Contribution ID: 192ab18a-eda3-4d77-aa9d-b92de774552b
Date: 04/03/2024 13:22:26

Public consultation on Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554

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 to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation (EU) 2022/2554.

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 Establishment

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. Are articles 1 and 2 appropriate and sufficiently clear?

- ( ) Yes
- (●) No

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

A rigid interpretation of the DORA Level 1 text on the subcontracting would lead to a disproportionate responsibility on financial entities. In such a reading, financial entities would have to fully monitor and control the subcontracting chain when it comes to critical or important functions. It would be near impossible to get full transparency and control over parties in the subcontracting chain, considering the chain can be very long. This is especially true as business processes and risk management include (competitively) sensitive information. Financial entities will not always be in the position to get (sub)contractors to provide the necessary information and controls.

The RTS should shed light on how to read Level 1 in this respect. It should acknowledge that a rigid interpretation would lead to inefficient allocations of resources, which would sour contracting relations and distract from controlling the biggest subcontracting risks. Indeed, the RTS should already speak out for a risk-based approach in the Recitals.

While we acknowledge the importance of maintaining a register and imposing obligations on subcontractors that deliver a substantial portion of the contracted ICT service, it is disproportionate to extend identical requirements for all subcontractors. The approach would hinder financial entities from using most cloud services, as providers will not be able (or willing) to accommodate such stringent requirements.

The scope of the RTS should be strictly limited to subcontracted activities that have a material contribution to critical or important functions, as is the case in the register of information on contractual arrangements. The risk assessment should take into account the size of the provider to avoid a disproportionate burden on subcontractors providing a minor service. Financial entities should not be required to assess the whole chain of subcontractors based on the elements listed in Article 1(a-i). That administrative burden would be disproportionate to its contribution to digital operational resilience.

What remains unclear in Article 1 is how increased or reduced risk plays out in the application of paragraphs 2 to 7, as these articles are quite normative and appear to have little room for interpretation or adaptation to an increased or reduced risk. The elements that need to be considered in the risk assessment as indicated in Article 3 and the elements that need to be specified in the contractual agreement (Article 4) should be eligible to change in case of reduced risk. Article 1 should make clear how proportionality can be applied and what the concrete consequences are for contracting subcontractors with a low risk profile.

We find it important to specify a non-exhaustive list of criteria or elements of risks to help financial entities in the implementation of the RTS's requirements. A similar list of requirements is provided when it comes to the policy of ICT-subcontracting. The differences in the requirements should be made explicit. In our view, the elements in Article 1 should be read as an exhaustive list without minimum requirements. This should be clarified.

Additionally, the elements a) to e) of article 1 are in our opinion properly described and clear. For element d), the requested information might be difficult to attain for cloud environments with distributed data centers. Elements f), g) and h) are multi-interpretable with regard to the scope. These elements can be interpreted as relating exclusively to the specific subcontracted services or as relating to ICT service as a whole. We emphasize that it is disproportionate to assess risks at the subcontractor level for the whole subcontracting chain. Only assessing risk at the ICT services level is feasible. With regard to i) the concentration risk, we suggest to add a further (short) explanation of which aspects can or should be taken into account, as this is open to multiple interpretations.

Question 2. Is article 3 appropriate and sufficiently clear?

- Yes

- [x] No

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

The description of ‘possible changes’ suggests that this should be a forward-looking assessment, which aims to address the effect of these changes in the risk assessment. In our opinion this is contrary to the term ‘periodically’, which suggests a more routine approach. This point should be clarified.

Many subcontractors perform relatively minor functions (for example, providing analytics, publicly available data or SMS services). To impose the same rigorous risk assessment criteria on these minor functions as on major subcontractors would not only be disproportionate but also impractical.

Certain provisions such as step-in rights are not feasible in the context of cloud services. For example, neither a financial entity nor the primary ICT service provider running on a third-party cloud environment can realistically assume control over operations of such hosting service providers. This highlights the necessity for making such provisions optional.

The Article does not consider that services are already subcontracted by ICT third-party service providers. The risk assessments performed by the financial entity at the moment of subcontracting are probably not fully compliant with Article 3. We believe it is not realistic to implement this Article by January 17th 2025, especially when the final version of this RTS is expected after July 2024. We suggest a transition period for implementation with regard to current subcontracted services of a year after final publication of this RTS.

Question 3. Is article 4 appropriate and sufficiently clear?

- [ ] Yes
- [x] No

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

With regard to conditions for subcontracting, we consider it difficult to (completely) fill out these specifications as part of describing the contractual arrangements. These identified ICT services might not be subcontracted in the (near) future or at all. The required information might not be available, leading to a very theoretical approach in drafting these contractual arrangements. In our opinion this puts extensive pressure on drafting specifications for a situation which might (or might not) occur. We would suggest to separate the identification of eligible ICT services for subcontracting from the conditions that will apply and suggest another timeframe for drafting these conditions.

With regard to Article 4 j), we are of the opinion that the latter part of the termination rights ('provision of services fails to meet service levels agreed by the financial entity') is disproportionate. It will lead to extensive pressure to meet agreed service levels. This element is a threat for the continuity of services. For the improvement of the maturity of the subcontracting chain, this element can be counterproductive. It is also unclear to which service levels this specific text applies. If this remains part of the revised RTS, we suggest to clarify if this regards the (ICT) subcontractor and, or, relates to the service levels as described in f) and g).

Finally, we would emphasize that the requested specifications do not support an effective and efficient business process with regard to subcontracting in case of multi-client situations where multiple financial entities are outsourcing to one ICT third party service-provider. Especially g) and h) provide unique, individual responses (per financial entity) which lead to customization in the contractual agreements between ICT third-party service provider and subcontractor. This leads to extensively high(er) administrative costs of subcontracting for the financial entity due to individual reporting timelines, service levels and security features at the subcontracting level and the level of ICT third-party service provider. It also provides the risk of not being able to find a subcontractor servicing a multi-client situation at the ICT third-party service provider, leading to other risks as (for example) higher concentration risks, and risks of inefficient or failing business processes.

Question 4. Is article 5 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

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

We once again note that it is impossible and disproportionate to fully monitor the entire subcontracting chain. It would lead to excessive documentation, which would take attention away from the biggest outsourcing risks. Besides the administrative burden, this Article has considerable cost implications. It also gives no consideration to the fact that a financial entity does not have access to certain information because of the confidentiality between service-provider and subcontractor (and subcontractors thereof). The aim of Article 5 can also be achieved by delegating these requirements to the ICT service provider and supervising the financial entity through supervision of the ICT service provider.

Question 5. Are articles 6 and 7 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

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

Although we believe the financial entity should be informed of changes to subcontracting arrangements and have termination rights when contractual agreements are violated, we believe Articles 6 and 7 do not fully support an effective and efficient business process with regard to subcontracting in case of multi-client situations where multiple financial entities are outsourcing to one ICT third party service-provider.

According to our interpretation, Article 6 suggests that every change has to be assessed as material or non-material with different possible outcomes per financial entity, with different timelines and different results as to approve or object to this change. This leads to a complicated situation which is not conducive for running efficient business processes and would lead to higher administrative costs. Specifically, with regard to article 6, we are of the opinion that the definition of 'material changes' is multi-interpretable and will lead to diverse opinions and actions. We suggest to add a (non-exhaustive) list of examples or elements to encourage equal interpretation of this definition amongst financial entities: 'any change relating to the in article 4 enumerated contractual items d), g), h), i) and / or j) can be seen as a material change'.

The notice period can differ for different financial entities, which will complicate coordination between ICT third party service-provider and subcontractor. The financial entity will not benefit from this situation as decisions regarding changes will be delayed or take extra time due to different notice periods. We suggest to add a more specific timeframe.

Also, we support the right to request modifications (Article 6.4). However, due to the contractual relationship of ICT third-party service provider with subcontractor, it is questionable if different modifications by different financial entities regarding a single subcontractor will be effectuated. More guidance with regard to implementation of this article in multi-client situations might enhance adequate implementation in the business.

Overall, with regard to Article 6, we believe it is unrealistic to require that material changes to subcontracting arrangements are only implemented after the financial entity has approved or not objected. The Article fails to take the practical realities of outsourcing relationships into account, especially with major ICT and cloud suppliers.

With regard to article 7, we notice that the right to terminate applies when the ICT third-party service provider implements material changes to subcontracting arrangements despite the objection of the financial entity, or without approval within the notice period. Article 6 indicates that material changes may only be implemented if the financial entity has approved or not objected. This situation where 'not objected' may be seen as a consent according to article 6, is a reason to use the right of termination in article 7. We suggest to clarify this by either removing 'without approval' in article 7 (preferred option) or 'not objected' in article 6 (although this option enhances the efficiency of the contract revising process).

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

Contact

Contact Form