EDPS

**EUROPEAN DATA PROTECTION SUPERVISOR**

The EU's independent data protection authority

10 January 2024

# Opinion 2/2024

on the Proposal for a Regulation amending the Cybersecurity Act as regards managed security services

edps.europa.eu

*The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)'… for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.*

*Wojciech Rafał Wiewiórowski was appointed as Supervisor on 5 December 2019 for a term of five years.*

*Under* ***Article 42(1)*** *of Regulation 2018/1725, the Commission shall 'following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data'.*

*This Opinion relates to the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services*[1]*. This Opinion does not preclude any future additional comments or recommendations by the EDPS, in particular if further issues are identified or new information becomes available. Furthermore, this Opinion is without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Regulation (EU) 2018/1725. This Opinion is limited to the provisions of the Proposal that are relevant from a data protection perspective.*

[1] COM(2023) 208 final.

**Executive Summary**

On 18 April 2023, the European Commission issued the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services ('the Proposal').

The objective of the Proposal is to enable 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 Regulation (EU) 2019/881. The EDPS has been consulted by the European Commission on 14 November 2023 pursuant to Article 42(1) of EUDPR.

In the present Opinion, the EDPS welcomes the objectives of the Proposal and considers that cybersecurity certification schemes for managed security services could indeed incentivize offering such services and at the same time make the choice of a qualified service provider easier for small and medium enterprises that do not have internal security specialists and are dependent on external service providers. The EDPS proposes a number of changes to elements of the new Article 51a and recommends to establish within the Proposal a requirement for providers to self-declare that their services and measures proposed through them comply with the applicable regulatory framework, including data protection, as a condition for certification.

# Contents

**THE EUROPEAN DATA PROTECTION SUPERVISOR,**

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ('EUDPR')[2], and in particular Article 42(1) thereof,

**HAS ADOPTED THE FOLLOWING OPINION:**

# 1. Introduction

1. On 18 April 2023, the European Commission issued the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services[3] ('the Proposal').

2. The objective of the Proposal is 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[4]. According to the explanatory memorandum[5], managed security services play an increasingly important role in the prevention and mitigation of cybersecurity incidents. The certification of managed security services is seen as an effective means of building trust in the quality of those services and thereby facilitating the emergence of a trusted European cybersecurity service industry. 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[6].

3. The present Opinion of the EDPS is issued in response to a consultation by the European Commission of 14 November 2023 pursuant to Article 42(1) of EUDPR. The EDPS welcomes the reference to this consultation in the last (not numbered) Recital of the Proposal.

[2] OJ L 295, 21.11.2018, p. 39.
[3] COM(2023) 208 final.
[4] 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.
[5] COM(2023) 208 final, p. 1.
[6] COM(2023) 208 final, p. 1.

## 2. General remarks

4. The EDPS welcomes the objectives of the Proposal and considers that cybersecurity certification schemes for managed security services could indeed incentivize offering such services and at the same time make the choice of a qualified service provider easier for small and medium enterprises that do not have internal security specialists and are dependent on external service providers.

5. The EDPS recalls the recommendations provided in the EDPS Opinion 7/2022[7], on the relationship between cybersecurity and data protection, which remain valid also in the context of the current Proposal. While cybersecurity has been a part of data protection legislation since its beginnings and is established today by Article 5(1)(f) of the GDPR as one of the main principles relating to the processing of personal data, the EDPS also recalled that information security measures not only enhance personal data security and contribute to the protection of personal data, but that they also have the potential to interfere with the rights and freedoms of data subjects, especially the fundamental rights to the protection of personal data and to the privacy of electronic communications. Some of the services offered as managed security services, for example penetration testing, may have the potential to severely interfere with said fundamental rights. The EDPS therefore considers that providers of managed security services, even where not formally considered controllers of a processing suggested or initiated by them, should make a reasonable effort to deploy or propose only security measures that comply with the regulatory environment applicable to their services and the measures proposed, including data protection legislation, in order to be certified under the European cybersecurity certification schemes for managed security services. This would allow for service providers to propose legally viable measures and reduce compliance risks for small and medium enterprises.

6. Two provisions in the Proposal contain the substance of extending the cybersecurity certification schemes to managed security services. Therefore, the EDPS scrutinized especially the proposed changes in Article 46(2) and the insertion of an Article 51a in Regulation (EU) 2019/881. The EDPS notes that the other changes are editorial consequential changes.

## 3. Appropriate data protection knowledge

7. The new Article 51a would list the security objectives of European cybersecurity certification schemes for managed security services, that is, at a high level, the objectives ensured by any such certification scheme. The list is based on the previous Article 51 on the security objectives of European cybersecurity certification schemes for ICT products, services and processes, but is adjusted to the specificities of managed security services. Similar to ICT products, services and processes, managed security services that have been evaluated in accordance with the certification schemes shall comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity and

[7] EDPS Opinion 7/2022 on the Proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union, issued on 17 May 2022, paragraphs 9 and 10.

confidentiality of data, which are accessed, processed, stored or transmitted in relation to the provision of those services[8]. In addition, in the view of the EDPS, the Proposal takes into account that security is managed as a service by providers and the objectives therefore must focus more on factors ensuring the ability of the prospective provider to carry out those services. The EDPS notes that this is achieved by setting the objectives that services are provided continuously with the requisite competence, expertise and experience by staff with a certain level of relevant technical knowledge and professional integrity.

8. The EDPS welcomes the approach taken in the new Article 51a. However, as already indicated in the general remarks, the EDPS has some concerns if regulatory compliance aspects, especially data protection aspects, are not among the objectives to be ensured with the certification schemes.

9. The EDPS recalls that one function of the certification would be to generate trust in the services and to make managed security services of high quality available to those entities with little resources. This function would be counteracted if any proposed measure would have to be legally evaluated by the client. If in particular a small and medium enterprise relies on the certification of its providers, it may well be that it would be overstrained by the task to independently and critically evaluate the lawfulness of the measures proposed, despite of its potential role as controller. In order to avoid situations in which certified providers would propose measures involving disproportionate or otherwise illegal data processing, the EDPS recommends to require a self-declaration of compliance of their services and measures proposed through them with the applicable regulatory framework, including data protection, as a condition for certification.

# 4. Other comments related to security objectives (Article 51a)

10. Article 51a point (c) contains a requirement for the service provider to protect data processed by the provider in relation to the provision of managed security services. Although the words 'or otherwise processed' work as a catch-all provision, the EDPS proposes to add the word 'generated' to the list. As defined in the new point 14a of Article 2 of the Cybersecurity Act, '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. Some of these risk management tools are able to identify and gather information which could be used adversely, for leveraging attacks to organisations (e.g. system vulnerabilities, publicly disclosed information which can be used for social engineering attacks). Systems used for security information and event management (SIEM) aggregate logs and correlate events to identify threats and generate reports on the systems' security. In the opinion of the EDPS, it would therefore be appropriate to emphasize the criticality of the information produced by these systems by explicitly mentioning them, together with the terms 'accessed, stored, transmitted' which are already listed, by adding the term 'generated'.

11. Point (d) sets as an objective of certification schemes to ensure that the availability and access to data, services and functions is restored in a timely manner in the event of a

[8] Cf. the proposed amendment of Article 46(2) of the Cybersecurity Act.

physical or technical incident. The EDPS considers that both aspects - physical or technical - are exhaustive when it comes to security measures, but do not cover the full range of possible security incidents. Security incidents stemming from human errors or malicious acts from employees should also be covered, even if they neither constitute a breach of technical nor physical security. In order not to exclude any type of security incident, the EDPS proposes the following wording: 'ensure that the availability and access to data, services and functions is restored in a timely manner in the event of a security incident', without further qualification of the incident.

12. Point (e) sets as an objective to ensure that authorised persons, programs or machines are able only to access the data, services or functions 'to which their access rights refer'. The EDPS notes that the words 'to which their access rights refer' is based on the corresponding point (c) of the existing Article 51. However, the EDPS proposes to seize the opportunity to make both provisions more substantial and also data-protection oriented: currently, they provide that users should only access the resources for which they were granted access. If, instead, the phrase would be replaced by 'appropriate to the fulfillment of their duties', the formalistic view would be replaced by a substantive view addressing both security and data protection considerations that access rights must correspond to the 'need to know' or 'need to access' principle.

# 5. Conclusions

13. In light of the above, the EDPS makes the following recommendation:

    – *to establish within the Proposal a requirement for providers to self-declare that their services and measures proposed through them comply with the applicable regulatory framework, including data protection, as a condition for certification.*

Brussels, 10 January 2024

*(e-signed)*
Wojciech Rafał WIEWIÓROWSKI