

Brussels, 23.10.2024
C(2024) 7277 final

COMMISSION IMPLEMENTING REGULATION (EU) .../...

of 23.10.2024

laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat

(Text with EEA relevance)

COMMISSION IMPLEMENTING REGULATION (EU) .../...

of 23.10.2024

laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates, and procedures for financial entities to report a major ICT-related incident and to notify a significant cyber threat

(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) 2016/1011¹, and in particular Article 20, fourth paragraph, thereof,

Whereas:

- (1) To ensure that financial entities report major incidents to their competent authorities in a consistent manner and to ensure that they provide those authorities with data of good quality, it should be specified which data fields financial entities need to provide at the various stages of the reporting referred to in Article 19(4) of Regulation (EU) 2022/2554. It is important that that information is presented in a way that allows for a single overview of the incident. It is therefore necessary to lay down a single reporting template for those purposes.
- (2) Financial entities should complete those data fields of the reporting template that correspond to the information requirements of the respective notification or report. However, financial entities that already have information which they are to provide at a later reporting stage, i.e. in the intermediate or final report, should be allowed to anticipate the submission of the data.
- (3) Since multiple or recurring incidents may constitute a major incident as referred to in Article 8 of Commission Delegated Regulation (EU) 2024/1772², the design of the reporting template and of the data fields should enable financial entities to report such recurring incidents.

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 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).

- (4) To ensure accurate and up to-date information, the reporting template should enable financial entities, when submitting the intermediate and final report, to update any information that was submitted previously, and where necessary reclassify major incidents as non-major.
- (5) The legal identification of entities should be aligned with the identifiers specified in the implementing technical standards adopted pursuant to Article 28(9) of Regulation (EU) 2022/2554.
- (6) Where financial entities outsource the major ICT-related incident reporting obligations to a third party, competent authorities should be aware of the identity of the third-party reporting on behalf of the financial entity prior to the submission of the first notification or reporting, in order to verify the legitimacy of the reporting third party.
- (7) To identify easily the impact of an incident that occurred at, or was caused by a third-party provider, and that affects multiple financial entities within a single Member State, and to reduce the reporting effort for financial entities, the reporting template should allow for the submission of an aggregated report covering aggregated information about the impact of the incident on all impacted financial entities that have classified the incident as major.
- (8) The reporting template should be designed in a technology neutral way to allow for its implementation into various incident reporting solutions that already exist or that may be developed for the implementation of the requirements of Regulation (EU) 2022/2554.
- (9) The design of the reporting template and data fields should facilitate the reporting of major ICT-related incidents by third parties to whom financial entities outsourced their reporting obligation in accordance with Article 19(5) of Regulation (EU) 2022/2554.
- (10) This Regulation is based on the draft implementing technical standards submitted to the Commission by the European Supervisory Authorities.
- (11) The European Supervisory Authorities have conducted open public consultations on the draft implementing technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Banking Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1093/2010³, 1094/2010⁴, 1095/2010⁵ of the European Parliament and of the Council.
- (12) 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

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>).

⁴ 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>).

⁵ 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>).

Council⁶ 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 set out in Regulation 2018/1725,

HAS ADOPTED THIS REGULATION:

Article 1

Template for reporting ICT-related major incidents

1. Financial entities shall use the template laid down in Annex I to submit the initial notification, the intermediate report, and the final report referred to in Article 19(4) of Regulation (EU) 2022/2554 as follows:
 - (a) financial entities that submit an initial notification shall complete the data fields of the template which correspond to the information to be provided in accordance with Article 2 of Commission Delegated Regulation (EU) 2024/xxx [C(2024) 6901]⁷, and may, where they already have that information, complete those data fields the completion of which is not required for an initial notification but is required for an intermediate or final report;
 - (b) financial entities that submit an intermediate report shall complete the data fields of the template which correspond to the information to be provided in accordance with Article 3 of Delegated Regulation (EU) 2024/xxx [C(2024) 6901] and may, where they already have the relevant information, complete data fields the completion of which is not required for the intermediate report, but is required for the final report.
 - (c) financial entities that submit a final report shall complete the data fields of the template which correspond to the information to be provided in accordance with Article 4 of Delegated Regulation (EU) 2024/xxx [C(2024) 6901].
2. Financial entities shall ensure that the information contained in the initial notification, and in the intermediate and final report, is complete and accurate.
3. Financial entities shall provide estimated values based on other available data and information, to the extent possible, where accurate data are not available at the time of reporting for the initial notification or the intermediate report.
4. When submitting an intermediate or final report, financial entities shall use the template laid down in Annex I to submit all required information and update, where applicable, the information that was previously provided in the initial notification or in the intermediate report.
5. Financial entities shall follow the data glossary and instructions set out in Annex II when completing the template laid down in Annex I.

⁶ 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>).

⁷ Commission Delegated Regulation (EU) 2024/xxx 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. (OJ L, xxx/xxx, ELI: xxx). [OP please insert reference to C(2024) 6901]

Article 2

Joint submission of initial notification, intermediate and final reports

Financial entities may combine the submission of the initial notification, the intermediate report, and the final report to provide two or all of those at the same time, where regular activities have recovered or the root cause analysis has been completed and provided that the time limits set out in Article 5 of Commission Delegated Regulation (EU) 2024/xxx [C(2024) 6901] are met.

Article 3

Recurring ICT-related incidents

Financial entities that provide information on non-major recurring ICT-related incidents that cumulatively meet the conditions for one major ICT-related incident as set out in Article 8(2) of Delegated Regulation (EU) 2024/1772, shall provide that information in an aggregated form.

Article 4

Use of secure electronic channels

1. Financial entities shall use secure electronic channels as made available by their competent authority to submit the initial notification and the intermediate and final reports.
2. Financial entities that are unable to use the secure electronic channels as made available by their competent authority shall inform their competent authority about a major ICT-related incident through other secure means in agreement with the competent authority. If required by the competent authority, financial entities shall resubmit the initial notification, or intermediate or final report, through the secure electronic channel as made available by their competent authority once they are able to do so.

Article 5

Reclassification of major ICT-related incidents

Where after further assessment, the financial entity concludes that the ICT-related incident previously reported as major, at no time fulfilled the classification criteria and thresholds set out in Article 8 of Delegated Regulation (EU) 2024/1772, the financial entity shall notify to the competent authority that it has reclassified the ICT-related incident from major to non-major by providing the information about that reclassification in the template laid down in Annex II to this Regulation in relation to the fields ‘type of report’ and ‘other information’.

Article 6

Notification of outsourcing of the reporting obligations

1. Financial entities that have outsourced the obligation to report major ICT-related incidents in accordance with Article 19(5) of Regulation (EU) 2022/2554 shall inform their competent authority of that outsourcing arrangement as soon as the outsourcing arrangement has been concluded and at the latest prior to the first notification or reporting.

2. Financial entities shall provide the competent authority with the name, contact details, and identification code of the third-party that will submit the major ICT-related incident notifications or reports for them.
3. Financial entities shall inform their competent authority as soon as they no longer outsource their reporting obligations as referred to in Article 19(5) of Regulation (EU) 2022/2554.

Article 7 *Aggregated reporting*

1. A third-party service provider to whom reporting obligations have been outsourced as referred to in Article 19(5) of Regulation (EU) 2022/2554 may use the template set out in Annex I to this Regulation to provide aggregated information about a major ICT-related incident impacting multiple financial entities in one single notification or report, and submit that notification or report to the competent authority on behalf of all impacted financial entities, provided that all of the following conditions are met:
 - (a) the major ICT-related incident to be reported originates from or is being caused by a third-party ICT service provider;
 - (b) that third-party service provider provides the relevant ICT service to more than one financial entity, or to a group;
 - (c) the ICT-related incident is classified as major by each financial entity covered in the aggregated notification or report;
 - (d) the major ICT-related incident affects financial entities within a single Member State and the aggregated report relates to financial entities which are supervised by the same competent authority;
 - (e) competent authorities have explicitly permitted this type of financial entities to aggregate their reporting.
2. Paragraph 1 shall not apply to credit institutions that are considered to be of significant relevance as referred to in Article 2 point (16) of Regulation (EU) No 468/2014⁸, operators of trading venues, and central counterparties, which shall only use the template in Annex I to submit major ICT-related incident notifications or reports individually to their competent authority.
3. Where competent authorities require information on the individual impact of the major ICT-related incident on a single financial entity, upon request of the competent authority, the financial entity shall submit an individual notification or a report on the major ICT-related incident.

Article 8 *Notification of significant cyber threats*

1. Financial entities that notify significant cyber threats to competent authorities in accordance with Article 19(2) of Regulation (EU) 2022/2554 shall use the template

⁸ REGULATION (EU) No 468/2014 OF THE EUROPEAN CENTRAL BANK of 16 April 2014 establishing the framework for cooperation within the Single Supervisory Mechanism between the European Central Bank and national competent authorities and with national designated authorities (OJ L 141, 14.5.2014, p. 1).

laid down in Annex III to this Regulation and follow the data glossary and instructions set out Annex IV to this Regulation.

2. Financial entities shall ensure that the information contained in the notification of significant cyber threats is complete and accurate.

Article 9

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