EDPS Formal comments on the draft Commission Implementing Regulation on laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat

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 3 July 2024, the European Commission consulted the EDPS on the draft Commission Implementing Regulation on laying down implementing technical standards for the application of Regulation (EU) 2022/2554 ('DORA Regulation')[2] with regard to the standard forms, templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat ('the draft Implementing Regulation').
2. The objective of the draft Implementing Regulation is to develop common draft implementing technical standards in order to establish the standard forms, templates and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat.
3. The draft Implementing Regulation is adopted pursuant to Article 20(b) of the DORA Regulation.
4. The EDPS previously issued Opinion 7/2021 on the DORA Regulation[3].

[1] OJ L 295, 21.11.2018, p. 39.
[2] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance), OJ L 333, 27.12.2022, p. 1–79.
[3] EDPS Opinion 7/2021 on the Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) 1060/2009, (EU) 648/2012, (EU) 600/2014 and (EU) 909/2014, issued on 10 May 2021.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

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[4].

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 Annex I accompanying the draft Implementing Regulation includes, among the information about the financial entity, the name of the entity submitting the report and contact details[5]. More significantly, field 3.35 titled "Indicators of Compromise (IoC)" in Annex I also encompasses a wide range of data which is likely to constitute personal data such as IP addresses, log files and email message data[6].

9. Against this background, the EDPS recalls the applicability of the EU data protection legal framework, in particular Regulation 2016/679 (GDPR)[7], when processing personal data within the scope of the draft Implementing Regulation. The EDPS recommends adding a recital recalling the applicability of the EU data protection legal framework and principles, such as data minimisation and storage limitation, for any activities under the draft Implementing Regulation that involve personal data processing. Moreover, if personal data is transferred to third countries, notably when financial entities outsource their reporting obligations as per Article 6 of the draft Implementing Regulation, the EDPS recalls the need to also comply with the additional requirements laid down in Chapter V of the GDPR.

[4] 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.

[5] For the sake of completeness, the EDPS recalls that data concerning legal persons may, in some instances, be considered as personal data, as clarified by the CJEU (See judgment of 9 November 2010, *Volker und Markus Schecke Gbr v. Land Hessen, and Eifert v. Land Hessen and Bundesanstalt für Landwirtschaft und Ernahrung*, Joined cases C-92/09 and C-93/09, EU:C:2010:662, paragraph 53). In these cases, the determining factor is whether the information 'relates to' an 'identifiable' natural person.

[6] See also EDPS Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive, paragraph 30.

[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.

10. Finally, the EDPS notes the absence of the reference to this consultation in a recital of the draft Implementing Regulation. Hence, the EDPS recommends inserting such a reference in a recital of the draft Implementing Regulation.

Brussels,