THE EU CYBERSECURITY ACT: AN OVERVIEW

ENISA

The European Union agency for cybersecurity

Read more

CYBERSECURITY CERTIFICATION FRAMEWORK

What it is?

Read more

The purpose of european cybersecurity certification

Increased digitization and connectivity increase cybersecurity risks, thus making society as a whole more vulnerable to cyber threats. To mitigate these risks, all necessary actions must be taken to improve cybersecurity at European Union level. Currently, the cybersecurity certification of ICT products, ICT services and ICT processes is used only to a limited extent. It mostly occurs at Member State level; however, a certificate issued by a national cybersecurity certification is not in principle recognized in other Member States. Companies thus may have to certify their ICT products, ICT services and ICT processes in several Member States where they operate, with a significant increase of their costs. Therefore, it has been necessary to adopt a common approach and to establish a European cybersecurity certification framework that lays down the main horizontal requirements for European cybersecurity certification schemes to be developed and allows European

cybersecurity certificates and EU statements of conformityfor ICT products, ICT services or ICT processes to be recognized and used in all Member States.
The European cybersecurity certification framework should have a two-fold purpose: first, it should help increase trust in ICT products, ICT services and ICT processes that have been certified under European cybersecurity certification schemes and, secondly, it should have the effect to reduce costs for undertakings operating in the digital single market.

ENISA
The European Union agency for cybersecurity

Regulation (EC) no. 460/2004 of the European Parliament and of the Council established the agency with the purposes of ensuring a high and effective level of network and information security within the Union, and developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administrations.

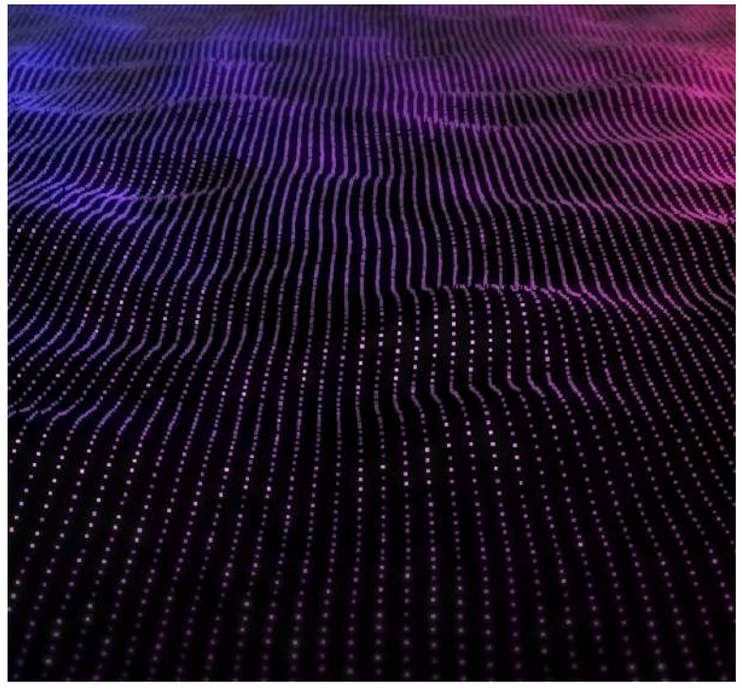
Regulation (EU) 2019/881 increases the role of ENISA by granting it a permanent mandate and allowing it to carry out not only technical consultancy duties but also activities to support the operational management of information incidents by Member States.

ENISA has a leading role in managing the certification system introduced by the Cybersecurity Act. In particular, ENISA shall support and promote the development and mplementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes. In particular, ENISA will be engage with the following activities

a) monitor developments, on an ongoing basis, in related areas of standardization and recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes;

b) prepare European cybersecurity certification schemes; and

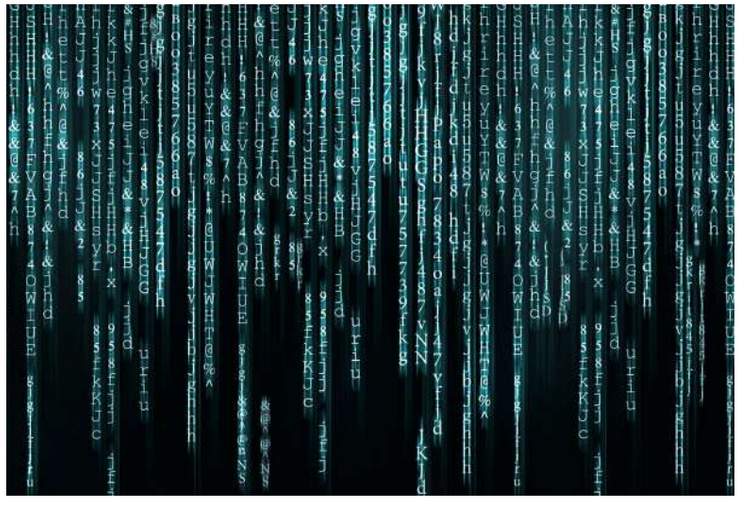
c) evaluate adopted European cybersecurity certification schemes.



CYBERSECURITY CERTIFICATION FRAMEWORK

European cybersecurity certification schemes are intended to harmonize cybersecurity practice within the Union and to contribute to increase the level of cybersecurity within the Union.

European cybersecurity certification schemes should be adopted by ENISA and will need to be formally approved by the European Commission through secondary actuative law. Following the adoption of the European cybersecurity certification schemes, the interested companies could require the certification of ICT products, ICT services and ICT processes. Recourse to the European cybersecurity certification and to EU statements of conformity should remain on a voluntary basis unless otherwise provided by Union law.



European cybersecurity certification schemes could provide for a conformity assessments to be carry out under the sole responsibility of the manufacturer or provider of ICT products, ICT services or ICT processes. In such cases, it should be sufficient that the manufacturer or provider of ICT products, ICT services or ICT processes itself carry out all checks to ensure that the ICT product, ICT services or ICT processes conform with the European cybersecurity certification scheme.

However, Member states should not be prevented from adopting or maintaining national cybersecurity certification schemes for national security purposes.
Member states should inform the Commission and the ECCG of any intention to draw up new national cybersecurity certification schemes.
The Commission and the ECCG should evaluate the impact of the new national cybersecurity certifications schemes on the proper functionally of the international market and ight of any strategic interest in requesting a European cybersecurity scheme instead.

Via Gateano Negri 8
20123 – Milan – Italy
Phone: +39 02 94391800
Fax: +39 02 94391819
E-Mail: segreteria@gvalex.it

GRECO VITALI ASSOCIATI