# Cybersecurity Act Introduces Cybersecurity Certification and Strengthens EU's Cybersecurity Agency

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

**Thomas Wahl**

**AUTHOR**

**Thomas Wahl**

Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2019, Vol. 14(2) eucrim pp 98 – 99

ISSN: 1862-6947

https://eucrim.eu

On 7 June 2019, the EU added another piece of cybersecurity legislation: the "Cybersecurity Act" (= Regulation (EU) 2019/881); it was published in the Official Journal L 151, p. 15. It introduces a framework for European Cybersecurity Certificates and reinforces the mandate of the EU Agency for Cybersecurity (ENISA). The Regulation had been proposed by the Commission as part of the "cybersecurity package" following the State of the Union Address by Commission President *Jean-Claude Juncker* in 2017 (see eucrim 3/2017, pp. 110-111).

It is clarified that this Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security, and the activities of the State in areas of criminal law.

The EU *Cybersecurity Certification Framework* is an internal market measure that lays down the main horizontal requirements for the development of European cybersecurity certification schemes. The mechanism attests that ICT products, ICT services, and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of, e.g., protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data.

Several advantages are expected from the new certification framework:

- Citizens/end users: increase in trust in digital products, because they can be sure that everyday devices/services are cyber-secure;
- Vendors and providers of products/services (including SMEs and start-ups): first, cost and time savings, because they must undergo the certification process only once, and the certificate is valid throughout the entire EU; second, the label can be used to make products/services more attractive for buyers/users, as they are labelled "cyber secure";
- Governments: better equipped to make informed purchase decisions.

Certification schemes established under the new EU framework are voluntary, i.e., vendors/providers can themselves decide whether they want their products/services to be certified. The Cybersecurity Act foresees, however, that the Commission will assess the mechanism and reflect on whether specific European cybersecurity certification schemes should become mandatory.

The Cybersecurity Act changes ENISA's mandate from a temporary one into a permanent one. ENISA will also receive more staff and money in order to fulfil its tasks. Current tasks, such as supporting policy development and the implementation of cybersecurity acts (e.g., the NIS Directive) and capacity building will be strengthened. New tasks have been added; ENISA will play a key role in implementing the Union's policy on cybersecurity certification. ENISA will also play a greater role in promoting cooperation and coordination on matters related to cybersecurity. Ultimately, it will be an independent centre of expertise on cybersecurity.

## About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union