceed the cybersecurity requirements laid down in the EU Cyber Resilience Act.

Impact

If adopted in its current form, the EU Cyber Resilience Act will significantly change the EU market with respect to products with digital elements.

On the users' end, through the CE marketing, consumers and businesses will be able to have more confidence in the cybersecurity state of products that are available on the EU Market. Users will have easy access to information with respect to a product's cybersecurity features and can take this information into account when selecting and using products with digital elements. Users will also be notified and receive vulnerability patches when an incident occurs.

On the other side, manufacturers and others involved in the distribution of products with digital elements on the EU market will be required to take cybersecurity into account during the product design, development and production phase, as well as after their products have been brought to the market. Cybersecurity will become a continuous compliance effort. Although there is a general consensus on the need for strong and consistent cybersecurity requirements to reduce vulnerabilities in products with digital elements, there is a risk that compliance costs related to the stringent conditions that must be met to introduce and keep products with digital elements on the EU market may make it difficult for small and medium-sized companies to compete on the digital market. There is also a risk that this may hinder technological advancement.

> **"The European Commission has proposed a comprehensive framework of #cybersecurity requirements for products with digital elements – the EU #CyberResilience Act, an important step towards a more robust harmonized set of cybersecurity rules. #respectdata"**

Comprehensive EU Cyber Security Law in the Pipeline
By David Dumont
Published in CPO Magazine | November 30, 2022

Next Steps

The EU Cyber Resilience Act now needs to go through the EU legislative process. It will be reviewed and discussed by the European Parliament and Council. If approved in its current wording, organizations will have two years to adapt to the new requirements, with the exception of the rules regarding reporting of vulnerabilities and incidents, which will be effective one year after the Cyber Resilience Act enters into force.

David Dumont *is a partner in the firm's Global Technology, Outsourcing & Privacy group in the firm's Brussels office. David assists large, multinational clients with various aspects of EU privacy and data protection law. He can be reached at +32 (0)2 643 58 18 or ddumont@HuntonAK.com.*

Originally published on November 30 at https://www.cpomagazine.com/cyber-security/comprehensive-eu-cyber-security-law-in-the-pipeline/.