EDPS Formal comments on the draft Commission Delegated Regulation supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria used for identifying financial entities required to perform threat-led penetration testing, the requirements and standards governing the use of internal testers, the requirements in relation to scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition

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 Delegated Regulation supplementing Regulation (EU) 2022/2554 ('DORA Regulation')[2] with regard to regulatory technical standards specifying the criteria used for identifying financial entities required to perform threat-led penetration testing ('TLPT'), the requirements and standards governing the use of internal testers, the requirements in relation to scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition ('the draft Delegated Regulation').

[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.

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

2. The draft Delegated Regulation is adopted pursuant to Article 26(11) of the DORA Regulation.

3. The EDPS previously issued Opinion 7/2021 on the DORA Regulation[3].

4. The objective of the draft Delegated Regulation is to approve the draft regulatory technical standards developed by the European Supervisory Authorities ('ESAs') in agreement with the European Central Bank ('ECB') to specify: the criteria to identify financial entities required to perform TLPT; the requirements regarding test scope, testing methodology and results of TLPT; the requirements and standards governing the use of internal testers; and the rules on supervisory and other cooperation needed for the implementation of TLPT and for mutual recognition of testing.

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 Delegated Regulation that are relevant from a data protection perspective.

2. Comments

8. The EDPS notes that the draft Delegated Regulation would imply the sharing of personal data by competent TLPT authorities with financial entities obliged to perform TLPT, namely the contact details of the members of the TLPT Cyber Team ('TCT')[5]. Conversely, the tested financial entity would be required to communicate the contact details of the control team lead during the TLPT preparation phase[6]. The draft Delegated Regulation would also imply the processing, by the tested financial entity, of personal data of members of the control team, including of staff of third-party service providers and other parties[7]. Tested financial entities would also be

[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.
[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] Article 3(4) and 8(1) of the draft Delegated Regulation.
[6] Article 8(1)(b) of the draft Delegated Regulation.
[7] Article 1(1) and 4(1) of the draft Delegated Regulation.

required to verify the professional knowledge, skills, experience, and potential conflicts of interest of the staff of the threat intelligence provider and the red team, including by keeping detailed curriculum vitae[8]. The remediation plan that tested financial entities would be required to share with the competent TLPT authority would also include, for each finding occurred in the framework of the TLPT, the financial entity's staff or functions responsible for the implementation of the proposed remediation measures or improvements[9].

9. Annex I accompanying the draft Delegated Regulation outlines the content of the TLPT project charter, including the name and contact details of the person responsible for the project plan, i.e. the Control Team Lead.

10. Annex III foresees that the targeted threat intelligence report shall include information on various elements, including an assessment of concrete actionable intelligence on the tested financial entity - such as information posted by employees on social media - and threat profiles of malicious actors (including specific individuals) that may target the financial entity.

11. In addition, the EDPS points out that it is very likely that during threat-led penetration testing exercises a wide range of data will be processed that is likely to qualify as personal data such as IP addresses, log files and email message data[10].

12. Against this background, the EDPS recalls the applicability of the EU data protection legal framework, in particular Regulation 2016/679 ('GDPR')[11], when processing personal data within the scope of the draft Delegated 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 Delegated Regulation that involve personal data processing.

13. Furthermore, the EDPS recommends ensuring that the draft Delegated Regulation provides for sharing of personal data only where it is necessary to achieve the objectives of each phase of the TLPT. For example, draft Delegated Regulation provides that both the red team and blue team test reports, as well the report summarizing the relevant findings of the TLPT, may be expunged of 'sensitive information'[12] *upon request*. In accordance with the principle of data minimisation,

[8] Article 5(2)(e), (2)(f) and (3) of the draft Delegated Regulation.
[9] Article 12(2)(d) of the draft Delegated Regulation.
[10] See also EDPS Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive, paragraph 30.
[11] 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.
[12] Article 1(13) of the draft Delegated Regulation defines 'sensitive information' as "*information that can readily be leveraged to carry out attacks against the ICT systems of the financial entity, intellectual property, confidential business data and/or personal data that can directly or indirectly harm the financial entity and its ecosystem would it fall in the hands of malicious actors.*" (emphasis added)

personal data should only be disclosed where necessary and otherwise removed or anonymized before the test reports are shared.

14. The EDPS welcomes that the draft Delegated Regulation mentions the need-to-know principle with regards to the information pertaining to any planned or ongoing TLPT[13]. However, the implementation of the need-to-know principle can be composed of several components, which depend on the context of access to information. Moreover, appropriate measures to limit access to information should not only be organisational and procedural but also technical in nature. Therefore, the EDPS recommends amending Article 4 to also make reference to appropriate technical measures. Specific examples of appropriate technical measures may include access control, strong encryption and logging and monitoring of access to the collected data.
15. Article 10 describes the testing phase for the red team. During this phase, it is likely that the red team will collect security-related information and personal data. However, Annex V, which specifies the content of the red team test report, does not include logs of the red team's activities. Logs are important as they give the exact actions that have been taken in order to achieve the TLPT's objectives. Therefore, the EDPS recommends adding log entries to the list of items under Annex V of the draft Delegated Regulation that would be included in the red team's report, wherever possible, to allow for a better understanding of the specific actions that are carried out by the red team.
16. Finally, the EDPS notes the absence of the reference to this consultation in a recital of the draft Delegated Regulation. Hence, the EDPS recommends inserting such a reference in a recital of the draft Delegated Regulation.

Brussels, 19 August 2024

[13] Article 4(2)(a) of the draft Delegated Regulation.