The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification

On 27 June the European Cybersecurity Act entered into force, setting the new mandate of ENISA, the EU Agency for Cybersecurity, and establishing the European cybersecurity certification framework.

European Commission

EU Cybersecurity Act

With the entry into force of the Cybersecurity Act, a new course is starting for ENISA, the EU Agency for Cybersecurity, which will enjoy a permanent mandate, increased responsibilities and resources. First example of its kind, the European cybersecurity certification framework establishes the governance and rules for EU-wide certification of ICT products, processes and services. Vice-President for the Digital Single Market Andrus Ansip, stated:

> Europe's Digital Single Market can only be a reality if it includes robust cybersecurity commitments. This Commission has pushed forward in making sure Europe has the necessary capabilities, including by proposing a European certification framework and having financing for cybersecurity research and development under the next long-term EU budget. Work on 5G security is a particular priority, as it has the potential to impact every aspect of our future.

Commissioner for Digital Economy and Society Mariya Gabriel, added:

The EU Cybersecurity Act has demonstrated the need for an EU approach to respond to all challenges, protect our citizens and stay competitive. In order to achieve this goal, Europe has granted a permanent mandate to the EU Agency for Cybersecurity. The Cybersecurity Act also enables EU-wide cybersecurity certification. With the Cybersecurity Act, the Directive on the security of networks and information systems and the proposed European Cybersecurity Competence Centre, we have put forward a strong EU pattern, based on our democratic values and safeguarding our citizens' interests.

The new mandate of ENISA

Founded in 2004, Greece-based, the EU Agency for cybersecurity has grown over the years and become a point of reference in the field, by supporting Member States and EU institutions in policy development and implementation, capacity building and EU-wide cooperation. ENISA has now been granted a permanent mandate and a new list of tasks. In particular, ENISA will have a key role in setting up and maintaining the cybersecurity certification framework by, for example, preparing the technical ground for specific certification schemes and informing the public on the certification schemes and the issued certificates through a dedicated website.
ENISA is also mandated to increase operational cooperation at EU level, helping Member States who would request it to handle cyber incidents, and supporting EU coordination in case of large-scale attacks and crises. This task builds on ENISA's role as secretariat of the national Computer Security Incidents Response Teams (CSIRTs) Network, established by the NIS Directive.
In order to fulfil its new mandate, the resources of the agency have been doubled, raising from 11 to 23 million EUR over a period of five years.

The cybersecurity certification framework

The Cybersecurity Act introduces for the first time EU-wide rules for cybersecurity certification. Companies in the EU will benefit from having to certify their products, processes and services only once and see their certificates recognised across the Union.
Under the framework, multiple schemes will be created for different categories of ICT products, processes and services. Each scheme will specify, among the others, the type or categories of ICT products, services and processes covered, the purpose, the security standards that shall be met and the evaluation methods. The schemes will also indicate the period of validity for the certificates issued. ENISA, upon request from the Commission or the European Cybersecurity Certification Group (composed by Member States), will prepare the certification schemes that will then be adopted by the Commission through implementing acts.
Alongside third party certification, conformity self-attestation by the manufacturer is allowed for the products that present low level of risk.
While the certification will remain voluntary, the Commission will assess whether mandatory certification is required for certain categories of products and services.

Next steps

The mandate of ENISA is applicable as of today. As regards the certification framework, the Commission will prepare the first requests for ENISA to develop certification schemes and set-up the governance structure with the establishment of the relevant expert groups:

1. the European Cybersecurity Certification Group, comprised of representatives from Member States that will have to appoint the representatives from their competent authorities;
2. the Stakeholder Cybersecurity Certification Group, which will be responsible to advise ENISA and the Commission.

The Commission will also prepare the "Union rolling work programme for European Cybersecurity Certification", which will identify strategic priorities for certification and in particular include a list of ICT products, services and processes or categories thereof that may benefit from being included in the scope of a European Cybersecurity Certification Scheme. The Union rolling work programme will be subject to a public consultation.

Downloads

The EU Cyber Act at a glance
Download

See also

FAQ

Related topics

Cybersecurity
Strengthening trust and security