Question ID

2025_7388

Legal act

Regulation (EU) No 2022/2554 (DORA Reg)

Topic

Register of information (DORA)

Article

Article 28

Paragraph

1-3

COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations

Not applicable

Article/Paragraph

N/A

Type of submitter

Competent authority

Subject matter

Obligation to maintain a register of information for FEs exempt under article 16

Question

Are financial entities, which according to article 16(1) in DORA are excluded from application of Articles 5 to 15, also are excluded from application of article 28 of DORA?

Background on the question

We have found that we need a clarification on this as it is unclear to us whether an FE mentioned in article 16(1) o DORA should also be relieved of the obligation to maintain and update a register of information.

Article 16(1) mentions only exemption from articles 5-15.

However, the wording of article 28 could suggest that such entities are exempt from application of all of article 28, including the obligation to maintain an RoI. For example:

Article 28(1): “Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework as referred to in Article 6(1) (…)”. The structure of this sentence suggests that only entities manage ICT risk within the framework referred to in article 6(1) are obligated to apply article 28(1).

Article 28(3) begins with the same structure as article 28(3), albeit only mentioning the ICT risk management framework without specific mention of article 6(1), so the conclusion would be the same as for article 28(1).

Submission date

26/03/2025

Final publishing date

08/08/2025

Final answer

DORA Recital 21 specifies that in order to maintain full control over ICT risk, financial entities need to have comprehensive capabilities to enable a strong and effective ICT risk management, as well as specific mechanisms and policies for handling all ICT-related incidents and for reporting major ICT-related incidents. It also states that the digital operational resilience baseline for financial entities should be increased while also allowing for a proportionate application of requirements for certain financial entities, particularly microenterprises, as well as financial entities subject to a simplified ICT risk management framework.

In addition, DORA Recital 43 states that financial entities which qualify as microenterprises or are subject to the simplified ICT risk management framework under this Regulation should not be required to establish a role to monitor their arrangements concluded with ICT third-party service providers on the use of ICT services.

However, DORA Article 28(3) establishes the obligation to maintain and update a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers with no exception.

All financial entities that are subject to DORA are required to maintain a register of information. Additionally, they must apply third-party risk management framework that is proportional to the risks associated with their activities. This means that the extent and complexity of the risk management measures should match the level of risk involved. For example, smaller financial entities, which typically use fewer ICT services, would have simpler risk management requirements compared to larger entities. The principle of proportionality is already embedded in the requirements of the register of information, ensuring that the measures are appropriate for the size and complexity of the entity's operations.

Status

Final Q&A

Answer prepared by

Answer prepared by the Joint ESAs Q&A
