Question ID

2025_7613

Legal act

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

Topic

ICT-related incidents (management / classification / reporting)

Article

3

Subparagraph

No. 8

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

Regulation (EU) 2024/1772 - RTS on the classification of ICT-related incidents and cyber threats

Article/Paragraph

Articles 6, 8, 9

Name of institution / submitter

BaFin

Country of incorporation / residence

Germany

Type of submitter

Competent authority

Subject matter

Classification of phishing-attacks as a reportable major ICT-related incident

Question

Can individual phishing incidents that target the customers of a financial entity in their “private sphere” be subsumed under “compromises the security of the network and information systems”

pursuant to Article 3 No. 8 of Regulation (EU) 2022/2554 and can they therefore constitute a major ICT-related incident that must be reported pursuant to Article 19 (1) of Regulation (EU) 2022/2554?

Background on the question

The question concerns the categorization of a phishing incident as an ICT-related incident in situations where the phishing incident is directed against the customers of financial entities in their “private sphere” – e.g. the customer clicks on a phishing link in his private email inbox or the customer fills in his credentials on a “phishing-homepage” of the financial entity.

In order for individual phishing incidents targeting the privacy of a financial entity's customer to be considered as ICT-related incidents, they would first of all have to fulfil the definition of a major ICT-related incident (Article 3 No 8 and 10 of Regulation (EU) 2022/2554). Therefore, these incidents would have to be classified as “compromis[ing] the security of the network and information systems” (cf. Article 3 No. 8 of Regulation (EU) 2022/2554). However, the wording of Art. 3 No. 8 of Regulation (EU) 2022/2554 leaves open whether this impairment must be directed against the financial entities itself or whether customers of the financial entity, may also be affected.

The further criteria for assessing a major ICT-related incident from Delegated Regulation (EU) 2024/1772 do not currently provide clarity, as the relationship between Article 6 of Delegated Regulation (EU) 2024/1772 and the definition in Article 3 of Regulation 2022/2554 is unclear.

Among the national supervisory authorities, the consideration of these phishing incidents is handled differently. The question submitted is therefore intended to ensure legal certainty in the interpretation of the aforementioned standard as well as the uniformity and comparability of reports of major ICT-related incidents.

Moreover, we would like to point out, that a reporting obligation in these cases would entail a considerable amount of additional work for financial entities due to the large number of phishing incidents. Mostly all of them would be reportable because the materiality thresholds of Article 8 (1) lit. a Delegated Regulation (EU) 2024/1772 and Article 9 (5) lit. b of Delegated Regulation (EU) 2024/1772 will be regularly met in this context (possible loss of data in case of a successful, malicious and unauthorised access, e.g. the customer clicks on a phishing link in his private email inbox and therefore the threat actor receives access to the customer account). It is questionable whether this is in line with the idea of reducing administrative burdens, as stated, for example, in recital 23 of Regulation (EU) 2022/2554.

Submission date

04/11/2025

Final publishing date

06/02/2026

Final answer

When a phishing incident in the private sphere of the customer does not affect services provided by the financial entity directly (or via any of the financial entity's third-party providers), it does not qualify as an 'ICT-related incident' or 'an operational or security payment-related incident' under DORA. Therefore, in that case, it cannot trigger the thresholds to be a major ICT-related incident and the related reporting obligation.

By contrast, if the financial entity itself is successfully targeted and faces an intrusion, for example through phishing emails sent to employees, or in case a widescale phishing campaign ending up affecting the financial entity's services, the incident can be qualified as an ICT-related incident under DORA. To the extent that this ICT-related incident reaches the relevant thresholds, it may be classified as a major ICT-related incident.

Status

Final Q&A

Answer prepared by

Answer prepared by the Joint ESAs Q&A
