Managed security services

2023/0108(COD) - 15/01/2025 - Final act

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

LEGISLATIVE ACT: Regulation (EU) 2025/37 of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services.

CONTENT: this regulation is part of the Cybersecurity legislative package which also includes a new regulation on cyber solidarity.

European certification schemes

This **targeted amendment** to the Cybersecurity Regulation aims to strengthen the EU's cyber resilience by allowing for the adoption in the future of European certification schemes for '**managed security services**'.

Managed security services, such as services related to cybersecurity incident management, penetration testing, security audits and consulting, including expert advice, related to technical support, have gained in importance for incident prevention and mitigation.

Managed security service providers have been the target of cyberattacks and, due to their high integration in operators' activities, they represent a particular risk. It is therefore important that essential and important entities exercise enhanced due diligence when selecting their managed security service providers.

The targeted amendment will contribute to **improving the quality of managed security services** and increasing their comparability, facilitate the emergence of reliable cybersecurity service providers and avoid fragmentation of the internal market. It will contribute to achieving the target of **75%** of EU businesses starting to use cloud computing services, big data or artificial intelligence or of more than **90%** of SMEs, including microenterprises, reaching at least a basic level of digital intensity and of essential public services being accessible online.

Role of the European Union Agency for Cybersecurity (ENISA)

ENISA will play an important role in the preparation of candidate European cybersecurity certification schemes. ENISA will:

- promote the use of European cybersecurity certification with a view to avoiding fragmentation of the internal market;

- contribute to the establishment and maintenance of a **European cybersecurity certification framework**;

- promote the development and implementation of Union policy on cybersecurity certification of ICT products and managed security services;

- compile and publish guidelines and develop good practices, concerning the cybersecurity requirements for ICT products, ICT services, ICT processes and managed security services ;

- facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, ICT services, ICT processes and managed security services.

Following a request from the Commission, ENISA will prepare a **candidate scheme** that meets the applicable requirements set out in the Regulation. When preparing a candidate scheme, ENISA will consult in a timely manner all relevant stakeholders through a formal, open, transparent and inclusive consultation process. For each candidate scheme, ENISA will set up an ad hoc working group to provide it with specific advice and expertise.

Information and consultation on the European cybersecurity certification schemes

The Commission will make **publicly available** the information on its request to ENISA to prepare a candidate scheme. During the preparation of a candidate scheme by ENISA, the European Parliament, the Council or both may request the Commission and ENISA to present relevant information on a draft candidate scheme on a quarterly basis.

Security objectives of European cybersecurity certification schemes

A European cybersecurity certification scheme for managed security services will be designed to achieve, as appropriate, at least the following security objectives:

- that the managed security services are provided with the requisite competence, expertise and experience;

- that the provider has established internal procedures to ensure that the managed security services are provided at all times to a sufficient level of quality;

- that data accessed, stored, transmitted or processed in the context of the provision of managed security services are protected against accidental or unauthorised access, storage, disclosure, destruction or other processing, or against loss or alteration or unavailability;

- that the availability of and access to data, services and functions is restored in a timely manner in the event of a physical or technical incident;

- that a record is kept and made available for the assessment of the data, services or functions that have been accessed, used or otherwise processed, at what times and by whom and to ensure that it is possible to evaluate these elements.

The Commission will **regularly evaluate** the effectiveness and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme should be made mandatory, through relevant provisions of Union law.

A **new Annex** contains the requirements to be met by conformity assessment bodies wishing to be accredited.

ENTRY INTO FORCE: 4.2.2025.