Managed security services

2023/0108(COD) - 24/04/2024 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 53 votes to 5, with 33 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) 2019 /881 as regards managed security services.

The European Parliament's position adopted at first reading under the ordinary legislative procedure amends the proposal as follows:

Subject matter

The proposed Regulation aims to enable the adoption of European cybersecurity certification schemes for managed security services. The definition of managed security services under this Regulation includes a non-exhaustive list of managed security services that could qualify for certification schemes, such as incident handling, penetration testing, security audits, and consulting related to technical support.

European certification schemes for managed security services should lead to the uptake of those services and to increased competition between providers offering managed security services. Without prejudice for the objective of ensuring sufficient and appropriate levels of relevant technical knowledge and professional integrity of such providers, certification schemes should, therefore, facilitate market entry and the offering of managed security services, by simplifying, to the extent possible, the potential regulatory, administrative and financial burden that providers, especially microenterprises or small and medium-sized enterprises (SMEs), could encounter when offering managed security services.

Additionally, in order to encourage the uptake of, and stimulate the demand for, managed security services, the schemes should contribute to the accessibility thereof, especially for smaller actors, such as microenterprises and SMEs, as well as local and regional authorities which have limited capacity and resources, but which are more prone to cybersecurity breaches with financial, legal, reputational, and operational implications.

The Union certification scheme for managed security services should contribute to the availability of secure and high-quality services which guarantee a safe digital transition and to the achievement of targets set up in the Digital Decade Policy Programme, especially with regard to the goal that 75% of Union undertakings start using Cloud, AI or Big Data, that more than 90% of microenterprises and SMEs reach at least a basic level of digital intensity and that key public services are offered online.

Preparation, adoption and review of a European cybersecurity certification scheme

Following a request from the Commission, ENISA will prepare a candidate scheme that meets the applicable requirements set out in the Regulation. Following a request from the European Cybersecurity Certification Group (ECCG) may prepare a candidate scheme that meets the applicable requirements. If ENISA rejects such a request, it will have to give reasons for its refusal. Any decision to reject such an application will be taken by the Management Board.

When preparing a candidate scheme, ENISA should consult all relevant stakeholders in a timely manner through a formal, open, transparent and inclusive consultation process. For each candidate scheme, ENISA should set up an ad hoc working group to provide specific advice and expertise. The ad hoc working groups set up for this purpose should include, where appropriate, experts from Member States' public administrations, EU institutions, bodies, offices and agencies and the private sector.

Information and consultation on the European cybersecurity certification schemes

The Commission should make the information on its request to **ENISA** to prepare a candidate scheme. During the preparation of a candidate scheme by ENISA, the European Parliament as well as the Council may request the Commission in its capacity as chair of the European Cybersecurity Certification Group (ECCG) and ENISA to present relevant information on a draft candidate scheme on a quarterly basis. Upon the request of the European Parliament or the Council, ENISA, in agreement with the Commission, may make available to the European Parliament and to the Council relevant parts of a draft candidate scheme in a manner appropriate to the confidentiality level required, and where appropriate in a restricted manner.

In order to enhance the dialogue between the Union institutions and to contribute to a formal, open, transparent and inclusive consultation process, the European Parliament as well as the Council may invite the Commission and ENISA to discuss matters concerning the functioning of European cybersecurity certification schemes for ICT products, ICT services, ICT processes or managed security services.

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

In a **statement**, the Commission recalled that it is recognised that a thorough review of the Cybersecurity Regulation is of the utmost importance, including the evaluation of the procedures leading to the development, adoption and review of European cybersecurity certification schemes.

This review should be based on a deep analysis and broad consultation on the impact, effectiveness and efficiency of the functioning of the European cybersecurity certification framework. The analysis carried out as part of the evaluation established in Article 67 of the Cybersecurity Act should include on-going scheme development activities, such as the one concerning European cybersecurity certification scheme for cloud services (EUCS) as well as those of adopted schemes such as the one concerning the European Common Criteria-based cybersecurity certification scheme (EUCC).

Accordingly, the Commission, which is responsible for the review of the Cybersecurity Act, should ensure that the review takes into account as appropriate the necessary elements mentioned in light of Article 67 when presenting the review to the co-legislators.