European Parliament
2019-2024

Plenary sitting

A9-0307/2023

26.10.2023

***I
REPORT

on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Committee on Industry, Research and Energy

Rapporteur: Josianne Cutajar

Symbols for procedures

*	Consultation procedure
***	Consent procedure
***I	Ordinary legislative procedure (first reading)
***II	Ordinary legislative procedure (second reading)
***III	Ordinary legislative procedure (third reading)

(The type of procedure depends on the legal basis proposed by the draft act.)

Amendments to a draft act

Amendments by Parliament set out in two columns

Deletions are indicated in ***bold italics*** in the left-hand column. Replacements are indicated in ***bold italics*** in both columns. New text is indicated in ***bold italics*** in the right-hand column.

The first and second lines of the header of each amendment identify the relevant part of the draft act under consideration. If an amendment pertains to an existing act that the draft act is seeking to amend, the amendment heading includes a third line identifying the existing act and a fourth line identifying the provision in that act that Parliament wishes to amend.

Amendments by Parliament in the form of a consolidated text

New text is highlighted in ***bold italics***. Deletions are indicated using either the ▌ symbol or strikeout. Replacements are indicated by highlighting the new text in ***bold italics*** and by deleting or striking out the text that has been replaced.
By way of exception, purely technical changes made by the drafting departments in preparing the final text are not highlighted.

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services

(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2023)0208),

– having regard to Article 294(2) and Article 114 of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C9-0137/2023),

– having regard to Article 294(3) of the Treaty on the Functioning of the European Union,

– having regard to the opinion of the European Economic and Social Committee of 13 July 2023[1],

– having regard to Rule 59 of its Rules of Procedure,

– having regard to the letter from the Committee on the Internal Market and Consumer Protection,

– having regard to the report of the Committee on Industry, Research and Energy (A9-0307/2023),

1. Adopts its position at first reading hereinafter set out;

2. Calls on the Commission to refer the matter to Parliament again if it replaces, substantially amends or intends to substantially amend its proposal;

3. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

[1] OJ C 349, 29.9.2023, p. 167.

Amendment 1

AMENDMENTS BY THE EUROPEAN PARLIAMENT*

to the Commission proposal

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[1],

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

Acting in accordance with the ordinary legislative procedure[2]**,**

---

* Amendments: new or amended text is highlighted in bold italics; deletions are indicated by the symbol ▌.

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

2 ***Position of the European Parliament of … (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[3] 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.

(1a) 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[4] (2022/0272(COD)), by setting up essential requirements for cybersecurity managed services, their application and their trustworthiness.

(2) Managed security services, which are services consisting of carrying out, or providing assistance for, activities relating to their customers' cybersecurity risk management, ***including detection, response to or recovery from incidents,*** have gained increasing importance in the prevention and mitigation of cybersecurity incidents. ***The activities of the providers of managed security services consist of services relating to prevention, identification, protection, detection, analysis, containment, response and recovery, including, but not limited to, cyber threat intelligence provision, real time threat monitoring through proactive techniques, including security-by-design, risk assessment, extended detection, remediation and response.*** Accordingly, the providers of those services are considered as essential or important entities belonging to a sector of high criticality pursuant to Directive (EU)

---

3 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).

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

2022/2555 of the European Parliament and of the Council[5]. 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.

(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

---

5 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).

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.

(4a) European certification schemes for managed security services should lead to the uptake of those services and to increased competition in the field, taking into account the specific needs of both providers and beneficiaries. Those schemes should, therefore, strike a balance between the their objective and the potential regulatory, administrative and financial burden that providers, especially microenterprises or small and medium-sized enterprises (SMEs), could encounter. Additionally, the schemes should encourage the use of certified managed security services by contributing 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.

(4b) The Union certification scheme for managed security services should ensure the availability of secure and high-quality services which guarantee a safe digital transition and contribute 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.

(4c) In the current fast evolving digital and technological landscape, the offer of educational resources and formal trainings differ and knowledge can be acquired in various ways, both formal, for example through university or courses and non-formal, for example through on the job trainings or longstanding work experience in the relevant field.

(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 ***dedicated*** certification scheme, it is therefore necessary to amend Regulation (EU) 2019/881. The ***development of certification schemes established pursuant to this Regulation should take into account the results and recommendations of the evaluation and review provided for in this Regulation.***

(5a) With a view to facilitating the growth of a reliable Union market, whilst also creating partnerships with likeminded third countries, including in light of the provisions of the Regulation (EU) .../... of the European Parliament and of the Council[6] (2023/0109(COD)) with regard to the access to the EU Cybersecurity Reserve, the certification process established within the framework established by this Regulation should be streamlined to ensure international recognition and alignment with international standards.

(5b) With the aim of ensuring the development of a trustworthy Union market for managed security services, the providers thereof and Member States should collaborate and contribute to the collection of data on the situation and the evolution of the cybersecurity labour market.

(5c) A Union-wide coordinated approach to strengthening the resilience of critical infrastructure is based on the Member States' capacity building. However, 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. 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, cooperation between Member States, the Commission, ENISA and stakeholders, including the private sector and academia,

---

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

should be 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. This should 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. Those measures should also aim to attract more women and girls in the field and contribute towards addressing the gender gap in science, technology, engineering, and mathematics. The private sector should also aim to deliver on-the-job training addressing the most in-demand skills, involving public administration and start-ups, as well as microenterprises and SMEs.

(5d) Appropriate funding and resources should be ensured for the purpose of the additional tasks entrusted to ENISA by the amendments to Regulation (EU) 2019/881 introduced by this Regulation.

(5e) In order to supplement certain non-essential elements of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission to provide for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes and managed security services. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[7] . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

---

7 OJ L 123, 12.5.2016, p. 1

(5e) 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][8],

HAVE ADOPTED THIS REGULATION:

[8] *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***, or advice on***

activities relating to cybersecurity risk management, including ***incident handling****,* penetration testing, security audits and consulting';

(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, 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. ***In that context, the Commission may include an in-depth assessment of existing training paths to bridge identified skills gaps and a list of proposals for addressing the needs for skilled employees and types of skills.***

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, 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) paragraph 7 is replaced by the following:

'7. The Commission, based on the candidate scheme prepared by ENISA, ***is empowered to*** adopt ***delegated*** acts ***in accordance with Article 65a, supplementing this Regulation by*** 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***.';***

(b) the following paragraph is inserted:

'7a. Before adopting such delegated acts, the Commission, in cooperation with ENISA, shall carry out and publish an impact assessment of the proposed European cybersecurity certification scheme. While preparing the impact assessment, the Commission shall carry out public consultations and shall consult the SCCG and ECCG.';

(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 51aSecurity 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 deployed in the provision of the managed security services are secure by default and by design ***and are provided with up-to-date software and hardware,*** 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 ***the specific interests and needs of microenterprises and SMEs;';***

(iii) the following subparagraph is added:

'With regard to the third subparagraph, point (d) of this Article, theCommission shall ensure appropriate financial support in the regulatory framework of existing Union programmes, in particular in order to ease the financial burden on microenterprises and SMEs, including start-ups acting in the field of managed security services.';

(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 ***delegated 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 Article 54(1), point (j), 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);’

(16a) the following article is inserted:

‘Article 65a
Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 49(7) shall be conferred on the Commission for a period of five years from … [date of entry into force of the amended regulation]. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Article 49(7) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 49(7) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by [two months] at the initiative of the European Parliament or of the Council.;'

(17) Article 67 is replaced by the following:

'Article 67

Evaluation and review

1. By 28 June 2024, and every three years thereafter, the Commission shall assess the impact, effectiveness and efficiency of ENISA and of its working practices, the possible need to modify ENISA's mandate and the financial implications of any such modification. The evaluation shall take into account any feedback provided to ENISA in response to its activities. Where the Commission considers that the continued operation of ENISA is no longer justified in light of the objectives, mandate and tasks assigned to it, the Commission may propose that this Regulation be amended with regard to the provisions related to ENISA.

2. The evaluation shall 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 also assess:

(a) the efficiency and effectiveness of the procedures leading to consultation, preparation and adoption of European cybersecurity certification schemes, as well as ways to improve and accelerate those

procedures;

(b) 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.

4. By 28 June 2024, and every three years thereafter, the Commission shall transmit a report on the evaluation together with its conclusions to the European Parliament, to the Council and to the Management Board. The findings of that report shall be made public.'

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*

EXPLANATORY STATEMENT

The Rapporteur supports the proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/8811 as regards managed security services, understanding its necessity to update and strengthen the European cybersecurity certification scheme by allowing it to cover important and growing industry services. Considering how individual Member States have already begun adopting certification schemes for managed security services, the Rapporteur takes the view that this amendment to the Cyber Security Act is critical to preventing significant divergences in national schemes that would result in a form of market fragmentation which is against the Union´s economic, and also strategic interests.

On this note, it is acknowledged how this proposal is envisioned to complement the Cyber Solidarity Act, particularly this specific extension to the European cybersecurity certification scheme, will allow for managed security services - corresponding to ´trusted providers´ in the Cyber Solidarity Act - to play an important role in the future EU Cybersecurity Reserve. Therefore, this proposal is one that is also of great importance in fostering broader Union cybersecurity capacity, which capacity is essential to counteract potential threats in an ever-evolving geopolitical reality.

Within the limits of the Commission´s proposal, the Rapporteur's objective is to consolidate and add further clarity to this targeted amendment to the Cybersecurity Act. This is illustrated by the Rapporteur´s changes to the definition of managed security services, clarifying that they are 'outsourced', while concurrently detailing further what can be included in the definition. Tabled amendments regarding the recognition of international cybersecurity standards are intended to foster a higher caliber of confidence while simultaneously developing comprehensive EU rules.

This draft report puts stronger emphasis on addressing the skills gap and in supporting Micro, Small and Medium Enterprises. On the former, tabled amendments build on the already implicit necessity of skills in the cyber certification scheme vis-a-vis 'the requisite competence, expertise and experience by staff with a very high level of relevant technical knowledge and professional integrity'. In the Rapporteur's view, whilst fostering cooperation

amongst all actors involved as well as between Member States, the private sector, academia and research institutions, the European certification scheme must act as an enabler of a new roadmap to training and empowering the workforce, collecting more data on the skills needed and contributing towards addressing the gender gap in STEM.

At the same time, micro, small and medium enterprises, which form the backbone of the European economy and certainly have a positive role to play in the cybersecurity industry, should benefit from appropriate financial support in the regulatory framework of existing Union programmes to ease any disproportionate financial burden placed upon them.

21.9.2023

LETTER OF THE COMMITTEE ON THE INTERNAL MARKET AND CONSUMER PROTECTION

Mr Cristian Silviu Buşoi
Chair
Committee on Industry, Research and Energy
BRUSSELS

Subject: Opinion on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Dear Mr Chair,

Under the procedure referred to above, the Committee on the Internal Market and Consumer Protection has been asked to submit an opinion to your committee. At its meeting of 23 May 2023, the committee decided to send the opinion in the form of a letter. It considered the matter at its meeting of 19 September 2023 and adopted the opinion at that meeting.

At that meeting[1], it decided to call on the Committee on Industry, Research and Energy (ITRE), as the committee responsible, to incorporate the following suggestions into its legislative report.

Yours sincerely,

Anna Cavazzini

SUGGESTIONS

The Committee on Internal Market and Consumer Protection calls on the Committee on Industry, Research and Energy, as the Committee responsible, to take into account the following suggestions:

[1] The following were present for the final vote: Anna Cavazzini (Chair), Andrus Ansip (Vice-Chair), Krzysztof Hetman (Vice-Chair), Alex Agius Saliba, João Albuquerque, Pablo Arias Echeverría, Laura Ballarín Cereza, Alessandra Basso, Brando Benifei, Biljana Borzan, Vlad Marius Botoş, Deirdre Clune, Dita Charanzová, David Cormand, Carlo Fidanza, Malte Gallée, Sandro Gozi, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Marcel Kolaja, Andrey Kovatchev, Jean-Lin Lacapelle, Morten Løkkegaard, Beata Mazurek, Leszek Miller, Anne Sophie Pelletier, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Tom Vandenkendelaere, Kim Van Sparrentak.

A. Whereas the Commission published a legislative proposal on managed security services that entails targeted amendments to the EU Cybersecurity Act on 18 April 2023[2];

B. Whereas on the legislative proposal for the EU Cybersecurity Act (2017/0225(COD))[3], the Committee on the Internal Market and Consumer Protection (IMCO) submitted an opinion under former Rule 54 of the Rules of Procedure to the responsible Committee on Industry, Research and Energy (ITRE) with shared competences on the cybersecurity certification framework, given IMCO´s clear competence in relation to certification schemes and, in general, standardisation, market surveillance and implementation of the Digital Single Market;

C. Whereas the EU Cybersecurity Act[4] aims to achieve 1) a high level of cybersecurity, cyber resilience and trust in the EU by setting objectives, tasks and organisational matters for a strengthened and renamed European Union Agency for Cybersecurity (ENISA), with a new permanent mandate, and 2) a framework for voluntary European cybersecurity certification schemes for information and communications technology (ICT) products, services and processes;

D. Whereas the proposed targeted amendments to include managed security services to the scope of the EU Cybersecurity Act and add a definition of those services that is closely aligned to the definition under the NIS 2 Directive[5]; whereas the amendments would enable the Commission by means of implementing acts to adopt European cybersecurity certification schemes for managed security services, in addition to ICT products, services and processes, which are already covered under the EU Cybersecurity Act;

E. Whereas managed security services play an increasingly important role in the prevention and mitigation of cybersecurity incidents;

1. Acknowledges that on 23 May 2022[6] the Council called for an increase of the overall level of cybersecurity in the EU by facilitating the emergence and development of trusted cybersecurity service providers; considers that, among others, the war in Ukraine, the current geopolitical context and continuous threats from third country regimes as well as a continuously growing market of digital technologies and digital transformation of processes in general have led to the need for a higher level of cybersecurity in the EU and its Member States; recommends that the Commission should take proactive measures to support the development of trusted cybersecurity service providers such as funding for research and development, training programmes to build cybersecurity skills, and incentives for businesses to invest in cybersecurity; suggests that the EU should strengthen its cooperation with NATO and other international partners to respond to cyber threats from third country regimes, including sharing of threat intelligence, joint exercises, and coordinated responses to cyber-attacks;

---

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0208

[3] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2017/0225(OLP)

[4] OJ L 151, 7.6.2019, p. 15

[5] OJ L 333/810, 27.12.2022

[6] 9364/22

2. Stresses that the certification of managed security services, based on non-discriminatory rules and reflecting European and international standards, is essential for building and guaranteeing trust in the quality of those services, in particular with an aim for achieving a high level of consumer protection; notes that some Member States have already adopted certification schemes for managed security services and that therefore it is essential to avoid fragmentation in the internal market and inconsistencies, which may affect the cybersecurity industry and businesses, and to enable a harmonised approach through the creation of a European cybersecurity certification scheme for such services; asks that the cybersecurity certification framework should incorporate the best practices from existing national certification schemes and be developed in consultation with key stakeholders in the cybersecurity industry;

3. Highlights that managed security service providers, in areas such as incident response, penetration testing, security audits and consultancy, play an important role in assisting entities in their efforts to prevent, detect, respond to or recover from cyber incidents; considers that as more and more companies struggle to maintain various complex software systems and interconnected corporate networks, they are necessarily relying on managed security service providers and therefore such providers should be considered an essential element in the EU's cybersecurity ecosystem; notes however that managed security service providers have also themselves been the target of cyberattacks and may pose a particular risk because of their close integration in the operations of their customers;

4. Recalls the importance of the recently adopted NIS 2 Directive to ensure a greater level of cyber resilience throughout the Union; calls for the rapid adoption and implementation of implementing acts under this Directive in order to ensure that providers of managed security services comply with the Directive's requirements on cybersecurity risk-management measures;

5. Recommends that managed security service providers should be required to adhere to relevant cybersecurity standards and undergo regular reviews to ensure their systems are secure to protect not only the providers themselves but also the entities they serve; considers that such reviews should assess the providers' compliance with the EU-wide cybersecurity certification framework and their ability to protect both their systems and those of their customers from cyber threats;

6. Welcomes the legislative proposal on managed security services, which aims to improve the quality of managed security services and to increase their comparability to the benefit of a proper functioning of the internal market and implementation of the Digital Single Market; stresses that certification of managed security services is relevant in the selection process for the EU Cybersecurity Reserve and is also a significant quality and trust indicator for private and public entities that aim to purchase such services;

7. Notes that the proposal strengthens the role of ENISA, which should support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, services, processes and managed security services, by regularly monitoring developments in related areas of standardisation and recommending technical specifications, where standards are not available; suggests that ENISA should be given additional resources and authority to carry out its expanded role, including funding for

research and development, and a clear mandate to coordinate with national cybersecurity agencies and industry stakeholders; underlines the essential role of computer security incident response teams (CSIRTs) in achieving predictable and safe digital space for businesses and citizens;

8. Calls on the Commission and ENISA to support and ensure consistent implementation of the European cybersecurity certification scheme based on non-discriminatory rules and reflecting European and international standards for the conformity self-assessment by the manufacturer or provider of ICT products, services, processes or managed security services, in accordance with the EU Cybersecurity Act; believes that the implementation should help to offset the costs of accreditation and encourage more manufacturers or providers to participate in the scheme;

9. Stresses that each certification scheme should be designed in such a way as to stimulate and encourage all actors involved in the sector concerned to develop and adopt regularly updated security standards, technical norms and security-by-design and privacy-by-design principles, at all stages of the product or service lifecycle; highlights that input from civil society and independent security researchers relevant stakeholders needs to be taken into account in a more systematic way when developing such principles; considers that the certification schemes should be consistent with other European cybersecurity certification schemes adopted in accordance with the EU Cybersecurity Act and should avoid disproportionate burden on providers; recommends that certification schemes should include clear and detailed guidelines on how to implement security-by-design and privacy-by-design principles, where such guidelines are in accordance with the provisions setting out the framework for European cybersecurity schemes in the EU Cybersecurity Act; suggests that, where necessary and proportionate, certification schemes should consist of a mechanism for continuous improvement, such as regular reviews and updates of the security standards and technical norms; considers that the mechanism should take into account the latest developments in cybersecurity threats and technologies; encourages that each certification scheme should include measures to promote transparency and accountability, such as public disclosure of certification results and penalties for non-compliance;

10. Calls for the introduction of an voluntary EU Trust Label for certified ICT products, services, processes and managed security services; highlights in this regard that the label could help raise awareness of cybersecurity across the internal market and give companies with good cybersecurity credentials a competitive edge; suggests that the EU Trust Label should be designed to be easily recognisable and understandable by consumers and businesses;

11. Recommends the Commission and ENISA to establish a dedicated research and development program for cybersecurity; recommends that the Commission and ENISA should establish a cybersecurity risk assessment framework for businesses containing guidelines on how to identify, assess, and mitigate cybersecurity risks, and could be tailored to different sectors and sizes of companies; suggests that the Commission and ENISA should offer help and assistance to the Member States to establish a cybersecurity incident reporting mechanism for consumers and businesses to facilitate the collection of data on cybersecurity incidents, which could be used to improve cybersecurity policies and practices.

PROCEDURE – COMMITTEE RESPONSIBLE

Title	Amending Regulation (EU) 2019/881 as regards managed security services
References	COM(2023)0208 – C9-0137/2023 – 2023/0108(COD)
Date submitted to Parliament	19.4.2023
Committee responsible Date announced in plenary	ITRE 1.6.2023
Committees asked for opinions Date announced in plenary	IMCO LIBE 1.6.2023 1.6.2023
Not delivering opinions Date of decision	LIBE 30.5.2023
Rapporteurs Date appointed	Josianne Cutajar 2.5.2023
Discussed in committee	19.7.2023 19.9.2023
Date adopted	25.10.2023
Result of final vote	+: 57 –: 0 0: 2
Members present for the final vote	Matteo Adinolfi, Nicola Beer, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Michael Bloss, Paolo Borchia, Marc Botenga, Markus Buchheit, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Beatrice Covassi, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Christian Ehler, Lina Gálvez Muñoz, Jens Geier, Bart Groothuis, Christophe Grudler, Henrike Hahn, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Thierry Mariani, Marina Mesure, Dan Nica, Niklas Nienass, Ville Niinistö, Johan Nissinen, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Clara Ponsatí Obiols, Manuela Ripa, Sara Skyttedal, Riho Terras, Patrizia Toia, Henna Virkkunen, Pernille Weiss, Carlos Zorrinho
Substitutes present for the final vote	Pascal Arimont, Tiziana Beghin, Franc Bogovič, Damien Carême, Martina Dlabajová, Francesca Donato, Matthias Ecke, Nicolás González Casares, Ladislav Ilčić, Luděk Niedermayer, Emma Wiesner
Substitutes under Rule 209(7) present for the final vote	Asim Ademov, Aušra Maldeikienė, Irène Tolleret
Date tabled	26.10.2023

FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE

57	+
ECR	Ladislav Ilčić
ID	Matteo Adinolfi, Paolo Borchia, Marie Dauchy, Thierry Mariani
NI	Tiziana Beghin, Francesca Donato, Clara Ponsatí Obiols
PPE	Asim Ademov, Pascal Arimont, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Franc Bogovič, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Aušra Maldeikienė, Luděk Niedermayer, Markus Pieper, Sara Skyttedal, Riho Terras, Henna Virkkunen, Pernille Weiss
Renew	Nicola Beer, Nicola Danti, Martina Dlabajová, Bart Groothuis, Christophe Grudler, Mauri Pekkarinen, Morten Petersen, Irène Tolleret, Emma Wiesner
S&D	Beatrice Covassi, Josianne Cutajar, Matthias Ecke, Lina Gálvez Muñoz, Jens Geier, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Dan Nica, Tsvetelina Penkova, Patrizia Toia, Carlos Zorrinho
The Left	Marc Botenga, Marina Mesure
Verts/ALE	Michael Bloss, Damien Carême, Ciarán Cuffe, Henrike Hahn, Niklas Nienass, Ville Niinistö, Manuela Ripa

0	-

2	0
ECR	Johan Nissinen
ID	Markus Buchheit

Key to symbols:
+ : in favour
- : against
0 : abstention