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 to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554

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 to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions ('the draft Delegated Regulation').
2. The draft Delegated Regulation is adopted pursuant to Article 30(5) 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') to specify further the elements referred to in Article 30(2)(a) of the DORA 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.
[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

which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions.

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 oblige financial entities to assess and decide, before entering into an arrangement with an ICT third party service provider, whether an ICT service supporting critical or important functions or material parts thereof may be subcontracted by the ICT third party service provider, taking into account a list of elements listed in Article 1 of the draft Delegated Regulation. Among those elements, the financial entity must consider:

    a. the type of ICT services;

    b. the location of the ICT subcontractor or its parent company (in particular, whether they are located in a third country), also considering the location where the ICT services are actually provided from and the location where the data is actually processed and stored;

    c. the length of the chain of subcontractors; and

    d. the nature of data shared with the ICT subcontractors.

9. Article 3 of the draft Delegated Regulation would also oblige financial entities to assess, inter alia:

    a. the due diligence processes implemented by the ICT third-party service provider;

[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.

b. that the latter is able to identify, notify and inform the financial entity of any subcontractors in the chain of subcontracting;

c. that the ICT third-party service provider ensures that the contractual arrangements with its subcontractors allow the financial entity to comply with its own obligations stemming from the DORA Regulation and other applicable requirements, and grant the financial entity and competent and resolution authorities the same contractual rights of access, inspection and audit along the chain of subcontractors;

d. that the ICT third-party service provider itself has adequate abilities, expertise, financial, human and technical resources, applies appropriate information security standards, and has an appropriate organisational structure, to monitor its subcontractors; and

e. the risks associated with the location of the potential subcontractors.

10. The EDPS recalls that when financial entities instruct ICT third-party service providers to process personal data on their behalf, they must comply with their obligations as controllers and processors (respectively) under Regulation 2016/679 ('GDPR')[5]. Among these obligations, financial entities are required to only engage ICT third-party service providers providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing of personal data meets the requirements of the GDPR and ensure the protection of the rights of data subjects, and ICT third-party service providers can only engage a subcontractor for the processing of such personal data with prior specific or general written authorisation of the financial entity[6]. Such engagement is only possible where the ICT third-party service provider contractually imposes on the subcontractor the same data protection obligations as set out in the contract between the financial entity and the ICT third-party service provider. The latter remains fully liable to the former for any failure on the part of the subcontractor to fulfil its obligations[7].

11. The EDPS further recalls that transferring personal data outside of the territory of the European Economic Area is subject to restrictions under Chapter V of the GDPR, and that processors (in this case, ICT third-party service providers) and their subcontractors may only transfer personal data to a third country on the documented instructions of the controller (in this case, the financial entity)[8].

12. Against this background, the EDPS recommends adding a recital recalling the applicability of the EU data protection legal framework and principles to any

[5] 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.
[6] Article 28(1) and (2) GDPR.
[7] Article 28(4) GDPR.
[8] Article 28(3)(a) GDPR.

processing of personal data within the scope of the draft Delegated Regulation, in particular Article 28 and Chapter V GDPR.

13. 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