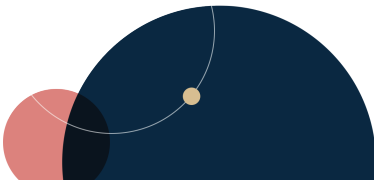
Steptoe

STEPTECHTOE | OCTOBER 28, 2024

Cybersecurity Awareness Month: Navigate the Shifting Sands of EU Cybersecurity Laws

Author
Anne-Gabrielle Haie



Overview

Consistent with tradition, on the occasion of cybersecurity awareness month, we present some key European Union (EU) cybersecurity legislative and regulatory developments that businesses should be aware of in order to devise and implement strong and legally compliant cybersecurity strategies.

Cyber Resilience Act

The Cyber Resilience Act (CRA) was adopted by the Council of the EU on October 10, 2024. The CRA requires that products with digital elements can only be made available on the EU market if they meet specific essential cybersecurity requirements. It applies to both tangible digital products, such as connected devices, and non-tangible digital products, such as software embedded in connected devices. The CRA excludes from its scope certain connected devices that are already covered by sectoral legislation (e.g., medical devices, motor vehicles and their trailers, civil aviation, marine equipment, etc.).

The CRA introduces a series of cybersecurity obligations for manufacturers, importers, and distributors of products with digital elements, as well as for open-source software stewards, based on their roles and responsibilities along the value chain. These obligations include essential requirements for the design, development, and production of such products; detailed rules for placing products with digital elements on the EU market to ensure their cybersecurity; and post-market obligations.

Following its adoption, the CRA will be published in the EU Official Journal, which is expected within the coming weeks. It will enter into force 20 days after this publication and will apply 36 months after its entry into force, although some provisions will apply at an earlier stage.

NIS 2 Directive

EU Member States had until October 17, 2024 to transpose the NIS 2 Directive into their national laws. The NIS 2 Directive is a key component of the EU's cybersecurity strategy and establishes measures for a common high level of cybersecurity for critical infrastructures across the EU. So far, only a handful of EU Member States, such as Belgium, Croatia, and Italy, have transposed it.

The EU NIS 2 Directive applies to entities deemed critical to the European Economic Area (EEA), economy, and society, referred to as "Essential Entities" and "Important Entities." It covers a broad range of sectors, including energy, health, transport, banking, financial markets infrastructure, digital infrastructures and providers, public administration, chemicals, manufacturing, and more. EU Member States have until April 17, 2025, to compile their lists of "Essential Entities" and "Important Entities."

The directive provides detailed risk-management measures, supply chain risk assessment obligations, obligations to report cybersecurity incidents, management liability, and administrative fines for non-compliance. Additionally, the NIS 2 Directive mandates the European Union Agency for Cybersecurity (ENISA) to set up and maintain a database that will include information regarding publicly known vulnerabilities of products and services.

On October 18, 2024, the European Commission adopted the first Implementing Regulation. This regulation further elaborates on the risk-management measures that need to be implemented by DNS service providers, TLD name registries, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, online search engines, social networking services platforms, and trust service providers. It also provides guidance on the criteria to be considered for determining when cybersecurity incidents should be considered significant.

Organizations must monitor the national transposition of the EU NIS 2 Directive as well as the provision of future guidance and recommendations on the application of the directive and establish or update their compliance programs accordingly.

Cybersecurity Act and European Cybersecurity Certification schemes

Based on the Cybersecurity Act, the European Commission adopted, on January 31, 2024, an Implementing Regulation on a European Common Criteria-based cybersecurity certification scheme (EUCC). The EUCC allows ICT suppliers who wish to showcase proof of assurance to go through a commonly understood EU assessment process to certify ICT products, such as technological components (chips, smartcards), hardware, and software. It provides a comprehensive set of rules, technical standards, requirements, and procedures to be applied across the EU with the objective of raising the level of cybersecurity of ICT products, services, and processes in the EU market. The EUCC entered into force on February 27, 2024, and it will enter into application on February 27, 2025.

Further, ENISA is currently working on two cybersecurity certification schemes, the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and the EU Cybersecurity Certification for 5G Networks (EU5G).

Moreover, on April 18, 2023, the European Commission proposed a targeted amendment to the Cybersecurity Act with the aim of enabling the adoption of EU Cybersecurity Certification Schemes for “managed security services,” covering areas such as incident response and security audits. Currently, this amendment awaits approval by the Council of the EU. Additionally, the European Commission has already announced that it will enhance the adoption process of European Cybersecurity Certification Schemes during its next term, within the framework defined in the Cybersecurity Act.

Although adherence to these schemes is voluntary, it allows service providers offering cybersecurity solutions to demonstrate compliance with relevant EU laws. Conversely, organizations subject to certain cybersecurity requirements, such as those within the scope of the EU NIS2 Directive, are mandated to use certified solutions.

Practices

AI, Data & Digital