EU Cybersecurity Agency (ENISA) and information and communication technology cybersecurity certification (Cybersecurity Act)

2017/0225(COD) - 07/06/2019 - Final act

PURPOSE: reform the current European Network and Information Security Agency (ENISA) to provide the EU with an increased cybersecurity capacity and define a framework for the establishment of a European Cybersecurity Certification Scheme.

LEGISLATIVE ACT: Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

CONTENT: with a view to ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation lays down:

- objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity); and

- a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.

European Union Cybersecurity Agency (ENISA)

The Regulation strengthens the current European Union Network and Information Security Agency (ENISA) into a permanent body, the EU Cybersecurity Agency.

ENISA shall carry out its tasks with the aim of achieving a high common level of cybersecurity throughout the Union, including by actively assisting Member States and EU institutions, bodies, offices and agencies to improve cybersecurity. It would serve as a reference point for cybersecurity advice and expertise for EU institutions, bodies, offices and agencies as well as for other relevant EU stakeholders.

ENISA’s tasks shall include:

- assist EU institutions, bodies, offices and agencies, as well as Member States, in the development and implementation of EU policies related to cybersecurity and help them to increase the protection of their networks and information systems, improve cyber-resilience and cyber-reaction capacities, and develop skills and competences in the field of cybersecurity;
- support EU policy on cybersecurity certification, for example by playing a central role in the development of certification systems;
- promote the use of the new certification system, for example by creating a website providing information on certificates;
- promote cooperation, including information sharing and coordination at EU level;

- support Member States' actions to prevent and respond to cyber threats, in particular in the event of cross-border incidents;
- promote a high level of awareness among citizens, organisations and businesses of cybersecurity issues, including computer hygiene and digital skills;
- organise regular EU-wide cyber security exercises, including a large-scale global exercise once every two years;
- produce long-term strategic analyses of cyber threats and incidents to identify emerging trends and help prevent incidents.

The mandate also provides for a network of national liaison officers to facilitate the exchange of information between ENISA and the Member States.

An ENISA Advisory Group composed of recognised experts representing relevant stakeholders, as well as a Stakeholder Group for Cybersecurity Certification shall also be established.

European Cybersecurity Certification Framework

The Regulation creates the first European cybersecurity certification scheme to ensure that products, processes and services sold in EU countries comply with cybersecurity standards.

The Commission shall publish, no later than one year after the entry into force of the Regulation, a rolling work programme of the Union for European Cybersecurity Certification which identifies strategic priorities for future European cybersecurity certification schemes. It shall maintain a dedicated website providing information on European cybersecurity certification schemes, European cybersecurity certificates and EU declarations of conformity.

The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law.

The Commission shall regularly monitor the impact of certification systems and assess their level of use by manufacturers and service providers.

There will be three different levels of insurance, depending on the level of risk associated with the intended use of the product, namely "basic", "substantial" or "high". At the most basic level, manufacturers or service providers shall be able to carry out the conformity assessment themselves.

In order to ensure equivalence of standards across the Union for European cybersecurity certificates and EU declarations of conformity, national cybersecurity certification authorities shall be subject to peer review.

ENTRY INTO FORCE: 27.6.2019. Certain provisions shall apply from 28.6.2021.