EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

17 May 2022

Opinion 7/2022

on the Proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union

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 on the information security in the institutions, bodies, offices and agencies of the Union. 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 draft Proposal that are relevant from a data protection perspective.

Executive Summary

The European Commission adopted on 22 March 2022 a Proposal for a Regulation of the European Parliament and of the Council on the information security in the institutions, bodies, offices and agencies of the Union ('the Proposal').

The EDPS welcomes the aim of the Proposal to improve the security of information handled by the EUIs, by establishing common information security rules as well fostering a coherent information security culture in a specific legal instrument.

The EDPS observes that personal data security as mandated by the EUDPR has a scope that only partially overlaps with the scope of the information security under the Proposal. The latter focuses on the confidentiality of information, whereas the EUDPR ensures also integrity and availability. Furthermore, the EUDPR personal data security provisions specifically address the risks for the rights and freedoms of natural persons.

The Proposal requires the EUIs to adopt information security measures, which will inevitably involve the processing of personal data and of electronic communications data, including traffic data. The EDPS considers that it must be made evident that all information security measures involving processing of personal data should be compliant with the current data protection and privacy legal framework and that EUIs should take relevant technical and organisational safeguards to ensure this compliance in an accountable way.

To achieve legal certainty and foreseeability, and to ensure compliance with the EUDPR, the EDPS strongly advises that the Proposal, or at the very least, a delegated act to be adopted subsequently by the Commission, clearly defines the personal data processing activities that are allowed for the purposes of this Regulation. The EDPS also draws the attention to the need to ensure compliance with the EUDPR rules regarding transfers of personal data to third countries and international organisations. Moreover, the EDPS recommends explaining in a Recital, that all of the EUDPR provisions will apply, including the rules on international transfers.

The EDPS stresses the importance of integrating the privacy and data protection perspective in the information security management, in order to achieve positive synergies between the Proposal and privacy and data protection legislation, and provides specific recommendations on how such synergies can be achieved, including: a specific obligation for EU officials responsible for information security to cooperate closely with the data protection officer designated in accordance with Article 43 EUDPR; the integration of end-to-end encryption in the list of minimum security measures of the Proposal, where applicable, and in particular when exchanging sensitive non-classified information; and the promotion of an integrated information security risk management and an integrated incident handling process that serve both information security and data protection obligations on data breach notifications.

Table of contents

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

Having regard to Regulation (EC) No 2018/1725 of the European Parliament and of the Council of 23 October2018 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[1], and in particular Articles 42(1)thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1. The European Commission adopted on 22 March 2022 a Proposal for a Regulation of the European Parliament and of the Council on the information security in the institutions, bodies, offices and agencies of the Union[2] ('the Proposal').

2. On the same date, the European Commission adopted another Proposal for a Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union[3] ('the Cybersecurity Proposal').

3. Both Proposals had been envisaged by the EU's Cybersecurity Strategy for the Digital Decade presented on 16 December 2020[4] ('the Strategy'). The overall aim of the Strategy was to strengthen the Union's strategic autonomy in the fields of cybersecurity and to improve its resilience and collective response as well as to build a global and open Internet with strong guardrails to address the risks to security and fundamental rights and freedoms of people in Europe.[5]

4. The Proposal constitutes one of the regulatory initiatives of the Strategy, and in particular in the area of Cybersecurity of the EU Institutions, bodies, offices and agencies ('the EUIs'). According to the Strategy, the aim of the Proposal is twofold:

   - to facilitate the **interoperability of classified information systems**, allowing a seamless transfer of information between the different entities, and

   - to enable an **inter-institutional approach to the handling of EU classified information and sensitive non-classified information**, which could also serve as a model for interoperability across Member States, stating that the EU should also further develop its ability to communicate in a secure manner with relevant partners, building to the extent possible on existing arrangements and procedures.

5. The EDPS observes that the subject matter of the Proposal at hand is also directly related to the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 ('NIS 2.0 Proposal'). The EDPS recalls that he issued the Opinion 5/2021 on the Cybersecurity Strategy[6] and the NIS 2.0 Directive ('NIS 2.0 Opinion')[7] . For this reason the present Opinion will refer to the NIS 2.0 Opinion.

6. According to the explanatory memorandum of the Proposal, due to the ever-increasing amount of sensitive non-classified ('SNC') information and European Union classified information ('EUCI') that the EUIs need to share amongst themselves and considering the dramatic development of the threat landscape, the European administration is exposed to attacks in all its areas of activity. The information handled by the EUIs is very attractive for the threat actors and needs to be appropriately protected.

7. According to the explanatory memorandum, the Proposal would:

   - establish harmonised and comprehensive **categories of information**, as well as **common handling rules** for all EUIs,

   - set up a lean **cooperation scheme on information security** between EUIs able to foster a coherent information security culture across the European administration,

   - **modernise the information security policies** at all levels of classification/categorisation, for all EUIs, taking into account the digital transformation and the development of teleworking as a structural practice.

8. On 22 March 2022 the Commission consulted the European Data Protection Supervisor pursuant to Article 42(1) of Regulation (EU) 2018/1725 ('EUDPR')[8]. The comments and recommendations in this Opinion are limited to the provisions in the Proposal that are most relevant from a data protection and privacy perspective.

2. General remarks

9. The EDPS recalls that information security, which is the subject matter of the Proposal, has been a part of data protection legislation since its beginnings. Today Article 4(1)(f) of the EUDPR establishes **security as one of the main principles relating to the processing of personal data**. Article 33 of the EUDPR further defines the obligations applicable to both controllers and processors, to **ensure an appropriate level of security of personal data**. Both provisions clearly establish that **personal data security is essential for compliance with EU data protection law**. This is why, on the one hand, this Opinion analyses the Proposal as to whether it establishes an effective information security management system or contains effective measures to increase the security of information including personal data.

10. On the other hand, information security measures do not only enhance personal data security and do not only contribute to the protection of personal data, but 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. Therefore, this Opinion analyses the Proposal also as to whether it provides for measures to be taken, among others, **based on a valid legal basis, with specific and limited purposes, and are adequate, necessary and proportionate**.

11. The EDPS takes note that the subject matter of the Proposal has a different perspective from both the NIS 2.0 and the Cybersecurity Proposals. It is our understanding that cybersecurity focuses on the protection of network and information systems, the users of such systems, and other persons affected by cyber threats, while **the Proposal concerns**

information security in any form, not just information processed by IT systems that are affected by cyber threats.

12. The EDPS wishes to underline that while for the NIS 2.0 Proposal, which provides for obligations on Member States, the application of Regulation (EU) 2016/679 ('GDPR') and Directive 2002/58/EC (ePrivacy Directive) is relevant when processing personal data, for the current Proposal, which lays down rules for EUIs, **the EUDPR applies and plays an equally important role**.

13. The EDPS **welcomes** the aim of the Proposal to **improve the security of information handled by the EUIs**, by establishing common information security rules as well fostering a coherent information security culture in a specific legal instrument.

3. Specific comments

3.1. Scope of the Proposal and relationship with data Protection and Privacy legislation

14. According to Article 3(b) of the Proposal, 'information security' means ensuring the authenticity, availability, confidentiality, integrity and non-repudiation of information. However, the EDPS **observes** that according to Article 2(2), information is classified only with regard to **confidentiality**, and that, according to Article 2(3), the confidentiality levels 'are based on the damage that unauthorised disclosure may cause to the legitimate private and public interests, including those of the Union, Union institutions and bodies and Member States or other stakeholders'. The emphasis on confidentiality is also present in the Information security risk management process described in Article 5, where only the confidentiality level of information is taken into consideration.

15. As a consequence, the EDPS submits that **personal data security** as mandated by the EUDPR **has a scope that only partially overlaps with the scope of the information security under the Proposal**. Article 4(1)(f) EUDPR requires ensuring **integrity and confidentiality** of personal data, while Article 33 EUDPR requires ensuring the ongoing **confidentiality, integrity, availability and resilience** of processing systems and services by addressing the **risks for the rights and freedoms of natural persons**.

16. At the same time, similarly to what was already stated[1] in the NIS 2.0 Opinion, the pursuance of the objectives of information security may lead to deploying measures that interfere with the rights to data protection and privacy of individuals. This implies ensuring that **any limitation of the right to the protection of personal data and privacy must fulfil the requirements of Article 52(1) of EU Charter of Fundamental Rights**, in particular be achieved by way of a legislative measure, be necessary and proportionate, and respect the essence of the right.

17. The Proposal requires the EUIs to apply information security measures, either as mandatory ones, or as measures selected from a risk management process taking into

[1] See: paragraph 11 of the NIS 2.0 Opinion

account certain criteria. In practice, some of these measures will inevitably **involve the processing of personal data and of electronic communications data, including traffic data**. The Proposal contains already some mandatory measures that would imply personal data processing:

- Article 11(2): 'Identification' and 'authentication';
- Article 11(3): 'Adequate security logs';
- Article 17(1)(a): 'Strong authentication';
- Article 17(1)(f): 'measures to prevent and detect data leaks'.

18. The EDPS notes that the organisations acting as controllers and processors do not always realise that the data processed in information security systems and services may include personal data (e.g. IP addresses, device identifiers, network log files, access control log files, etc.). This might lead to certain risks of non-compliance with data protection and privacy principles, such as lawfulness of processing, data minimisation, purpose limitation, storage limitation, and obligations for lawful data transfers. The EDPS considers that it must be made evident that **all information security measures involving processing of personal data should be compliant with the current data protection and privacy legal framework** and that EUIs should take relevant technical and organisational safeguards to ensure this compliance in an accountable way. Even more so, if there is no appropriate legal basis for EUIs in order to process personal data to implement certain security measures, the creation and justification of such a legal basis should be considered.

19. Where an EU legal act envisages the processing of personal data, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data are being processed have sufficient guarantees that their personal data are effectively protected against the risk of abuse and against any unlawful access and use of that data (see, CJEU, judgment of 8 April 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 54, and by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., Liberty and Others v. the United Kingdom, 1 July 2008, no. 58243/00, § 62 and 63; Rotaru v. Romania, § 57 to 59, and S. and Marper v. the United Kingdom, § 99).

20. To achieve legal certainty and foreseeability, and to ensure compliance with the EUDPR, in particular with Article 5(1)(a) and 5(2), the EDPS **strongly advises that the Proposal clearly defines the personal data processing activities that are allowed for the purposes of this Regulation (unless differently specified in another sectoral/specific legal text)**, including: the purpose(s) of the processing; categories of personal data; categories of data subjects; definition of roles as applicable (controller, processor, joint controllers), retention periods, recipients in case of transmission to entities not subject to the EUDPR. The EDPS considers that these elements should be provided for explicitly in the Proposal, or at the very least, in a delegated act to be adopted subsequently by the Commission. The Proposal should provide for such a delegation. The EDPS also draws attention to the need to ensure compliance with the EUDPR rules regarding transfers of personal data to third countries and international organisations.

21. The EDPS **welcomes** Recital 6 according to which the Proposal is without prejudice **to** the EUDPR. Moreover, the EDPS observes that Article 46(9) contains a reference to the EUDPR,

in particular when transferring EUCI containing personal data to third countries. The EDPS recalls that the EUDPR will apply to all processing of personal data by force of law. Therefore, no substantive provision is needed in the Proposal that establishes the application of the EUDPR in whole or in part. The EDPS acknowledges that international transfers of personal data are a complex subject requiring an additional reminder of the applicability of the EUDPR. In that case, the EDPS recommends explaining in a Recital, possibly Recital 6, that **all of the EUDPR provisions** will apply, **including** the rules on international transfers. Recital 6 can also be used to include any other general data protection recommendations made in this Opinion that do not aim at changing the substantive provisions.

22. The Proposal regulates EU classified information in a very extensive way. EUCI, as all the other information in the scope of the Proposal, can also contain personal data. As a result, they are subject to the applicable data protection rules, which apply also in this case and must be taken into account further to the EUCI provisions. We recommend recalling this explicitly in a recital, given the level of detail of the EUCI rules in the text.

3.2. Synergies with data protection and privacy

23. Article 33 of the EUDPR considers individuals and their rights and freedoms as assets to protect in the security risk management approach when personal data are processed.

24. The EDPS reiterates that **integrating the privacy and data protection assets and perspective in the traditional information security management process will ensure a holistic approach and enable synergies to the EUIs when managing information security and protecting the information they process without unnecessary multiplication of efforts.**

25. The use of technologies for improving information security should not unduly interfere with the rights and freedoms of individuals. The first step to avoid or mitigate those risks is to apply the requirements of data protection by design and by default laid down in Article 27 EUDPR, which will assist in integrating the appropriate safeguards such as **pseudonymisation** and **encryption,** or to implement principles such as **storage limitation and data minimization**, in the design and use of these technologies and systems.

26. The EDPS recalls that encryption, including end-to-end encryption are critical and irreplaceable technologies for effective data protection and privacy[2]. The EDPS welcomes Articles 11 and 17 of the Proposal that include encryption in the list of minimum measures for the protection of information at rest and in transit.

27. As the use of tools and services for electronic collaboration and communication have now become standard in our normal working modalities, it is very important to safeguard also the security of electronic communications. Beyond its benefits for privacy of electronic communications, **end-to-end encryption** can also protect information in the scope of this Proposal, while being exchanged when using electronic collaboration and communication tools. For this reason, the EDPS **strongly recommends including end-to-end**

[2] *"The Future of Encryption in the EU", Keynote Speech by Supervisor Wiewiórowski at the ISOC 2020 Webinar*

encryption in the list of minimum security measures of the Proposal, where applicable, and in particular when exchanging sensitive non-classified information.

28. Taking into account the accelerated use and adoption of cloud services by the EUIs, the EDPS **recommends adding in Article 5(3),** that **in the factors under consideration by the information security risk management process, also the threats stemming from access based on third countries jurisdiction (e.g. by their public authorities) shall be considered**. This is another example of possible synergies between information security and data protection. Tackling these risks for the one domain, the risks for the other domain are tackled for the same information systems that process personal data and information in the scope of the Proposal.

29. Finally, when dealing with information security incidents that may entail a personal data breach, or when dealing with a personal data breach that shows useful elements to tackle an information security incident, it is **strongly advisable to explain in a relevant recital** the benefits of having **an integrated incident handling process[3] that serves both information security and data protection obligations on data breach notifications**. In this way, the controller can save time, resources and have a much more efficient incident response for both domains.

30. To ensure such synergies between information security and data protection, **the EDPS strongly advises that the proposal provide for a specific obligation for EU officials responsible for information security to cooperate closely with the data protection officer designated in accordance with Article 43 EUDPR**, when dealing with activities such as applying data protection by design and by default to information security measures, selecting security measures that involve personal data, integrated risk management, integrated security incident handling.

4. Conclusions

31. In light of the above, the EDPS makes the following main recommendations:

- the EDPS strongly advises that the Proposal clearly defines the personal data processing activities that are allowed for the purposes of this Regulation, including: the purpose(s) of the processing; categories of personal data; categories of data subjects; definition of roles as applicable (controller, processor, joint controllers), retention periods, recipients in case of transmission to entities not subject to the EUDPR. The EDPS considers that these elements should be provided for explicitly in the Proposal, or at the very least, in a delegated act to be adopted subsequently by the Commission. The Proposal should provide for such a delegation.

[3] *See also the EDPS Guidelines on Personal Data Breach Notification*

- the EDPS recommends explaining in a Recital, that all of the EUDPR provisions will apply, including the rules on international transfers. Recital 6 can also be used to include any other general data protection recommendations made in this Opinion that do not aim at changing the substantive provisions.

- the EDPS strongly recommends including end-to-end encryption in the list of minimum security measures of the Proposal, where applicable, and in particular when exchanging sensitive non-classified information.

- the EDPS recommends adding in Article 5(3), that in the factors under consideration by the information security risk management process, also the threats stemming from access based on third countries jurisdiction (e.g. by their public authorities) shall be considered.

- the EDPS strongly advises to explain in a relevant recital the benefits of having an integrated information security risk management and an integrated incident handling process that serves both information security and data protection obligations on data breach notifications.

- the EDPS strongly advises that the proposal provides for a specific obligation for EU officials responsible for information security to cooperate closely with the data protection officer designated in accordance with Article 43 EUDPR, when dealing with activities such as applying data protection by design and by default to information security measures, selecting security measures that involve personal data, integrated risk management, integrated security incident handling.

Brussels, 17 May 2022

Wojciech Rafał WIEWIÓROWSKI

[e-signed]

Notes

[1] OJ L 295, 21.11.2018, p. 39.
[2] COM(2022) 119 final
[3] COM(2022) 122 final
[4] The EU's Cybersecurity Strategy for the Digital Decade | Shaping Europe's digital future (europa.eu) including a Joint Communication with the High Representative of the Union for Foreign Affairs and Security Policy (JOIN(2020)18)
[5] See chapter I. INTRODUCTION, page 4 of the Strategy.

[6] Joint Communication from the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy to the European Parliament and the Council, titled 'The EU's Cybersecurity Strategy for the Digital Decade'
[7] EDPS Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive
[8] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018).