EDPS Formal comments on the draft Commission Implementing Regulation laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

Having regard to Regulation (EU) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals 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')[1], and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING FORMAL COMMENTS:

1. Introduction and background

1. On 29 July 2024, the European Commission consulted the EDPS on the draft Commission Implementing Regulation laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers ('the draft Implementing Regulation'). The draft Implementing Regulation is accompanied by an Annex, laying down the technical and methodological requirements referred to in Article 2 of the draft Implementing Regulation.

[1] OJ L 295, 21.11.2018, p. 39.

2. The draft Implementing Regulation is adopted pursuant to Article 21(5) and Article 23(11) of Directive (EU) 2022/2555 (the NIS 2 Directive)[2].

3. The EDPS previously issued Opinion 5/2021 on the NIS 2 Directive[3].

4. The objective of the draft Implementing Regulation is to lay down the technical and the methodological requirements of the measures referred to in Article 21(2) of the NIS 2 Directive and to further specify the cases in which an incident should be considered significant as referred to in Article 23(3) of the NIS 2 Directive[4].

5. The present formal comments of the EDPS are issued in response to a consultation by the European Commission pursuant to Article 42(1) of EUDPR.

6. These formal comments do not preclude any additional comments by the EDPS in the future, in particular if further issues are identified or new information becomes available, for example as a result of the adoption of other related implementing or delegated acts[5].

7. Furthermore, these formal comments are without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Article 58 of the EUDPR and are limited to the provisions of the draft Implementing Regulation that are relevant from a data protection perspective.

2. Comments

8. The EDPS notes that the draft Implementing Regulation would imply the processing of personal data by the 'relevant entities' referred to under Article 1 (namely, DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers).

9. Indeed, having regard to the specification of the cases in which an incident must be considered as significant as referred to in Article 23(3) of the NIS 2 Directive and specified in the draft Implementing Regulation[6], the EDPS notes that the draft Implementing Regulation refers to activities that may entail the processing of

[2] 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) (Text with EEA relevance), OJ L 333, 27.12.2022, p. 80–152.

[3] Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive, issued on 11 March 2021.

[4] Recital 1 of the draft Implementing Regulation.

[5] In case of other implementing or delegated acts with an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data, the EDPS would like to remind that he needs to be consulted on those acts as well. The same applies in case of future amendments that would introduce new or modify existing provisions that directly or indirectly concern the processing of personal data.

[6] Articles 3-14 of the draft Implementing Regulation.

personal data. Beyond the processing of names of staff when assigning roles and responsibilities in the context of the security governance, examples of processing that may involve personal data are: IP addresses in log files to be processed in the context of the logging and monitoring process; or device identifiers processed in the context of the configuration management process.

10. Moreover, having regard to the technical and methodological requirements of the measures referred to in Article 21(2) of the NIS 2 Directive and set out in the Annex to the draft Implementing Regulation, the EDPS notes that the activities referred to in this document may also entail the processing of personal data. Examples of such processing are: processing of names of staff in the context of the risk management process; processing of IP addresses and of device identifiers in the context of the incident management process; processing of contact details of staff in the context of awareness campaigns; processing of personal data in the context of the business continuity management and of the supplier management; processing of personal data for security testing; processing of personal data in the context of reporting activities.

11. Against this background, the EDPS recalls the applicability of the Union's legislation for the protection of personal data to the processing of personal data falling under the scope of the draft Implementing Regulation. Therefore, the EDPS recommends adding a recital in the draft Implementing Regulation recalling the applicability of the EU data protection laws, namely Regulation 2016/679 ('GDPR')[7] and Directive 2002/58/EC (ePrivacy Directive)[8].

12. More specifically, having regard to the technical and methodological requirements of the measures referred to in Article 21(2) of the NIS 2 Directive and set out in the Annex to the draft Implementing Regulation[9] and in particular to the rules for event assessment and classification (3.4.), as well as for incident response (3.5.), the EDPS notes that significant security incidents very often also constitute personal data breaches in the meaning of Article 4(12) of the GDPR. The entities involved in the assessment of a security incident and of a personal data breach are also usually the same. Therefore, synergic attention to both aspects is important both in the preparation phase (avoiding and/or minimising the possible impact of the incident) and in the security incident management phase. Against this background, the EDPS recommends adding to the Annex the following rules:

    a. inserting, after the rule 3.4.1., the rule: "*As preparation for security incidents that are also personal data breaches pursuant to Article 4(12) of the GDPR, the*

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47.

[9] See Article 2 of the draft Implementing Regulation.

relevant entities shall establish rules on how to handle these personal data breaches in conjunction with the assessment of the security incident";

b. inserting, after the rule 3.4.2.(b), the rule: "*carry out an assessment of whether the event constitutes a personal data breach pursuant to Article 4(12) of the GDPR.*";

c. amending the rule 3.5.1., adding after the first sentence the wording: "*If the security event represents a personal data breach, the entity shall follow the policy laid down in accordance with Article 33 and Article 34 of the GDPR.*"

Brussels,