Contribution ID: c1364348-f067-4dcc-8027-441d447cd878
Date: 04/03/2024 13:17:32

Public consultation on Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft Implementing Technical Standards on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat

Fields marked with * are mandatory.

Intorduction

The European Supervisory Authorities (EBA, EIOPA and ESMA) have published the second batch of Consultation Papers on the mandates stemming from the Digital Operational Resilience Act (DORA) with the aim to collect market participants' feedback on the proposed Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft Implementing Technical Standards on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat.

Market participants are invited to provide their feedback to the draft technical standards by responding to the questions presented in this consultation paper.

The feedback received will be taken into account in the finalisation of the draft technical standards, which are due to be submitted to the European Commission by 17 July 2024.

Comments are most helpful if they:

- respond to the questions stated;
- indicate the specific point to which a comment relates; contain a clear rationale;
- provide evidence (including relevant data, where applicable) to support the views expressed;
- reflect a cross-sectoral (banking, insurance, markets and securities) approach, to the extent possible;
- and describe any alternative approaches the ESAs could consider.

To submit your comments, please click on the blue "Submit" button in the last part of the present survey. Please note that comments submitted after 4 March 2024 or submitted via other means may not be processed.

Please clearly express in the consultation form if you wish your comments to be published or to be treated as confidential. A confidential response may be requested from the ESAs in accordance with the ESAs' rules on public access to documents. We may consult you if we receive such a request.

Any decision we make not to disclose the response is reviewable by the ESAs' Boards of Appeal and the European Ombudsman.

The protection of individuals with regard to the processing of personal data by the ESAs is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of the ESA websites.

General Information

* Name of the Reporting Stakeholder

Dutch Federation of Pension Funds

Legal Entity Identifier (LEI), if available

* Type of Reporting Organisation

- ( ) ICT Third-Party Service Provider
- (•) Financial Entity
- ( ) Industry Association/Federation
- ( ) Consumer Protection Association
- ( ) Competent Authority
- ( ) Other

* Financial Sector

- [ ] Banking and payments
- [ ] Insurance
- [ ] Markets and securities
- [x] Other

* If other, please specify

Pensions

* Jurisdiction of Esstablishment

Netherlands

* Geographical Scope of Business

- (●) EU domestic
- ( ) Eu cross-border
- ( ) Third-country
- ( ) Worldwide (EU and third-country)

* Name of Point of Contact

Martin van Rossum

* Email Address of Point of Contact

rossum@pensioenfederatie.nl

* Please provide your explicit consent for the publication of your response.

- [x] Yes, publish my response
- [ ] No, please treat my response as confidential

Questions

Question 1. Do you agree with with the proposed timelines for reporting of major incidents?

- ( ) Yes
- (●) No

* 1b. Please provide your reasoning and suggested changes.

We note that no proportionality is given with regards to timelines for reporting. That does no justice to the size nor risk of different types of financial entities. Level 1 of DORA (article 20, (a) iii) outlines: “take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations, and in particular, with a view to ensuring that, for the purposes of this paragraph, point (a), point (ii), different time limits may reflect, as appropriate, specificities of financial sectors”.

IORPs are at the end of the financial value chain, offering B2C services. Any ICT-related incidents therefore have a limited impact on the financial sector. IORPs are not operating on a 24-hour a-day and 7 days a week basis like in the payment sector. Moreover, the vast majority of IORPs is very small and reporting costs will weigh disproportionately on them. We urge ESAs to explore the idea of different timelines depending on the type of financial entity, to better capture the specificities of the different types of financial entities.

We understand the urgency related to major incidents but question how soon supervisors can and will act in such cases and if that justifies the short timeline for the initial notification.

A perverse incentive is given to delay the classification of an incident as major. Considering that the initial report should be filed within 4 hours after the classification and within 24 hours from the time of detection of the incident, financial entities would have an incentive to classify the incident as major only after 20 hours, in order to have the maximum amount of time for the initial notification. It seems best to drop reference to a certain amount of hours after classification as major and only maintain the 24-hour reporting deadline.

We are concerned that timelines are too short for situations where an incident originates further in the subcontracting chain or relates to multiple financial entities. The organization where the incident originates will be overwhelmed by requests from financial entities that all take their own approach and information requirements, creating disproportionate administration costs. Uniform reporting and extended deadlines are needed in such cases.

While financial entities have the responsibility for correct and complete incident reporting, they need to be able to rely on (sub)contracting parties to report the relevant and correct information. It is helpful to have a single template with data fields for reporting incidents up the subcontracting chain as well as a standardized process for submitting reports. That will help both financial entities and third parties in adhering to a uniform standard for information requests.

The third party or sub-contractor could be allowed to report to the supervisor directly on behalf of the financial entity. Considering the short timelines and limited ability of financial entities to manage the incident response at third parties, let alone subcontractors, they should be able to rely on those reports to some reasonable extent. The financial entity would then only have to report the effects of the incident to its own organization.

With regards to CTPPs, considering the size of their financial entity customer base and considering the supervision and oversight provided in DORA, it seems best for them to report incidents directly to all supervisors.

The deadline for initial notification could also be extended in cases where the incident originates with a third party or subcontractor. Timelines are too short to request and process data from third parties. Consequently, either the amount of data that needs to be provided must be limited or deadlines needs to be longer.

Question 2. Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the initial notification for major incidents under DORA?

- ○ Yes
- ◉ No

* 2b. Please provide your reasoning and suggested changes.

We strongly urge to perform an additional review on the proposed data fields, to reduce the number of data fields which are regarded absolutely necessary for an initial report. The large amount of data fields will mean that financial entities will rush to obtain information from various departments, without time to assess this information, which would not lead to a coherent or holistic approach to the reporting. That time is better spent in incident resolution.

The number of questions for an initial notification is extensive and will negatively impact the timeline of notification. A minimalistic approach is preferred for the initial notification. That is in line with the political goal of rationalizing reporting requirements and reducing them by 25%, as outlined in the 2023 State of the Union. At the same time, competent authorities risk being overwhelmed with data to process.

The data fields regarding recurring incidents (2.11-13) are more appropriate for the intermediate report as this information may not be available within the first four hours and requires analysis and input from IT staff mitigating the Incident.

Data fields 2.9 and 2.10, requesting descriptions, are suggestive and will not result in objectively measurable information. It should be considered to specify these questions more. The financial entity might not have good insight in the direct impacts of incidents on other financial entities and third-party providers, and vice versa.

Data field 2.15 will not result in relevant information without detailed knowledge of how the business continuity plan in question is structured. Therefore, we suggest to remove this question.

Lastly, data field 2.16 demands ‘Other information’. This can be anything and will result in irrelevant discussions at the financial entity. Instead, we find it more appropriate for the supervisor to request more specific additional information later in the process.

Question 3. Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the intermediate report for major incidents under DORA?

- ○ Yes
- ◉ No

* 3b. Please provide your reasoning and suggested changes.

Again, we strongly urge to perform an additional review on the proposed data fields, to reduce the number of data fields. The required information is extensive and may not be available in time. We consider that the required information will not be of great added value in the spirit of this process. A minimalistic approach is preferred for the intermediate report. That is in line with the political goal of rationalizing reporting requirements and reducing them by 25%, as outlined in the 2023 State of the Union. At the same time, competent authorities risk being overwhelmed with data to process.

Additionally, and perhaps more significantly, gathering the information for the intermediate report can take a

lot of capacity and resources. It should be considered that major incidents are very infrequent and the ways to gather and assess the needed information are not a standard procedure for the financial entity. This will result in significant effort and use of resources to assess (under time constraints) ways to gather and to report, resulting in a larger than needed resource claim and cost to resolve the incident. This will mean that these activities are included in the Business Continuity Plan, without direct impact on resolving the incident at hand. We suggest considering the necessity of this information considering the purpose of the process.

We repeat that data fields asking for descriptions (3.21, 3.23 and 3.37) are suggestive and will not result in objectively measurable information. Such reporting should be avoided.

Question 4. Do you agree with the data fields proposed in the draft RTS and the Annex to the ITS for inclusion in the final report for major incidents under DORA?

- ○ Yes
- ◉ No

* 4b. Please provide your reasoning and suggested changes.

The breakdown of costs and losses in data fields 4.14 till 4.25 will be especially time-consuming and burdensome. Some of these costs will not materialize within a month and therefore data will not be available. This concerns for example customer redress and compensation (4.19) and fees due to non-compliance with contractual obligations (4.18).

The reporting of staff costs under data field 4.17 can lead to a disproportionate amount of administration. As major incidents are likely infrequent, the reporting of staff cost needs to be implemented ad hoc when an incident occurs. Reporting is only mandatory ‘when applicable’, though in practice there will always be staff costs involved. Instead, reporting on staff costs should be voluntary.

Resolution of an incident is likely considered a ‘run’ activity that requires no separate recording of hours spent. This will lead to frustration among staff about adhering to such an ad hoc procedure with no direct impact on incident resolution. It also takes time to organize during a crisis. We suggest more space should be given to provide estimates and to report in less detail, in order to limit the required overhead.

Question 5. Do you agree with the data fields proposed in the RTS and the Annex to the draft ITS for inclusion in the notification for significant cyber threats under DORA?

- ○ Yes
- ◉ No

* 5b. Please provide your reasoning and suggested changes.

We would like to suggest to change some fields from “mandatory” to “optional”. It is of foremost importance to report threats as soon as possible. The more mandatory fields, the longer it takes to report and the more resistance there will be to reporting a threat. This is relevant as reporting is not mandatory. Our suggestion is to change the classification of data fields 10, 11, 12 and 18 from “yes” to “optional”; and of data fields 19 and 20 from “yes, if applicable” to “optional”. If those data fields are not reported, the report is still valuable, in our opinion.

Question 6. Do you agree with the proposed reporting requirements set out in the draft ITS?

- ○ Yes

No

* 7b. Please provide your reasoning and suggested changes.

We note that an incident at an ICT third party service provider can lead to a large number of reports when a lot of financial entities use the same ICT third-party service provider. This, combined with the fact that many questions in the intermediate and final report require input from the ICT third-party service provider leads us to believe a more efficient way of reporting an incident should be possible where an incident affects multiple financial entities because it is caused by the same ICT third-party.

To promote effective incident reporting and resolution, the financial entity should be able to delegate the responsibility to report to the third party or subcontractor. It should be able to rely on the correctness and completeness of the report to some reasonable extent. With regards to CTPPs, considering the size of their financial entity customer base and considering the supervision and oversight provided in DORA, it seems best for them to report incidents directly to all supervisors. The financial entity then only has to report the effects of the incident to its own organization, to the extent a response is warranted.

This is essential, as the third party otherwise risks to be overwhelmed by questions from clients within the first hours after an incident occurs. The financial entity's involvement in that case would have very limited possibilities to contribute to incident resolution. Rather, it should trust on the third party for resolution and reporting in the short term.

8. Do you have any further comment you would like to share?

Contact

Contact Form