EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

17 May 2022

Opinion 8/2022

on the Proposal for a Regulation laying down measures for a high common level of cybersecurity at 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 Commission Proposal for a Regulation laying down measures for a high common level of cybersecurity at 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.

Executive Summary

On 22 March 2022, the European Commission adopted a Proposal for a Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union ('the Proposal').

The EDPS welcomes the aim of the Proposal to improve the cybersecurity posture of the Union Institutions, bodies, offices and agencies ('EUIs'), and equally welcomes the new role of of the former 'Computer Emergency Response Team', now called 'Cybersecurity Centre' (CERT-EU), taking into account the amplified digitisation, the rapidly evolving cybersecurity threat landscape and the recent digitalisation shift due also to the Covid-19 pandemic.

The EDPS regrets that the Proposal does not align with the NIS Directive, and the NIS 2.0 Proposal so that consistent and homogeneous rules for Member States and the EUIs are achieved, contributing to the overall Union cybersecurity level. The EDPS recommends adding in the Proposal that its minimum security requirements should be at least equal or higher than the minimum security requirements of the entities of NIS and NIS 2.0 Proposal.

In order to comply with the Proposal, the EUIs, as well as CERT-EU will have to deploy certain cybersecurity processes and measures, which are bound to imply additional processing of personal data. 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, must clearly provide a legal ground for the processing of personal data by CERT-EU and the EUIs, including in particular the purposes of processing and the categories of personal data.

The EDPS stresses the importance of integrating the privacy and data protection perspective in the cybersecurity management, in order to achieve positive synergies between the Proposal and privacy and data protection legislation, and provides specific recommendations how such synergies can be achieved, including a specific obligation for EU officials responsible for cybersecurity to cooperate closely with the data protection officer designated in accordance with EUDPR.

The EDPS strongly advises that the Proposal provide for close cooperation between CERT-EU and EDPS, in activities like when addressing incidents resulting in personal data breaches, when addressing significant vulnerabilities, significant incidents or major attacks, that have the potential to result in personal data breaches, as well as when CERT-EU has indications that an infringement of the Proposal entails a personal data breach.

The EDPS also strongly recommends that the Proposal provide for the EDPS' participation in the 'Interinstitutional Cybersecurity Board' (IICB).

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. On 22 March 2022, the European Commission adopted a Proposal for a Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union[2] ('the Proposal').

2. On the same date, the European Commission adopted 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[3] ('the Infosec Proposal').

3. Both Proposals were 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 is to strengthen the Union's strategic autonomy in the field 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 for the EU institutions, bodies, offices and agencies (EUIs). According to its explanatory memorandum, the aim of the Proposal is twofold:

   - to address the increasingly hostile cyber threat landscape and the increased incidence of more sophisticated cyberattacks affecting the EU institutions, bodies and agencies, driving the need for increased investments to reach a high level of cyber maturity, and

   - to reinforce the EU Computer Emergency Response Team (CERT-EU) with an improved funding mechanism that is necessary to increase its ability to help EU institutions, bodies and agencies to apply the new cybersecurity rules, and improve their cyber resilience.

5. The EDPS observes that the subject matter of the Proposal at hand is interlinked with 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. In line with the Strategy, the Proposal aims at further improving the resilience of all Union institutions, bodies and agencies together with their incident response capacities. It is also in line with the Commission's priorities to make Europe fit for the digital age and to build a future-ready economy that works for the people. Moreover, it stresses that the security and resilience of the public administration is a cornerstone in the digital transformation of society as a whole.

7. According to the explanatory memorandum, the Proposal:

   - outlines measures with a view to ensuring a high common level of cybersecurity for the European Union institutions, bodies and agencies,

   - establishes the 'Interinstitutional Cybersecurity Board', which shall be responsible for monitoring the implementation of the proposed Regulation,

   - establishes the new role of the Computer Emergency Response Team for the EU institutions, agencies and bodies ('CERT-EU')[8], as the 'Cybersecurity Centre' for the Union institutions, bodies and agencies, in line with developments in the Member States and globally.

8. On 22 March 2022 the European Commission requested the EDPS to issue an Opinion on the Proposal pursuant to Article 42(1) of Regulation (EU) 2018/1725 ('EUDPR')[9]. 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 **observes** that while the NIS 2.0 Proposal applies to Member States public and private essential and important entities, the Proposal applies to the Union institutions, bodies, offices and agencies.

10. 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 affecting how EUIs, **the EUDPR applies and plays an equally important role**.

11. The EDPS **welcomes** the aim of the Proposal to improve the cybersecurity posture of the Union Institutions, bodies, offices and agencies through a self-standing and dedicated legal instrument, a Regulation. The EDPS equally welcomes the new role of CERT-EU, taking into account the amplified digitisation, the rapidly evolving cybersecurity threat landscape and the recent digitalisation shift due also to the Covid-19 pandemic.

12. The EDPS **recommends** adding in a separate recital, as per standard practice, that 'the European Data Protection Supervisor was consulted in accordance with Article 42 of

Regulation (EU) 2018/1725 of the European Parliament and of the Council and delivered an opinion on ... [EDPS Opinion date]'.

13. The EDPS recalls that in his NIS 2.0 Opinion, he recommended that the co-legislators create **an actionable link between the NIS 2.0 Proposal and legislative actions at the level of the EUIs, in order to achieve consistent and homogeneous rules** for Member States and the EUIs[1]. This is of the outmost importance to ensure a common high level of effectiveness and resilience, in particular in the functioning of the whole national and EU public administration, due to the increasing role that the latter plays based on the Treaties.

14. The EDPS **regrets** that the Proposal does not explain sufficiently in the explanatory memorandum nor in the relevant recitals (4) and (5), in what way it aligns with the NIS Directive, and the NIS 2.0 Proposal and how it contributes to the overall Union cybersecurity level through the link with the NIS Directive and the NIS 2.0 Proposal.

15. In view of the essential and important role of the EUIs for the functioning of the Union, the **EDPS submits that the minimum security requirements of the Proposal should be at least equal or higher than the minimum security requirements of the entities falling within the scope of the NIS and the NIS 2.0 Proposal**, in line with Article 3 of the NIS 2.0 Proposal ('Minimum harmonisation)'. For this reason, the EDPS **recommends** adding in a recital that **the Proposal builds on the NIS 2.0 Proposal**, and further explain the link between the Proposal and the NIS Directive as well as the NIS 2.0 Proposal in recitals (4) and (5). In addition, the EDPS recommends the inclusion of wording in the main text as follows: "The minimum security requirements should be at least equal or higher than the minimum security requirements of the entities under the scope of NIS 2.0 Proposal".

16. In particular, the EDPS **observes** that the Proposal **does not fully align with the NIS 2.0 Proposal** in the following points:

    - Article 5(1) of the NIS 2.0 Proposal requires that 'Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity'. The EDPS suggest that the Proposal should include the promotion of an adoption of **a common cybersecurity strategy of all EUIs**, reflecting the requirements set by Article 5 of the NIS 2.0 Proposal.

    - There seems to be some misalignment between the minimum cybersecurity measures[2] of the Proposal and the minimum measures listed in Article 18 of the NIS 2.0 Proposal. In this context the **EDPS regrets that the Proposal does not contain an explicit reference to the use of cryptography and encryption (and end-to-end encryption)**, which are essential technologies to protect all information at rest and in transit and to also protect electronic communications.

    - Contrary to the NIS 2.0 Proposal[3], the Proposal does not include provisions for the **collaboration** between the CERT-EU and the Interinstitutional Cybersecurity

[1] *paragraph 25 EDPS NIS 2.0 Opinion*
[2] *Annex I and II of the Proposal*
[3] *Recitals 58, 77, Articles 28, 32 NIS 2.0 Proposal*

Board **with the European Data Protection Supervisor**. **The EDPS strongly recommends that such collaboration be institutionalised through a provision in the Proposal,** to allow EDPS to monitor cybersecurity developments that might have implications for personal data security of the EUIs and to monitor compliance of cybersecurity measures. This point is further elaborated in section 3.3.

3. Specific comments

3.1. Scope of the Proposal and relationship with data protection and privacy legislation

17. The EDPS notes that the entities subject to the Proposal are the same entities subject to the EUDPR, which are the 'Union institutions, bodies, offices and agencies'. While this term is found in the title of the Proposal, the rest of the text uses the term 'Union institutions, bodies and agencies'. The EDPS **recommends** using the term **'Union institutions, bodies, offices and agencies'** consistently across the Proposal in order to avoid misunderstandings.

18. The EDPS reiterates[4] that Article 4(1)(f) of EUDPR establishes **security as one of the main principles relating to the processing of personal data**. Article 33 EUDPR further defines this obligation, 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**.

19. The EDPS observes, on the one hand, that the Proposal uses the same definition of cybersecurity as the NIS 2.0 Proposal: "*the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats*", where cyber threat means "*any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons*"[5]. It is clear from this definition that the objective of cybersecurity has a different focus than that of the EUDPR security provisions, as in Articles 4(1)(f) and 33 ('personal data security'). While cybersecurity aims to protect '*network and information systems, the users of such systems, and other persons*' from cyber threats, personal data security has a different specific aim: to protect personal data from **any threat** (including the cyber threats) that can lead to adverse consequences for the **rights and freedoms of individuals**. This is why the EDPS stated in paragraph 10 of the NIS 2.0 Opinion that **by improving cybersecurity, personal data security as well as the privacy of electronic communications are also improved**. That comment remains valid in the present context.

20. On the other hand, the EDPS reiterates[6] that the pursuance of the objectives of cybersecurity may lead to deploying measures that interfere with the rights to data

---

[4] Paragraph 10 EDPS NIS 2.0 Opinion
[5] 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, COM (2020) 823 final
[6] Paragraph 11 EDPS NIS 2.0 Opinion

protection and privacy of individuals. This means ensuring that **any potential limitation of the right to the protection of personal data and privacy must meet the requirements of Article 52(1) of EU Charter of Fundamental Rights**, in particular being provided for by law, necessary and proportionate, and respecting the essence of the right.

21. In order to comply with the Proposal, the EUIs, as well as CERT-EU, will have to deploy certain cybersecurity processes and measures, which are bound to **imply additional processing of personal data and of electronic communications data, including traffic data**. Such measures would be adopted in relation to the cybersecurity risk management, or because they belong to the list of minimum cybersecurity measures[7] such as access control, communications security, incident management and multi-factor authentication.

22. In this context, the EDPS observes that the organisations acting as controllers and processors do not always realise that the data processed in cybersecurity systems and services may constitute personal data (e.g. IP addresses, device identifiers, network log files, access control log files, etc.). This exacerbates risks of non-compliance with data protection and privacy legislation, as for example the principles of lawfulness of processing, purpose limitation, data minimisation, storage limitation, and obligations for lawful data transfers. The EDPS therefore considers that it should be clarified, for the avoidance of any doubt, in a new recital that "**All cybersecurity systems and services involved in the prevention, detection, and response to cyber threats should be compliant with the current data protection and privacy framework, and should take relevant technical and organisational safeguards to ensure this compliance in an accountable way**".

23. The EDPS **welcomes** Recital 22 according to which all personal data processed under this Proposal should be processed in accordance with data protection legislation, including Regulation (EU) 2018/1725. Moreover, the EDPS recommends adding in that recital that "**the Proposal does not seek to affect the application of existing EU laws governing the processing of personal data, including the tasks and powers of the EDPS".**

24. The EDPS **observes** that Article 18(3) requires that the processing of personal data carried out under this Proposal should be subject to the EUDPR, giving the impression that this is only required in the context of information handling by CERT-EU and the EUIs. To avoid possible misinterpretations, the EDPS **recommends** moving the provision of Article 18(3) to recital 22 in order to cover **any personal data processing** performed by CERT-EU and the EUIs in the context of the Proposal, including but not limited to: the cybersecurity services provided by CERT-EU pursuant to Article 12, the information sharing pursuant to Article 18, sharing obligations pursuant to Article 19, measures involving personal data in relation to the cybersecurity risk management of the Article 4, and the list of minimum cybersecurity measures[8] of the Proposal, that involve personal data processing.

25. 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 to effectively protect their personal data

[7] *Annex I & II of the Proposal*
[8] *Annex I & II of the Proposal*

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).

26. To achieve legal certainty and foreseeability, and to ensure compliance with the EUDPR, in particular with Article 5(1) (a) and (2), the EDPS **strongly advises that the Proposal must clearly provide for a legal ground for the processing of personal data by CERT-EU and the EUIs**, including in particular the purposes of processing and the categories of personal data. In addition, the following elements should be explicitly laid down: (a) Identification of the controller(s), processors or joint controllers, as applicable; (b) Categories of data subjects; (c) Retention periods or at least criteria to determine such periods. 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.

3.2. Synergies with data protection and privacy

27. The EDPS reiterates[9] that **integrating the privacy and data protection perspective in the traditional cybersecurity management is capable of ensuring a holistic approach and therefore enabling important synergies to the EUIs when managing cybersecurity and protecting the information they process without unnecessary multiplication of efforts**.

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

29. The EDPS wishes to reiterate **that encryption, including end-to-end encryption, is a critical and irreplaceable technology for effective data protection and privacy**. While encryption is **very effective in dealing with cybersecurity risks**, it does this **without involving additional personal data processing**.

30. Considering the accelerated use and adoption of cloud services by the EUIs, the EDPS **strongly recommends including 'encryption at rest', 'encryption in transit' as well as 'end-to-end encryption' in the list of minimum cybersecurity measures of the Annex II of the Proposal**.

31. As already underlined on previous occasions, the management of risks for the rights and freedoms of individuals, when their personal data are processed, is an obligation under Article 33 of the EUDPR. Whereas the cybersecurity risk management measures of Article

[9] *Paragraph 16 EDPS NIS 2.0 Opinion*

4 of the Proposal aim at protecting network and information systems (and the data therein), Article 33 EUDPR aims at addressing risks for individuals (not necessarily belonging to the same organisation) and their rights, by protecting their personal data. There is a difference in the assets to protect among the two activities, which might lead to different conclusions in certain circumstances. At the same time, the cybersecurity risk management process can contribute to the assessment of the data protection impact of weaknesses in the security of personal data. For this reason, the EDPS recommends **integrating the privacy and data protection considerations into cybersecurity risk management** to ensure a holistic approach and enable synergies without unnecessary multiplication of efforts.

32. Finally, concerning the cybersecurity incidents that may entail a personal data breach, or a personal data breach that shows indications of a cybersecurity incident, it is **strongly advisable to explain in a relevant recital** the benefits of having **an integrated incident handling process[10] that serves both cybersecurity 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.

33. To ensure such synergies between cybersecurity and data protection, **the EDPS strongly advises that the proposal provides for a specific obligation for the Local Cybersecurity Officer defined in article 4(5) to cooperate with the data protection officer designated in accordance with Article 43 EUDPR,** when dealing with overlapping activities like applying data protection by design and by default to cybersecurity measures, selecting cybersecurity measures that involve personal data, integrated risk management, and integrated security incident handling.

3.3. The role of the EDPS

34. The EDPS observes that the Proposal **does not make any reference to the EDPS**, despite the important interplay between cybersecurity and data protection and privacy, as described above.

35. The EDPS needs to be involved in both of these aspects, on the one hand to **monitor cybersecurity developments** that can have implications for data protection and privacy, and on the other hand to **monitor and ensure compliance of cybersecurity measures** that involve personal data.

36. In contrast to the Proposal, Article 28 and Article 32 of the NIS 2.0 Proposal provide specific provisions for **collaboration between cybersecurity and data protection authorities**.

37. **To ensure consistency between Member States and the EUIs, and in** line with Article 28 of the NIS 2.0 Proposal, the EDPS **strongly advises** adding a provision in Article 12 'CERT-EU mission and tasks' of the Proposal that '**CERT-EU shall work in close cooperation with the EDPS, when addressing incidents resulting in personal data breaches or in breach of confidentiality of electronic communications**'.

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

38. In the same spirit, the EDPS considers that **CERT-EU shall inform the EDPS when addressing significant vulnerabilities, significant incidents or major attacks that have the potential to result in personal data breaches and/or in the breach of confidentiality of electronic communications**. A corresponding obligation should be added in Article 12 'CERT-EU mission and tasks' of the Proposal.

39. Moreover, the EDPS **recommends** providing in Article 12 that that the EDPS shall be involved in the CERT-EU cybersecurity awareness raising activities of the EUIs, in order to cover the interplay between personal data breach and cybersecurity incidents.

40. Moreover, in line with the Article 32 of the NIS 2.0 Proposal the EDPS **recommends** adding a provision in Article 12 'CERT-EU mission and tasks' of the Proposal that would specify that **CERT-EU shall inform without undue delay the EDPS when it has indications that an infringement by the EUIs of the obligations laid down in the Proposal entails a personal data breach**.

41. The EDPS is not included in the list of the permanent participants of the 'Interinstitutional Cybersecurity Board' ('IICB') defined in the Article 9 of the Proposal. As highlighted above, the security of personal data processing, and therefore also cybersecurity, is one of the cornerstones for data protection. In addition the EDPS is mandated by Article 57(1)(h) EUDPR to monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies. This includes cybersecurity developments, so as to be able to issue specific Data Protection guidance related to cybersecurity, the EDPS **strongly advises that the European Data Protection Supervisor is added in Article 9(3) as a permanent participant in the IICB with one representative.**

3.4. Information sharing and CERT-EU services

42. According to Article 12, CERT-EU provides certain cybersecurity services in which it acts as the processor of cybersecurity information that includes personal data. It must be ensured from the outset that such data processing activities are in full compliance with EUDPR and GDPR.

43. Article 16(2) states that CERT-EU 'may exchange incident-specific information with national counterparts in the Member States to facilitate detection of similar cyber threats or incidents without the consent of the affected constituent', and that 'CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the consent of the affected constituent'.

44. Article 19 allows CERT-EU to request and obtain information from the information systems inventories of the EUIs, in order to coordinate vulnerability management and incident response. Furthermore, it obliges EUIs, upon request of the CERT-EU and without undue delay, to provide it with digital information created by the use of electronic devices involved in their respective incidents.

45. The EDPS considers that there is high probability that the incident-specific information as well as the digital information created by the use of electronic devices involved in the incident will contain personal data. Thus, the EDPS advises clarifying the categories of

personal data to be processed in these exchanges, the purpose or purposes of processing, the recipients of data and the possible data transmission, to achieve the necessary legal clarity, legal certainty and foreseeability. 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.

46. Furthermore, the EDPS notes the use of the expression 'consent' which the legislator has defined already in Article 3 (15) EUDPR. Given that the Proposal in the context of Article 16(2) refers to EUIBAs ('constituents') rather than data subjects, the EDPS suggest to use the term 'authorization' instead of 'consent'.

47. Article 17(3) states that 'CERT-EU may, with the consent of the constituent affected by an incident, provide information related to the incident to [non-Member State counterparts] partners that can contribute to its analysis'. The EDPS recalls that such international data transfers should be in full compliance with the Chapter V of the EUDPR. Consequently, the EDPS recommends including in the Proposal a recital with reference to the aforementioned chapter.

4. Conclusions

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

- the EDPS recommends adding in a recital that the Proposal builds on the NIS 2.0 Proposal, and further explain the link between the Proposal and the NIS Directive as well as the NIS 2.0 Proposal in the recitals (4) and (5). In addition, the EDPS recommends the inclusion of wording in the main text as follows: "The minimum security requirements should be at least equal or higher than the minimum security requirements of the entities of NIS and NIS 2.0 Proposal".

- the EDPS strongly advises that the Proposal must clearly provide a legal ground for the processing of personal data by CERT-EU and the EUIs, including in particular the purposes of processing and the categories of personal data. In addition, the following elements should be explicitly laid down: (a) Identification of the controller(s), processors or joint controllers, as applicable; (b) Categories of data subjects; (c) Retention periods or at least criteria to determine such periods. 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 strongly recommends including 'encryption at rest', 'encryption in transit' as well as 'end-to-end encryption' in the list of minimum cybersecurity measures of the Annex II of the Proposal.

- the EDPS strongly advises that the proposal provides for a specific obligation for the Local Cybersecurity Officer defined in article 4(5) to cooperate with the data protection officer designated in accordance with Article 43 EUDPR, when dealing with overlapping activities like applying data protection by design and by default to

cybersecurity measures, selecting cybersecurity measures that involve personal data, integrated risk management, and integrated security incident handling.

- the EDPS strongly advises adding a provision in Article 12 'CERT-EU mission and tasks' of the Proposal that 'CERT-EU shall work in close cooperation with the EDPS, when addressing incidents resulting in personal data breaches or in breach of confidentiality of electronic communications'.

- the EDPS recommends adding an obligation for CERT-EU to inform the EDPS when addressing significant vulnerabilities, significant incidents or major attacks that have the potential to result in personal data breaches and/or in the breach of confidentiality of electronic communications.

- the EDPS recommends providing in Article 12 that that the EDPS shall be involved in the CERT-EU cybersecurity awareness raising activities of the EUIs, in order to cover the interplay between personal data breach and cybersecurity incidents.

- the EDPS recommends adding a provision in Article 12 'CERT-EU mission and tasks' of the Proposal that would specify that CERT-EU shall inform without undue delay the EDPS when it has indications that an infringement by the EUIs of the obligations laid down in the Proposal entails a personal data breach.

- the EDPS strongly advises that the European Data Protection Supervisor is added in Article 9(3) as a permanent participant in the IICB with one representative.

Brussels, 17 May 2022

Wojciech Rafał WIEWIÓROWSKI

[e-signed]

Notes

[1] OJ L 295, 21.11.2018, p. 39.
[2] COM(2022) 122 final
[3] COM(2022) 119 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 of the Strategy, page 4.
[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] The current role of CERT-EU stems from the Interinstitutional Agreement 2018/C 12/01
[9] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018).