COMMENTARY

JUNE 2019

IN SHORT

The Situation: The European Union's Cybersecurity Act became effective on June 27, 2019.

The Result: The Act will strengthen the ability of the European Union Agency for Network and Information Security ("ENISA") to help Member States address cybersecurity threats.

Looking Ahead: Businesses initially will be able to certify that their products meet EU cybersecurity standards on a voluntary basis, but the certification eventually may become mandatory.

Boosting the European Union's Cybersecurity and Cyber-Resilience

The Cybersecurity Act (Regulation (EU) 2019/881 of April 17, 2019) was published in the EU Official Journal on June 7, 2019, and entered into force on June 27, 2019. The Cybersecurity Act has two main objectives: (i) strengthening the mandate of the EU cybersecurity watchdog, ENISA to support EU Member States with tackling cybersecurity threats and attacks; and (ii) establishing an EU-wide cybersecurity certification framework ("Framework") in which ENISA will play a key role.

Under the new Framework, ENISA will coordinate the preparation of candidate cybersecurity certification schemes to be submitted to the European Commission for adoption. The Framework will enable the issuance of European cybersecurity certificates and statements of conformity for information and communication technology ("ICT") products, services, and processes to be recognized in all EU Member States.

> EU Member States will develop rules on penalties for infringements of the Framework and for infringements of EU cybersecurity certification schemes.

What Will the Cybersecurity Act Mean for Businesses?

The Cybersecurity Act offers businesses the opportunity to certify that their products meet EU cybersecurity standards. The cybersecurity certification will be voluntary, unless otherwise specified by EU or Member State law. The EU Commission will regularly assess whether a specific scheme is to be made mandatory.

The certification scheme may specify one or more of the following security assurance levels: basic, substantial, or high. For the basic level, it will be possible for ICT manufacturers or service providers to carry out the conformity assessment themselves. For substantial or high levels, the assessment will be done by national cybersecurity certification authorities.

EU Member States will develop rules on penalties for infringements of the Framework and for infringements of EU cybersecurity certification schemes.

How Does the Cybersecurity Act Relate to Other EU Legislation?

The Cybersecurity Act is part of the European Union's overall cyber ecosystem aiming to

increase the safety of the European Union's digital environment. This legislative framework includes the Directive on Security of Network and Information Systems establishing notification and security requirements for operators of essential services and digital service providers such as cloud providers. The proposed ePrivacy Regulation strives to protect the rights to privacy and confidentiality of communications and promote trusted and secure internet of things applications in the digital single market. The General Data Protection Regulation requires controllers and processors across all industry sectors to implement appropriate data security measures.

THREE KEY TAKEAWAYS

1. The Cybersecurity Act lays down the main requirements for European cybersecurity certification schemes to be developed. It will allow European cybersecurity certificates and EU statements of conformity for ICT products, services, or processes to be recognized in all EU Member States.
2. Initially, certification pursuant to the cybersecurity schemes will be voluntary but may gradually become mandatory in the European Union for critical products or activities.
3. Businesses designing, manufacturing, or implementing ICT products, services, or processes should monitor the upcoming discussions for the adoption of cybersecurity certification schemes, assess their level of compliance with respect to such schemes, and/or consider certification once the schemes are available.

Undine von Diemar
Munich

Jörg Hladjk
Brussels

Olivier Haas
Paris

Jonathon Little
London

Lucie Fournier, a legal researcher in the Brussels Office, assisted in the preparation of this Commentary.

YOU MIGHT BE INTERESTED IN: **Go To All Recommendations >>**

Proposed Algorithmic Accountability Act Targets Bias in Artificial Intelligence

French Blocking Statute: A Renewed Interest?

Current Trends: Discovery of Electronically Stored Information on Mobile Devices and Social Media

Data Breach Class Actions in Australia

North Point, 901 Lakeside Avenue, Cleveland, Ohio 44114-1190
www.jonesday.com