EUROPEAN
COMMISSION

Brussels, 23.10.2024
C(2024) 6901 final

COMMISSION DELEGATED REGULATION (EU) …/...

of 23.10.2024

supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE DELEGATED ACT

One of the objectives of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) is to harmonise and streamline the ICT-related incident reporting regime for financial entities (FEs) in the European Union (EU).

Article 20 of DORA mandates the European Supervisory Authorities (ESAs) to develop through the Joint Committee and in consultation with the European Central Bank and European Union Agency for Cybersecurity:

- Draft Regulatory Technical Standards (RTS) establishing the content of the reports for ICT-related incidents and the notification for significant cyber threats, and the time limits for FEs to report these incidents to competent authorities.

Article 20 of DORA further requires the ESAs to ensure that the requirements of this Regulation are proportionate and consistent with the approach for incident reporting under Directive (EU) 2022/2555 (NIS2).

2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT

As part of developing the standards set out in this Regulation, the ESAs published the draft RTS on 8 December 2023 for a three-month consultation period, which closed on 4 March 2024. The ESAs received 109 responses from a variety of market participants across the financial sector. The ESAs' final report provides a full overview of stakeholder responses.

In the light of the comments received, the ESAs agreed with most of the proposals and their underlying arguments and have introduced changes to the RTS. These changes are related to the time limits for reporting initial notification, intermediate report and final report, reporting over weekend and bank holidays, aggregated reporting and streamlining the content of the reporting template.

On the reporting time limits, the ESAs have extended the time limit for reporting the intermediate report with up to 24 hours and the final report with at least 72 hours by starting the calculation of the timelines from the submission of the previous notification/report, instead of the moment of classification of the incident as indicated in the initial draft RTS proposed for consultation.

On weekend and bank holiday reporting, the ESAs have reduced the scope of incidents that need to be reported, removed the obligation for smaller financial entities to report the initial notification, and have extended the time limit for submission of the notifications and reports by noon at the first working day, instead of within 1-hour as indicated in the initial draft RTS proposed for consultation.

Finally, ESAs have introduced aggregated reporting at national level for FEs supervised by a single competent authority, if certain conditions are met.

3. LEGAL ELEMENTS OF THE DELEGATED ACT

Article 1 sets out the format of the type of information that needs to be provided by the financial entities.

Article 2 sets out the nature of the general information that needs to be provided by the financial entities in the case of the major ICT related incident initial notification, and the intermediate and final reports.

Article 3 defines the information that needs to be provided by the financial entities on the major ICT related incident in their initial notification.

Article 4 defines the information that needs to be provided by the financial entities on the major ICT related incident in their intermediate report.

Article 5 defines the information that needs to be provided by the financial entities about the major ICT related incident in their final report.

Article 6 establishes the time limits for the submission of the initial notification, the intermediate report and final reports referred to in Article 19(4) of Regulation (EU)2022/2554.

Article 7 defines the content of the voluntary notification for the significant cyber threats.

Article 8 contains the final provisions on entry into force.

COMMISSION DELEGATED REGULATION (EU) …/...

of 23.10.2024

supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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[1], and in particular Article 20, third subparagraph thereof,

Whereas:

(1) To ensure the harmonisation and simplication of the notification and reporting requirements for major ICT-related incidents referred to in Article 19(4) of Regulation (EU) 2022/2554, the time limits for reporting major ICT-related incidents should follow a consistent approach for all types of financial entities. For these reasons, the time limits should also, to the greatest extent possible, follow a consistent approach with, and at least be equivalent in effect to, the requirements set out in Directive (EU) 2022/2555 of the European Parliament and of the Council[2].

(2) To avoid imposing an undue reporting burden on financial entities at a time when they are handling the ICT-related incident, the content of the initial notification should be limited to the most significant information. To be able to take proper supervisory action, competent authorities need to receive information about major ICT-related incidents as quickly as possible after the financial entity has classified an ICT-related incident as major. Consequently, the time limit for submitting an initial notification as referred to in Article 19(4), point (a), of Regulation (EU) 2022/2554 should be as short as possible after an ICT-related incident has been classified as major, whilst still allowing for flexibility, especially for service business models that are not particularly time-critical, in case financial entities need more time to handle the ICT-related incident after becoming aware of it.

---

1 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 (OJ L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

2 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(3) After having received the initial notification, competent authorities should receive more detailed information about the ICT-related incident in the intermediate report and all relevant information in the final report. The information in those reports should enable competent authorities to further assess the ICT-related incident and evaluate supervisory actions they may want to take.

(4) The reporting time limits referred to in Article 20, first paragraph, point (a)(ii), of Regulation (EU) 2022/2554 should therefore balance the need for competent authorities to receive the information quickly, with the need to provide financial entities with sufficient time to obtain complete and accurate information.

(5) Taking into account the criteria set out in Article 20, first paragraph, point (a), of Regulation (EU) 2022/2554, the reporting timelines should not pose a disproportionate burden to microenterprises and to other financial entities that are not significant. In addition, to avoid a disproportional burden on financial entities, the reporting time limits should take into account weekends and bank holidays.

(6) Since significant cyber threats are to be notified on a voluntary basis, the content of such notifications should not impose a burden on financial entities and should be more limited than the information requested for major ICT-related incidents.

(7) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Supervisory Authorities.

(8) The European Supervisory Authorities have conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Stakeholders Groups established in accordance with Article 37 of Regulations (EU) No 1093/2010, 1094/2010 and 1095/2010 of the European Parliament and of the Council[3].

(9) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[4] and delivered a positive opinion on 22 July 2024. Any processing of personal data within the scope of this Regulation should be performed in accordance with the applicable data protection principles and provisions from Regulation 2018/1725,

---

[3] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj); Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj) and Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

[4] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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 (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

HAS ADOPTED THIS REGULATION:

Article 1

General information to be provided in initial notifications and intermediate and final reports on major ICT-related incidents

Financial entities shall include in the initial notification, the intermediate report, and the final report, as referred to in Article 19(4) of Regulation (EU) 2022/2554, the following general information:

(a) the type of submission (initial notification, intermediate report, or final report);

(b) the name of the financial entity, its LEI code, and the type of financial entity, as referred to in Article 2(1) of Regulation (EU) 2022/2554;

(c) the name and identification code of the entity that submits the initial notification, or intermediate or final report, for the financial entity;

(d) where applicable, the names and LEI codes of all financial entities covered in the aggregated initial notification or intermediate or final report;

(e) the contact details of the persons responsible for communicating with the competent authority on the major ICT-related incident;

(f) where applicable, the identification of the parent undertaking of the group to which the financial entity belongs;

(g) where there is monetary impact, the currency the amounts are based on.

Article 2

Specific information to be provided in initial notifications

Initial notifications as referred to in Article 19(4), point (a), of Regulation (EU) 2022/2554 shall contain at least all of the following specific information:

(a) the incident reference code assigned by the financial entity;

(b) the date of detection, time of detection, and classification of the incident pursuant to Article 8 of Commission Delegated Regulation (EU) 2024/1772[5];

(c) a description of the ICT-related incident;

(d) the criteria, laid down in Articles 1 to 8 of Delegated Regulation (EU) 2024/1772, on the basis of which the financial entity classified the ICT-related incident as major;

(e) the Members States that are impacted by the ICT-related incident;

(f) information on how the ICT-related incident was discovered;

(g) where available, information about the origin of the ICT-related incident;

(h) information about whether the financial entity has activated a business continuity plan;

[5] Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT-related incidents and cyber threats, setting out materiality thresholds and specifying the details of reports of major incidents (OJ L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

(i) where applicable, information about the reclassification of the ICT-related incident from major to non-major;

(j) where available, any other relevant information.

Article 3

Specific information to be provided in intermediate reports

Intermediate reports as referred to in Article 19(4), point (b), of Regulation (EU) 2022/2554 shall contain at least all of the following specific information:

(a) where applicable, the incident reference code provided by the competent authority;

(b) the date and time of occurrence of the ICT-related incident;

(c) where applicable, the date and time when the financial entity has recovered its regular activities;

(d) information about how the criteria laid down in Articles 1 to 8 of Delegated Regulation (EU) 2024/1772 have been fulfilled, on the basis of which the financial entity classified the ITC-related incident as major;

(e) the type of ICT-related incident;

(f) where applicable, the threats and techniques used by the threat actor;

(g) affected functional areas and business processes;

(h) affected infrastructure components supporting business processes;

(i) impact on the financial interest of clients;

(j) information about reporting about the ICT-related incident to other authorities;

(k) temporary actions or measures taken or planned to be taken by the financial entity to recover from the ICT-related incident;

(l) where applicable, information on indicators of compromise.

Article 4

Article Specific information to be provided in final reports

Final reports as referred to in Article 19(4), point (c), of Regulation (EU) 2022/2554 shall contain all of the following specific information:

(a) information about the root causes of the ICT-related incident;

(b) dates and times when the ICT-related incident was resolved and the root cause(s) addressed;

(c) information on the resolution of the ICT-related incident;

(d) where applicable, information relevant for resolution authorities;

(e) information about direct and indirect costs and losses stemming from the ICT-related incident and information about financial recoveries;

(f) where applicable, information about recurring ICT-related incidents.

Article 5

Time limits for the initial notification, and for the intermediate and final reports

1. Financial entities shall submit the initial notification and the intermediate and final reports as referred to in Article 19(4), points (a), (b) and (c), of Regulation (EU) 2022/2554 within the following time limits:

   (a) for the initial report: as early as possible, but in any case, within four hours from the classification of the ICT-related incident as a major ICT-related incident and no later than 24 hours from the moment the financial entity has become aware of the ICT-related incident;

   (b) for the intermediate report: at the latest within 72 hours from the submission of the initial notification, even where the status or the handling of the incident have not changed as referred to in Article 19(4), point (b), of Regulation (EU) 2022/2554. Financial entities shall submit an updated intermediate report without undue delay, and in any case when the regular activities have been recovered;

   (c) for the final report: no later than one month after either the submission of the intermediate report, or, where applicable, after the latest updated intermediate report.

2. Where the financial entity has not classified an ICT-related incident as major within 24 hours from the moment the financial entity has become aware of the ITC-related incident but classifies that ICT-related incident as major at a later stage, the financial entity shall submit the initial notification within four hours from the classification of the ICT-related incident as a major incident.

3. Financial entities that are unable to submit the initial notification, intermediate report, or final report within the time limits set out in paragraph 1, shall inform the competent authority thereof without undue delay, but no later than the respective time limits for the submission of the notification or report, and shall explain the reasons for the delay.

4. Where the time limit for the submission of an initial notification, intermediate report, or a final report falls on a weekend day or a bank holiday in the Member State of the reporting financial entity, the financial entity may submit the initial notification, intermediate or final reports by noon of the next working day.

5. Paragraph 4 shall not apply for the submission of an initial notification or an intermediate report by credit institutions, central counterparties, operators of trading venues, and other financial entities identified as essential or important entities pursuant to Article 3 of Directive (EU) 2022/2555.

6. Competent authorities may decide that paragraph 4 shall not apply for the submission of an initial notification or an intermediate report by financial entities, other than those referred to in paragraph 5, which are significant or have a systemic character for the financial sector at national or Union level. Competent authorities shall notify their decision to the identified financial entities. The decision of the competent authority shall only apply in respect of incidents reported after the date of notification of the decision by the competent authority to the identified financial entities.

Article 6
Content of the voluntary notification of significant cyber threats

The content of the voluntary notification in relation to significant cyber threats as referred to in Article 19(2) of Regulation (EU) 2022/2554 shall cover all of the following:

(a) general information about the notifying financial entity as set out in Article 1;

(b) the date and time of detection of the significant cyber threat and any other relevant timestamps related to the significant cyber threat;

(c) a description of the significant cyber threat;

(d) information about the potential impact of the significant cyber threat on the financial entity, its clients, or financial counterparts;

(e) the classification criteria that would have triggered a major incident report laid down in Articles 1 to 8 of Delegated Regulation (EU) 2024/1772 if the cyber threat had materialised;

(f) information about the status of the significant cyber threat and any changes in the threat activity;

(g) where applicable, a description of the actions taken by the financial entity to prevent the materialisation of the significant cyber threats;

(h) information about any notification of the significant cyber threat to other financial entities or authorities;

(i) where applicable, information on indicators of compromise;

(j) where available, any other relevant information.

Article 7
Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 23.10.2024

For the Commission
The President
Ursula VON DER LEYEN