Council of the European Union

Brussels, 15 March 2024
(OR. en)

7592/24

Interinstitutional File: 2023/0108(COD)

LIMITE

CYBER 84
JAI 441
TELECOM 115
DATAPROTECT 138
MI 290
IND 146
CODEC 758

NOTE

From:	Presidency
To:	Permanent Representatives Committee
No. prev. doc.:	6610/24
No. Cion doc.:	8511/23
Subject:	Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services - Analysis of the final compromise text with a view to agreement (first reading)

INTRODUCTION

1. On 18 April 2023, the Commission submitted to the Council and the European Parliament a proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services[1], which aims to include European cybersecurity certification schemes for managed security services in the scope of the Cybersecurity Act.

[1] 8511/23.

2. The draft Regulation is based on Article 114 of the Treaty on the Functioning of the European Union (TFEU) (ordinary legislative procedure).

3. The European Social and Economic Committee delivered its opinion on 13 July 2023[2]. The European Data Protection Supervisor delivered an opinion on 10 January 2024[3]. The European Committee of the Regions decided not to deliver an opinion on the proposal.

STATE OF PLAY

4. At its meeting on 15 November 2023, the Permanent Representatives Committee granted the Spanish Presidency a mandate to enter into negotiations with the European Parliament. The first trilogue was held on 4 December 2023.

5. At the second trilogue held on 5 March 2024, a provisional agreement was reached between co-legislators, resulting in the final compromise text as set out in the annex to this note.

6. The provisional agreement also concluded that a statement by the European Commission would be published in the C-Series of the Official Journal and would have a reference and a link to it in the L-Series, together with the legislative act. This statement can be found in an addendum to this note.

[2] 12041/23.
[3] 5322/24.

CONCLUSION

7. The Permanent Representatives Committee is therefore invited to:

– confirm agreement on the final compromise text as set out in the annex to this note with a view to reaching an agreement at first reading with the European Parliament;

– authorise the Chair of the Permanent Representatives Committee to send a letter to inform the Chair of the European Parliament's ITRE Committee that, should the European Parliament adopt its position at first reading on the text of the proposal in the exact form as set out in the annex to this note, and subject to revision of that text by the lawyer-linguists of both institutions, the Council will approve the European Parliament's position and the act will be adopted in the wording which corresponds to the European Parliament's position.

PE-CONS No/YY – 2023/0108 (COD)

REGULATION (EU) 2024/...
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of ...

amending Regulation (EU) 2019/881 as regards managed security services

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[4],

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure[5],

---

4 ***OJ C 349, 29.9.2023, p. 167.***

5 ***Position of the European Parliament of … [(OJ …)/(not yet published in the Official Journal)] and decision of the Council of ….***

Whereas:

(1) Regulation (EU) 2019/881 of the European Parliament and of the Council[6] sets up a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ***information and communications technology (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.

(2) In order to ensure the Union's resilience to cyberattacks and to prevent any vulnerabilities in the Union market, this Regulation is intended to complement the horizontal regulatory framework establishing comprehensive cybersecurity requirements for all products with digital elements in accordance with Regulation (EU) .../... of the European Parliament and of the Council[7] (2022/0272(COD)), by setting up essential requirements for cybersecurity managed services, their application and their trustworthiness.

---

6 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

7 ***Regulation (EU) .../... of the European Parliament and of the Council of ... on ... (OJ L, …, ELI: …).***

(3) Managed security services ***are services provided by managed security service providers as defined in Article 6, point (40), of Directive (EU) 2022/2555 of the European Parliament and of the Council[8]. Therefore, the definition of managed security services in this Regulation should be consistent with the one of managed security service providers in Directive (EU) 2022/2555. These*** services ***consist*** of carrying out, or providing assistance for activities relating to their customers' cybersecurity risk management, ***and*** 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 ▌. Pursuant to Recital 86 of that Directive, 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. Managed security service providers 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. Essential and important entities within the meaning of Directive (EU) 2022/2555 should therefore exercise increased diligence in selecting a managed security service provider.

[8] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

(4) 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. Managed security services could encompass cybersecurity services that support the preparedness, prevention, detection, analysis, mitigation, response to, and recovery from cybersecurity incidents. Cyber threat intelligence provision and risk assessment related to technical support might also qualify as managed security services. There may be separate European cybersecurity certification schemes for different managed security services. The European cybersecurity certificates issued in accordance with such schemes should refer to specific managed security services of a specific provider of these services.

(5) Managed security services providers ***can*** also play an important role in ***relation to*** Union ***actions supporting*** response and immediate recovery ▌ in case of significant and large-scale cybersecurity incidents***, relying on services from trusted private providers and on testing of critical entities for potential vulnerabilities based on EU risk assessments. Certification of managed security services may play a role in the selection of*** trusted providers ▌ .

(6) Certification of managed security services is not only relevant in the selection process for the EU Cybersecurity Reserve but it is also an essential quality indicator for private and public entities that intend to purchase such services. In light of the criticality of the managed security services and the sensitivity of the data they process, certification could provide potential customers with important guidance and assurance about the trustworthiness of these services. European certification schemes for managed security services contribute to avoiding fragmentation of the single market. This Regulation therefore aims at enhancing the functioning of the internal market.

(7) 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.

(8) It is important to provide support to microenterprises and small and medium-sized enterprises (SMEs) in the implementation of this Regulation and in recruiting the specialised cybersecurity skills and expertise necessary to provide managed security services with the requirements laid down in this Regulation. The Digital Europe Programme and other relevant Union programmes provide that the Commission should establish financial and technical support that enable these enterprises to contribute to the growth of the European economy and to strengthening the common level of European cybersecurity in the EU landscape, including by streamlining the financial support from the Digital Europe Programme and other relevant Union programmes and by supporting microenterprises and SMEs.

(9) 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.

(10) In addition to the deployment of ICT products, ICT services or ICT processes, managed security services often provide additional service features that rely on the competences, expertise and experience of their personnel. A very high level of these competences, expertise and experience as well as appropriate internal procedures should be part of the security objectives in order to ensure a very high quality of the managed security services provided. In order to ensure that all aspects of ▌ managed security ***services*** can be covered by ***dedicated*** certification ***schemes***, it is therefore necessary to amend Regulation (EU) 2019/881. The ***results and recommendations of the evaluation and review provided for in*** Regulation (EU) ***2019/881 should be taken into account.***

(11) With a view to facilitating the growth of a reliable Union market, whilst also creating partnerships with likeminded third countries, the certification process established within the framework established by this Regulation should be streamlined to facilitate international recognition and alignment with international standards.

(12) The Union is faced with a talent gap, characterised by a shortage of skilled professionals, and a rapidly evolving threat landscape as acknowledged in the Commission communication of 18 April 2023 on the Cybersecurity Skills Academy. Educational resources and forms of formal training differ and knowledge can be acquired in various ways, both formal, for example through university or courses, and informal, for example through on-the-job training or work experience in the relevant field. Therefore, in order to facilitate the emergence of high-quality, essential managed security services and to have a better overview of the composition of the Union cybersecurity workforce, it is important that cooperation between Member States, the Commission, ENISA and stakeholders, including the private sector and academia, is strengthened through the development of public-private partnerships, support of research and innovation initiatives, the development and mutual recognition of common standards and certification of cybersecurity skills, including through the European Cyber Security Skills Framework. Such cooperation would also facilitate the mobility of cybersecurity professionals within the Union as well as the integration of cybersecurity knowledge and training in educational programmes, while ensuring access to apprenticeships and traineeships for young people, including persons living in disadvantaged regions, such as islands, sparsely populated, rural and remote areas. It is important that those measures aim to attract more women and girls in the field and contribute towards addressing the gender gap in science, technology, engineering, and mathematics, and that the private sector aims to deliver on-the-job training addressing the most in-demand skills, involving public administration and start-ups, as well as microenterprises and SMEs. It is also important that the providers and Member States collaborate and contribute to the collection of data on the situation and the evolution of the cybersecurity labour market.

(13) ENISA plays an important role in the preparation of European certification candidate schemes. The Commission should assess the necessary budgetary resources for ENISA's establishment plan, in accordance with the procedure set out in Article 29 of Regulation (EU) 2019/881 when preparing the draft general budget of the Union.

(14) This Regulation provides for targeted amendments to Regulation (EU) 2019/881 to add the possibility to create cybersecurity certification schemes for managed security service providers. In doing so, it also specifies and clarifies certain provisions concerning the preparation and functioning of all European cybersecurity certification schemes with a view to ensuring their transparency and openness. The latter amendments, which are limited to specification or clarification of Regulation (EU) 2019/881, in particular the amendments to Articles 49 and 49a, should not prejudge in any way the broader evaluation and review of that Regulation required under its Article 67, including specifically the evaluation of the impact, effectiveness and efficiency of that Regulation's Title relating to cybersecurity certification schemes. This evaluation and review regarding the Title relating to cybersecurity certification schemes should be based on a broad consultation of stakeholders and a full and thorough analysis of the procedures involved.

(15) Since the objective of this Regulation, namely to enable the adoption of European cybersecurity certification schemes for managed security services, cannot be sufficiently achieved by the Member States but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(16) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[9] and delivered an opinion on 10 January 2024[10],

HAVE ADOPTED THIS REGULATION:

---

9 ***Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).***

10 ***OJ C.../....***

Article 1

Amendments to Regulation (EU) 2019/881

Regulation (EU) 2019/881 is amended as follows:

(1) in Article 1(1), first subparagraph, point (b) is replaced by the following:

‘(b) 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, ICT processes, and managed security services 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.’;

(2) Article 2 is amended as follows:

(a) points 9, 10 and 11 are replaced by the following:

‘(9) ‘European cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services, ICT processes, or managed security services;

(10) ‘national cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services, ICT processes and managed security services falling under the scope of the specific scheme;

(11) ‘European cybersecurity certificate’ means a document issued by a relevant body, attesting that a given ICT product, ICT service, ICT process or managed security service has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;’;

(b) the following point is inserted:

‘(14a) ‘managed security service’ means a service ***provided to a third party*** consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, ***such as*** incident ***handling,*** penetration testing, security audits and ***consulting, including expert advice, related to technical support;***’;

(c) points 20, 21 and 22 are replaced by the following:

‘(20) ‘technical specifications’ means a document that prescribes the technical requirements to be met by, or conformity assessment procedures relating to, an ICT product, ICT service, ICT process or managed security service;

(21) ‘assurance level’ means a basis for confidence that an ICT product, ICT service, ICT process or managed security service meets the security requirements of a specific European cybersecurity certification scheme, and indicates the level at which an ICT product, ICT service, ICT process or managed security service has been evaluated but as such does not measure the security of the ICT product, ICT service, ICT process or managed security service concerned;

(22) ‘conformity self-assessment’ means an action carried out by a manufacturer or provider of ICT products, ICT services, or ICT processes or managed security services, which evaluates whether those ICT products, ICT services, ICT processes or managed security services meet the requirements of a specific European cybersecurity certification scheme;’;

(3) in Article 4, paragraph 6 is replaced by the following:

‘6. ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation, with a view to increasing the transparency of the cybersecurity of ICT products, ICT services, ICT processes, and managed security services, thereby strengthening trust in the digital internal market and its competitiveness.’;

(4) Article 8 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. ENISA shall support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services, ICT processes and managed security services, as established in Title III of this Regulation, by:

(a) monitoring developments, on an ongoing basis, in related areas of standardisation and recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes pursuant to Article 54(1), point (c), where standards are not available;

(b) preparing candidate European cybersecurity certification schemes ('candidate schemes') for ICT products, ICT services, ICT processes and managed security services in accordance with Article 49;

(c) evaluating adopted European cybersecurity certification schemes in accordance with Article 49(8);

(d) participating in peer reviews pursuant to Article 59(4);

(e) assisting the Commission in providing the secretariat of the ECCG pursuant to Article 62(5).';

(b) paragraph 3 is replaced by the following:

'3. ENISA shall compile and publish guidelines and develop good practices, concerning the cybersecurity requirements for ICT products, ICT services, ICT processes and managed security services, in cooperation with national cybersecurity certification authorities and industry in a formal, structured and transparent way.';

(c) paragraph 5 is replaced by the following:

‘5. ENISA shall 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.’;

(5) in Article 46, paragraphs 1 and 2 are replaced by the following:

‘1. The European cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services, ICT processes and managed security services.’;

2. The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes. It shall attest that the ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle. In addition, it shall attest that managed security services that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity and confidentiality of data, which are accessed, processed, stored or transmitted in relation to the provision of those services, and that those services are provided continuously with the requisite competence, expertise and experience by staff with a ***sufficient and appropriate*** level of relevant technical knowledge and professional integrity.***'***;

(6) in Article 47, paragraphs 2 and 3 are replaced by the following:

‘2. The Union rolling work programme shall in particular include a list of ICT products, ICT services and ICT processes or categories thereof, and managed security services, that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme.

3. Inclusion of specific ICT products, ICT services and ICT processes or categories thereof, or of managed security services, in the Union rolling work programme shall be justified on the basis of one or more of the following grounds:

(a) the availability and the development of national cybersecurity certification schemes covering a specific category of ICT products, ICT services, or ICT processes or managed security services and, in particular, as regards the risk of fragmentation;

(b) relevant Union or Member State law or policy;

(c) market demand;

(ca) technological developments and the availability and development of international cybersecurity certification schemes and international and industrial standards;

(d) developments in the cyber threat landscape;

(e) request for the preparation of a specific candidate scheme by the ECCG.;'

(7) ▌ Article 49 ***is amended as follows***:

(a) paragraphs 1, 2, 3 and 4 are replaced by the following:

'1. Following a request from the Commission pursuant to Article 48, ENISA shall prepare a candidate scheme which meets the applicable requirements set out in Articles 51, 51a, 52 and 54.

2. Following a request from the ECCG pursuant to Article 48(2), ENISA may prepare a candidate scheme which meets the applicable requirements set out in Articles 51, 51a, 52 and 54. If ENISA refuses such a request, it shall give reasons for its refusal. Any decision to refuse such a request shall be taken by the Management Board.';

3. When preparing a candidate scheme, ENISA shall consult all relevant stakeholders in a timely manner by means of a formal, open, transparent and inclusive consultation process. When transmitting the candidate scheme to the Commission, as per Article 49(6), ENISA shall provide information on how it has complied with this obligation.

4. For each candidate scheme, ENISA shall establish an ad hoc working group in accordance with Article 20(4) for the purpose of providing ENISA with specific advice and expertise. The ad-hoc working groups established for this purpose shall, as appropriate and without prejudice to the procedures and discretion established by Article 20(4), include experts from the public administrations of the Member States, the Union institutions, bodies, offices and agencies, and the private sector.';

(b) paragraph 7 is replaced by the following:

'7. The Commission, based on the candidate scheme prepared by ENISA, may adopt implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes and managed security services which meets the requirements set out in Articles 51, ***51a,*** 52 and 54. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).';

(8) The following Article is inserted:

'Article 49a

Information and consultation on the European cybersecurity certification schemes

1. The Commission shall make the information on its request to ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme referred to in Article 48 publicly available.

2. During the preparation of a candidate scheme by ENISA in line with Article 49, 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, and without prejudice to Article 27, 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.

3. 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.

4. The Commission shall take into account, where appropriate, elements arising from the views expressed by the European Parliament and the Council on the matters referred to in paragraph 3 of this Article when evaluating this Regulation in line with Article 67.';

(9) Article 51 is amended as follows:

(a) the title is replaced by the following:

‘Security objectives of European cybersecurity certification schemes for ICT products, ICT services and ICT processes’

(b) the introductory sentence is replaced by the following:

‘A European cybersecurity certification scheme for ICT products, ICT services or ICT processes shall be designed to achieve, as applicable, at least the following security objectives:’

(10) The following Article is inserted:

‘Article 51a
Security objectives of European cybersecurity certification schemes for managed security services

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

(a) ▌ that the managed security services are provided with the requisite competence, expertise and experience, including that the staff in charge of providing these services has a ***sufficient and appropriate*** level of technical knowledge and competence in the specific field, sufficient and appropriate experience, and the highest degree of professional integrity;

(b) ▌ that the provider has appropriate internal procedures in place to ensure that the managed security services are provided at a ***sufficient and appropriate*** level of quality at all times;

(c) ***to*** protect data accessed, stored, transmitted or otherwise processed in relation to the provision of managed security services against accidental or unauthorised access, storage, disclosure, destruction, other processing, or loss or alteration or lack of availability;

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

(e) ▌ that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;

(f) ***to*** record, and enable to assess, which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;

(g) ▌ that the ICT products, ICT services and ICT processes ▌ deployed in the provision of the managed security services are secure by default and by design, ***and where applicable,*** include the latest security updates ***and do not contain publicly known vulnerabilities***;';

(11) Article 52 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services, ICT processes and managed security services: 'basic', 'substantial' or 'high'. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service, ICT process or managed security service, in terms of the probability and impact of an incident.';

(b) paragraph 3 is replaced by the following:

‘3. The security requirements corresponding to each assurance level shall be provided in the relevant European cybersecurity certification scheme, including the corresponding security functionalities and the corresponding rigour and depth of the evaluation that the ICT product, ICT service, ICT process or managed security service is to undergo.’;

(c) paragraphs 5, 6 and 7 are replaced by the following:

‘5. A European cybersecurity certificate or EU statement of conformity that refers to assurance level ‘basic’ shall provide assurance that the ICT products, ICT services, ICT processes and managed security services for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks. The evaluation activities to be undertaken shall include at least a review of technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.

6. A European cybersecurity certificate that refers to assurance level 'substantial' shall provide assurance that the ICT products, ICT services, ICT processes and managed security services for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services, ICT processes or managed security services correctly implement the necessary security functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.

7. A European cybersecurity certificate that refers to assurance level ‘high’ shall provide assurance that the ICT products, ICT services, ICT processes and managed security services for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services, ICT processes or managed security services correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken.’;

(12) in Article 53, paragraphs 1, 2 and 3 are replaced by the following:

‘1. A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services, ICT processes and managed security services that present a low risk corresponding to assurance level ‘basic’.

2. The manufacturer or provider of ICT products, ICT services, ICT processes or managed security services may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By issuing such a statement, the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services shall assume responsibility for the compliance of the ICT product, ICT service, ICT process or managed security service with the requirements set out in that scheme.

3. The manufacturer or provider of ICT products, ICT services, ICT processes or managed security services shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products, ICT services or managed security services with the scheme available to the national cybersecurity certification authority referred to in Article 58 for the period provided for in the corresponding European cybersecurity certification scheme. A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.';

(13) in Article 54, paragraph 1 is amended as follows:

(a) point (a) is replaced by the following:

'(a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services, ICT processes and managed security services covered;';

(aa) point (g) is replaced by the following:

'(g) the specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the applicable security objectives referred to in Articles 51 and 51a are achieved;';

(b) point (j) is replaced by the following:

'(j) rules for monitoring compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements;';

(c) point (l) is replaced by the following:

'(l) rules concerning the consequences for ICT products, ICT services, ICT processes and managed security services that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme;';

(d) point (o) is replaced by the following:

‘(o) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services, ICT processes and managed security services, security requirements, evaluation criteria and methods, and assurance levels;’;

(e) point (q) is replaced by the following:

‘(q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services, ICT ***processes*** or managed security services ▌;**’**;

(14) Article 56 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. ICT products, ICT services, ICT processes and managed security services that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 49 shall be presumed to comply with the requirements of such scheme.’;

(b) paragraph 3 is amended as follows:

(i) the first subparagraph is replaced by the following:

‘The Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law to ensure an adequate level of cybersecurity of ICT products, ICT services, ICT processes and managed security services in the Union and improve the functioning of the internal market. The first such assessment shall be carried out by 31 December 2023, and subsequent assessments shall be carried out at least every two years thereafter. Based on the outcome of those assessments, the Commission shall identify the ICT products, ICT services, ICT processes and managed security services covered by an existing certification scheme which are to be covered by a mandatory certification scheme.’;

(ii) the third subparagraph is amended as follows:

(aa) point (a) is replaced by the following:

‘(a) take into account the impact of the measures on the manufacturers or providers of such ICT products, ICT services, ICT processes or managed security services and on the users in terms of the cost of those measures and the societal or economic benefits stemming from the anticipated enhanced level of security for the targeted ICT products, ICT services, ICT processes or managed security services;’;

(bb) point (d) is replaced by the following:

‘(d) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measure on the manufacturers or providers of ICT products, ICT services, ICT processes or managed security services, including ***the specific interests and needs of microenterprises and*** SMEs***;’***;

(c) paragraphs 7 and 8 are replaced by the following:

‘7. The natural or legal person who submits ICT products, ICT services, ICT processes or managed security services for certification shall make available to the national cybersecurity certification authority referred to in Article 58, where that authority is the body issuing the European cybersecurity certificate, or to the conformity assessment body referred to in Article 60 all information necessary to conduct the certification.

8. The holder of a European cybersecurity certificate shall inform the authority or body referred to in paragraph 7 of any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, ICT service, ICT process or managed security services that may have an impact on its compliance with the requirements related to the certification. That authority or body shall forward that information without undue delay to the national cybersecurity certification authority concerned.’;

(15) in Article 57, paragraphs 1 and 2 are replaced by the following:

‘1. Without prejudice to paragraph 3 of this Article, national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services, ICT processes and managed security services that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7). National cybersecurity certification schemes and the related procedures for the ICT products, ICT services, ICT processes and managed security services that are not covered by a European cybersecurity certification scheme shall continue to exist.

2. Member States shall not introduce new national cybersecurity certification schemes for ICT products, ICT services, ICT processes and managed security services already covered by a European cybersecurity certification scheme that is in force.’;

(16) Article 58 is amended as follows:

(a) paragraph 7 is amended as follows:

(i) points (a) and (b) are replaced by the following:

‘(a) supervise and enforce rules included in European cybersecurity certification schemes pursuant to point (j) of Article 54(1) for the monitoring of the compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with other relevant market surveillance authorities;

(b) monitor compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services, ICT processes or managed security services that are established in their respective territories and that carry out conformity self-assessment, and shall, in particular, monitor compliance with and enforce the obligations of such manufacturers or providers set out in Article 53(2) and (3) and in the corresponding European cybersecurity certification scheme;’;

(ii) point (h) is replaced by the following:

‘(h) cooperate with other national cybersecurity certification authorities or other public authorities, including by sharing information on the possible non-compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of this Regulation or with the requirements of specific European cybersecurity certification schemes; and;’;

(b) paragraph 9 is replaced by the following:

‘9. National cybersecurity certification authorities shall cooperate with each other and with the Commission, in particular, by exchanging information, experience and good practices as regards cybersecurity certification and technical issues concerning the cybersecurity of ICT products, ICT services, ICT ***processes*** and managed security services.**’**;

(17) in Article 59 (3), points (b) and (c) are replaced by the following:

‘(b) the procedures for supervising and enforcing the rules for monitoring the compliance of ICT products, ICT services, ICT processes and managed security services with European cybersecurity certificates pursuant to Article 58(7), point (a);

(c) the procedures for monitoring and enforcing the obligations of manufacturers or providers of ICT products, ICT services, ICT processes or managed security services pursuant to Article 58(7), point (b);’;

(18) in Article 67, paragraphs 2 and 3 are replaced by the following:

2. The evaluation shall also assess the impact, effectiveness and efficiency of the provisions of Title III of this Regulation***, including the procedures leading to the adoption of cybersecurity certification schemes and their evidence bases,*** with regard to the objectives of ensuring an adequate level of cybersecurity of ICT products, ICT services, ICT processes and managed security services in the Union and improving the functioning of the internal market.

3. The evaluation shall assess whether essential cybersecurity requirements for access to the internal market are necessary in order to prevent ICT products, ICT services, ICT processes and managed security services which do not meet basic cybersecurity requirements from entering the Union market.’.

(19) the Annex shall be replaced by the text set out in the Annex to this Regulation.

Article 2

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at ...,

For the European Parliament	*For the Council*
The President	*The President*

ANNEX

REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES

Conformity assessment bodies that wish to be accredited shall meet the following requirements:

1. ***A conformity assessment body shall be established under national law and shall have legal personality.***

2. ***A conformity assessment body shall be a third-party body that is independent of the organisation or the ICT products, ICT services, ICT processes or managed security services that it assesses.***

3. ***A body that belongs to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products, ICT services, ICT processes or managed security services which it assesses may be considered to be a conformity assessment body, provided that its independence and the absence of any conflict of interest are demonstrated.***

4. ***The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product, ICT service, ICT process or managed security service which is assessed, or the authorised representative of any of those parties. That prohibition shall not preclude the use of the ICT products assessed that are necessary for the operations of the conformity assessment body or the use of such ICT products for personal purposes.***

5. ***The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, manufacture or construction, the provision, the marketing, installation, use or maintenance of the ICT products, ICT services, ICT processes or managed security services which are assessed, or represent parties engaged in those activities. The conformity assessment bodies, their top-level management and the persons responsible for carrying out the conformity assessment tasks shall not engage in any activity that may conflict with their independence of judgement or integrity in***

relation to their conformity assessment activities. That prohibition shall apply, in particular, to consultancy services.

6. If a conformity assessment body is owned or operated by a public entity or institution, the independence and absence of any conflict of interest shall be ensured between the national cybersecurity certification authority and the conformity assessment body, and shall be documented.

7. Conformity assessment bodies shall ensure that the activities of their subsidiaries and subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.

8. Conformity assessment bodies and their staff shall carry out conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field, and shall be free from all pressures and inducements which might influence their judgement or the results of their conformity assessment activities, including pressures and inducements of a financial nature, especially as regards persons or groups of persons with an interest in the results of those activities.

9. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. Any subcontracting to, or consultation of, external staff shall be properly documented, shall not involve any intermediaries and shall be subject to a written agreement covering, among other things, confidentiality and conflicts of interest. The conformity assessment body in question shall take full responsibility for the tasks performed.

10. At all times and for each conformity assessment procedure and each type, category or sub-category of ICT products, ICT services, ICT processes or managed security services, a conformity assessment body shall have at its disposal the necessary:

(a) staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;

(b) descriptions of procedures in accordance with which conformity assessment is to be carried out, to ensure the transparency of those procedures and the possibility

of reproducing them. It shall have in place appropriate policies and procedures that distinguish between tasks that it carries out as a body notified pursuant to Article 61 and its other activities;

(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the technology of the ICT product, ICT service, ICT process or managed security service in question and the mass or serial nature of the production process.

11. A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner, and shall have access to all necessary equipment and facilities.

12. The persons responsible for carrying out conformity assessment activities shall have the following:

(a) sound technical and vocational training covering all conformity assessment activities;

(b) satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate authority to carry out those assessments;

(c) appropriate knowledge and understanding of the applicable requirements and testing standards;

(d) the ability to draw up certificates, records and reports demonstrating that conformity assessments have been carried out.

13. The impartiality of the conformity assessment bodies, of their top-level management, of the persons responsible for carrying out conformity assessment activities, and of any subcontractors shall be guaranteed.

14. The remuneration of the top-level management and of the persons responsible for carrying out conformity assessment activities shall not depend on the number of conformity assessments carried out or on the results of those assessments.

15. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the Member State in accordance with its national law, or the Member State itself is directly responsible for the conformity assessment.

16. The conformity assessment body and its staff, its committees, its subsidiaries, its subcontractors, and any associated body or the staff of external bodies of a conformity assessment body shall maintain confidentiality and observe professional secrecy with regard to all information obtained in carrying out their conformity assessment tasks under this Regulation or pursuant to any provision of national law giving effect to this Regulation, except where disclosure is required by Union or Member State law to which such persons are subject, and except in relation to the competent authorities of the Member States in which its activities are carried out. Intellectual property rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this point.

17. With the exception of point 16, the requirements of this Annex shall not preclude exchanges of technical information and regulatory guidance between a conformity assessment body and a person who applies for certification or who is considering whether to apply for certification.

18. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of SMEs in relation to fees.

19. Conformity assessment bodies shall meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing certification of ICT products, ICT services, ICT processes or managed security services.

20. Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of the relevant standard that is harmonised under Regulation (EC) No 765/2008 for the accreditation of laboratories performing testing.