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

2017/0225(COD) - 12/03/2019 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 586 votes to 44, with 36 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council on ENISA, the European Union Cybersecurity Agency and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

The position of the European Parliament adopted at first reading under the ordinary legislative procedure has amended the Commission proposal as follows:

Enhanced powers for the EU Cybersecurity Agency (ENISA)

In order to ensure the proper functioning of the internal market while seeking to achieve a high level of cybersecurity, the proposed regulation would set out the objectives, tasks and organisational issues concerning ENISA (the European Union Agency for Cybersecurity).

ENISA would 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. To this end, it should develop its own resources, including its technical capacities and skills.

ENISA should, among other things:

- assist Member States and EU institutions, bodies, offices and agencies in (i) building capacity and preparedness to prevent, detect and respond to cyber threats and incidents; (ii) developing and promoting cyber security policies to support the overall availability or integrity of the public core of the open Internet; and (iii) implementing, on a voluntary basis, policies on vulnerability disclosure;

- promote information sharing and coordination at EU level, between Member States, EU institutions, bodies, offices and agencies and relevant public and private sector stakeholders on cybersecurity issues;

- promote the use of European cybersecurity certification to avoid fragmentation of the internal market;

- support Member States in the field of cybersecurity awareness and education by promoting closer coordination and the exchange of good practices between Member States. Such support could include the development of a network of national education contact points and a cybersecurity training platform;

- raise public awareness of the risks associated with cybersecurity and provide guidance to citizens, organisations and businesses on good practices for individual users, including IT hygiene and digital skills;

- facilitate the technical management of incidents with significant or substantial impact, in particular by supporting the voluntary sharing of technical solutions between Member States or by producing combined technical information, such as technical solutions voluntarily shared by Member States;

- promote the concepts of security from the design stage and privacy from the design stage at EU level;

- contribute, where appropriate, to cooperation with organisations such as the OECD, OSCE and NATO, for example through joint exercises in the field of cybersecurity.

ENISA should keep the European Parliament regularly informed of its activities.

National Liaison Officer Network

The Management Board should establish, on a proposal from the Executive Director, a network of national liaison officers composed of representatives of all Member States (national liaison officers). This network would facilitate the exchange of information between ENISA and the Member States and would help ENISA to publicise its activities and disseminate the results of its work and recommendations to relevant stakeholders across the Union.

European Cybersecurity Certification Framework

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

The Commission should 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 should maintain a dedicated website providing information on European cybersecurity certification schemes, European cybersecurity certificates and EU declarations of conformity.

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