

Managed security services

2023/0108(COD) - 18/04/2023 - Legislative proposal

PURPOSE: to create European cybersecurity certification schemes for managed security services.

PROPOSED ACT: Regulation of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: 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 sets up 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.

Managed security services, which are services consisting of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management, have gained increasing importance in the prevention and mitigation of cybersecurity incidents. Accordingly, the providers of those services are considered as essential or important entities belonging to a sector of high criticality pursuant to Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union.

Managed security service providers in areas such as incident response, penetration testing, security audits and consultancy, play a particularly important role in assisting entities in their efforts to prevent, detect, respond to or recover from incidents. They have however also themselves been the target of **cyberattacks** and pose a particular risk because of their close integration in the operations of their customers.

Some Member States have already begun adopting certification schemes for managed security services. There is therefore a growing risk of **fragmentation** of the internal market for managed security services owing to inconsistencies in cybersecurity certification schemes across the Union. This proposal aims to prevent such fragmentation.

CONTENT: the proposed targeted amendment to amend the scope of the European cybersecurity certification framework in the Cybersecurity Act aims to enable, by means of Commission implementing acts, the adoption of **European cybersecurity certification schemes for 'managed security services'**, in addition to information and technology (ICT) products, ICT services and ICT processes, which are already covered under the Cybersecurity Act.

The proposal also introduces a definition of those services, which is very closely aligned to the definition of 'managed security services providers' under the NIS 2 Directive (Article 2 of the Cybersecurity Act). It also adds new provisions on the security objectives of European cybersecurity certification adapted to 'managed security services'.

Lastly, a number of technical amendments are made to ensure that the relevant articles apply also to 'managed security services'.