Council of the European Union

Brussels, 21 April 2023
(OR. en)

8511/23

Interinstitutional File: 2023/0108(COD)

CYBER 91
JAI 469
TELECOM 107
DATAPROTECT 109
MI 312
IND 180
CODEC 661

PROPOSAL

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	19 April 2023
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2023) 208 final
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security services

Delegations will find attached document COM(2023) 208 final.

Encl.: COM(2023) 208 final

EUROPEAN
COMMISSION

Strasbourg, 18.4.2023
COM(2023) 208 final

2023/0108 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

This explanatory memorandum accompanies the proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881[1] as regards managed security services.

The proposed targeted amendment 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. Managed security services play an increasingly important role in the prevention and mitigation of cybersecurity incidents.

In its conclusions of 23 May 2022[2] on the development of the European Union's cyber posture, the Council called upon the Union and its Member States to reinforce efforts to raise the overall level of cybersecurity, for example by facilitating the emergence of trusted cybersecurity service providers, and stressed that encouraging the development of such providers should be a priority for the industrial policy of the Union in the cybersecurity field. It also invited the Commission to propose options to encourage the emergence of a trusted cybersecurity service industry. The certification of managed security services is an effective means of building trust in the quality of those services and thereby facilitating the emergence of a trusted European cybersecurity service industry.

The Joint Communication 'EU Policy on Cyber Defence' adopted by the Commission and the High Representative on 10 November 2022[3], announced that the Commission would explore the development of EU-level cybersecurity certification schemes for cybersecurity industry and private companies. Managed security services providers will also play an important role in the EU-level cybersecurity reserve, the gradual set-up of which is supported by the Cyber Solidarity Act, proposed in parallel to this Regulation. The EU-level cybersecurity reserve is to be used to support response and immediate recovery actions in the event of significant and large-scale cybersecurity incidents. The relevant cybersecurity services provided by 'trusted providers' referred to in the Cyber Solidarity Act, correspond to 'managed security services' in this proposal.

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 enables the creation of European cybersecurity certification schemes for those services to prevent such fragmentation.

• Consistency with existing policy provisions in the policy area

This proposal is consistent with the Cybersecurity Act, which it amends. It builds on the provisions of that Regulation and adapts them to also include managed security services. The

---

1 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 151/15, 7.6.2019.

2 9364/22.

3 JOIN(2022) 49 final.

proposed amendments are limited to what is strictly necessary and do not alter the characteristics or the functioning of the Cybersecurity Act.

This proposal is also consistent with 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)[4]. The providers of managed security services are considered to be essential or important entities belonging to a sector of high criticality under Directive (EU) 2022/2555. Recital 86 of that Directive states that 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.

This proposal aims to improve the quality of managed security services and to increase their comparability. It thereby enables essential and important entities to exercise the increased diligence in selecting a managed security service provider as required under Directive (EU) 2022/2555. Moreover, the definition of 'managed security services' in this proposal is derived from and very similar to the definition of 'managed security services providers' in Directive (EU) 2022/2555. For these reasons, the proposal is highly complementary with the NIS 2 Directive.

Finally, this proposal is complementary with the proposed Cyber Solidarity Act. The proposed Cyber Solidarity Act lays down a process to select the providers to form an EU-level cybersecurity reserve, which should, *inter alia*, take into account whether those providers have obtained European or national cybersecurity certification. Future certification schemes for managed security services will thus play a significant role in the implementation of the Cyber Solidarity Act.

- **Consistency with other Union policies**

This proposal does not affect the Cybersecurity Act's consistency with Regulation (EU) 2016/679 (the General Data Protection Regulation, 'GDPR')[5] and its provisions on establishing certification mechanisms and data protection seals and marks for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The Cybersecurity Act remains without prejudice to the certification of data processing operations, including when such operations are embedded in products and services, under the GDPR.

Furthermore, this proposal does not affect the Cybersecurity Act's compatibility with Regulation (EC) No 765/2008 on accreditation and market surveillance requirements[6], in particular as regards the framework on national accreditation bodies and conformity assessment bodies, and national certification supervisory authorities.

4 OJ L 333/810, 27.12.2022.
5 OJ L 119/1, 4.5.2016.
6 OJ L 218/30, 13.8.2008.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

This proposal amends the Cybersecurity Act, which is based on Article 114 of the Treaty on the functioning of the European Union (TFEU). As in the case of the Cybersecurity Act, this proposal aims to avoid fragmentation of the internal market, namely by enabling the adoption of European cybersecurity certification schemes for managed security services. Member States have started to adopt national certification schemes for managed security services. There is thus a concrete risk of fragmentation of the internal market for these services, which the present proposal aims to address. Therefore, Article 114 TFEU is the relevant legal basis for this initiative.

• Subsidiarity (for non-exclusive competence)

The objective of enabling the adoption of European cybersecurity certification schemes for managed security and avoiding fragmentation of the internal market cannot be achieved at national level but only at Union level. Furthermore, managed security services, which are the targeted subject of the proposed amendment, are offered by providers active across the Union, as are their largest potential customers. Action at Union level is therefore both necessary and more effective than action at national level.

• Proportionality

The proposal is a targeted amendment of the Cybersecurity Act. It is limited to what is strictly necessary to achieve its objective, namely to enable the adoption of European cybersecurity certification schemes for managed security services, in addition to ICT products, ICT services and ICT processes. The proposed amendments adapt, in particular, the scope of the European cybersecurity certification framework to include 'managed security services', introduce a definition of those services in line with the NIS 2 Directive, and amend the security objectives of European cybersecurity certification in order to adapt it to 'managed security services'. The other amendments are of a technical nature and are intended to ensure that the relevant articles apply also to 'managed security services'. The proposed initiative is thus proportionate to the objective.

• Choice of the instrument

As the proposal amends Regulation (EU) 2019/881, the appropriate legal instrument is a Regulation.

3. RESULTS OF *EX POST* EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

• *Ex post* evaluations/fitness checks of existing legislation

Not applicable.

• Stakeholder consultations

Targeted consultations with Member States and ENISA have been carried out. In these consultations, Member States described their current activities and views as regards certification of managed security services. ENISA explained its views and its findings from discussions with Member States and stakeholders. The comments and information received from Member States and ENISA have fed into this proposal.

• Collection and use of expertise

Not applicable.

- **Impact assessment**

A waiver from the need for an impact assessment has been requested as the proposal is a very limited and targeted amendment to the Cybersecurity Act. It would empower the Commission to adopt, by means of implementing acts, certification schemes for 'managed security services', in addition to ICT products, ICT services and ICT processes, which are already covered by the Act. However, the amendment would only have an effect once such certification schemes are adopted at a later stage. Moreover, the amendment would not change the voluntary character of the certification schemes.

- **Regulatory fitness and simplification**

Not applicable.

- **Fundamental rights**

The proposal does not have any foreseeable consequences for the protection of fundamental rights.

4. BUDGETARY IMPLICATIONS

None.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The provisions to be amended by the proposal will be evaluated as part of the periodic evaluation of the Cybersecurity Act to be carried out by the Commission in accordance with Article 67 thereof. That evaluation assesses, *inter alia*, the impact, effectiveness and efficiency of the provisions on the Cybersecurity Certification Framework with regard to the objectives of ensuring an adequate level of cybersecurity of ICT products, ICT services and ICT processes in the Union and of improving the functioning of the internal market. The proposal contains an amendment that ensures that the evaluation is also to cover managed security services. The Commission also sends a report on the evaluation and its conclusions to the European Parliament, the Council and the ENISA Management Board and makes the findings of the report public.

- **Detailed explanation of the specific provisions of the proposal**

The proposal contains two articles. While Article 1 contains the amendments to Regulation (EU) 2019/881, Article 2 concerns the entry into force. Article 1 contains targeted amendments to amend the scope of the European cybersecurity certification framework in the Cybersecurity Act to include 'managed security services' (Articles 1 and 46 of the Cybersecurity Act). It 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 a new Article 51a on the security objectives of European cybersecurity certification adapted to 'managed security services'. Lastly, the proposal contains a number of technical amendments to ensure that the relevant articles apply also to 'managed security services'.

2023/0108 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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,

Having regard to the opinion of the Committee of the Regions;

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Regulation (EU) 2019/881 of the European Parliament and of the Council[7] 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.

(2) 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[8]. 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

[7] 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).

[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).

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.

(3) Managed security services providers also play an important role in the EU Cybersecurity Reserve whose gradual set-up is supported by Regulation (EU) …/…. [laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents] The EU Cybersecurity Reserve is to be used to support response and immediate recovery actions in case of significant and large-scale cybersecurity incidents. Regulation (EU) …/…[laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents] lays down a selection process for the providers forming the EU Cybersecurity Reserve, which should, inter alia, take into account whether the provider concerned has obtained a European or national cybersecurity certification. The relevant services provided by 'trusted providers' according to Regulation (EU) …./…..[laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents] correspond to 'managed security services' in accordance with this Regulation.

(4) 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.

(5) 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 a managed security service can be covered by a certification scheme, it is therefore necessary to amend Regulation (EU) 2019/881

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 and delivered an opinion on [DD/MM/YYYY

HAVE ADOPTED THIS REGULATION:

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 consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, penetration testing, security audits and consultancy’;

(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 very high 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;

(d) developments in the cyber threat landscape;

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

(7) in Article 49, 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, 52 and 54. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).';

(8) 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:'

(9) 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) ensure 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 very high level of technical knowledge and competence in the specific field, sufficient and appropriate experience, and the highest degree of professional integrity;

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

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

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

(g) ensure that the ICT products, ICT services and ICT processes [and the hardware] deployed in the provision of the managed security services are secure by default and by design, do not contain known vulnerabilities and include the latest security updates;';

(10) 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.';

(11) 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.';

(12) 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;';

(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 or managed security services processes;';

(13) 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 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.'

(14) 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.';

(15) 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 and managed security services processes.';

(16) 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);';

(17) 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 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.'.

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 Strasbourg,

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