Contribution ID: 194e8ee8-7f0e-411f-87cc-57f17915251e
Date: 11/09/2023 12:34:42

Public consultation on draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554

Fields marked with * are mandatory.

Introduction

The European Supervisory Authorities (EBA, EIOPA and ESMA) have published the first 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 further specify the detailed content of the policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers under 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 January 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 11 September 2023 or submitted via other means may not be processed.

Please clearly express in the consultation form if you wish your comments to be disclosed 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

52988368

* 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

* Jurisdiction of Establishment

The 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

Questions

Question 1: Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?

- ◉ Yes
- ○ No

1a. Please provide additional comments (if any).

As a general comment, it should be noted that a large part of the guidance provided in the different RTS and ITS consultation documents presented by the ESAs, effectively results in a translation of DORA Level I principle-based requirements into DORA Level II rule-based requirements. Furthermore, these rule-requirements are based in several instances on existing requirements for one specific category of financial institutions (e.g. banks), which means they are ill-fitting for pension funds.

In the introduction of these more stringent rule-based requirements, the proportionality principle introduced in article 4 DORA has been substantially limited. Size effectively seems to be the only remaining measure of proportionality, while the nature, scale and complexity of the services, activities and operations are no longer regarded.

As a result, many of the initial DORA requirements are translated into level II implementation requirements that are more stringent than necessary for pension funds (IORPs) and their service providers to realize an acceptable level of digital operational resilience.

Article 1 is clear and appropriate. Additional guidance is helpful with regards to further specify the context and to what level of the required risk assessment should be described in the policy. In addition, we see no added value to perform such an assessment for intra-group service providers.

Article 2 is clear and appropriate.

We appreciate the choice made by European Supervisory Authorities to refer to the definition of ‘critical or important functions’ provided by DORA, rather than providing more detailed criteria in the RTS. This makes it possible to tailor approaches to different sub-sectors in the financial sector. It ensures the creation of more risk-based control measures, by which the effectiveness of DORA is increased. Nevertheless, we would appreciate sector-specific guidance from the NCA. The broad definition leaves room for differences of interpretation, by which a pension fund could be unintentionally non-compliant.

Question 2: Is article 3 regarding the governance arrangements appropriate and sufficiently clear?

- ○ Yes
- ◉ No

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

Most requirements are already in place within most organizations in the Dutch pension sector. They are however not necessarily documented in one specific policy on the use of ICT services supporting critical or important functions. We consider it unnecessary to have this documented in one policy. It would be helpful for NCAs to have room to take this into consideration.

Moreover, we find it unnecessary to mandatorily review such a policy every year. It would lead to unnecessary overhead costs. It would be appreciated if the review frequency for the policy on the use of ICT services supporting critical or important functions would be at least once every three years.

The ESAs require the use of independent sources to assess the ICT third-party service provider. While the use of independent sources is a good practice that pension funds try to use in most cases, it is not always possible to find publicly available independent assessments. In such cases it would cost extra resources to get an independent review. We point at the possibility of financial entities to perform a review inhouse. We therefore suggest to make an independent review voluntary.

Pension funds outsource most of their core activities to pension service provider. This practice is reflected in DORA Recital 21. That means that pension service providers perform a review of ICT third-party service providers. In our view, they are able to provide a sufficient level of assurance.

Question 3: Is article 4 appropriate and sufficiently clear?

- ◉ Yes
- ○ No

3a. Please provide additional comments (if any).

Question 4: Is article 5 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

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

Requirements with regards to managing contract and third parties during the duration of the contract, as well as having a ‘Know your customer’ process in place are good practices. However, the specific requirement to have this process in place is ineffective in the pension sector as pension funds often outsource the management of third-party providers to their main processor/ICT provider. DORA recital 21 emphasizes that this practice by pension funds should be respected. It would be helpful if contract and third-party management could be delegated to the main processor, which will otherwise be the sole object of this process.

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

- ○ Yes
- ◉ No

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

Article 6 is clear and appropriate. Such a risk assessment is considered good practice, and already a practice within most organizations within the pension sector. We have no further comments concerning this article.

Article 7 is sufficiently clear and partially appropriate. Conducting a Due Diligence assessment prior to contracting a third party is common practice within our industry and will require limited additions to our current processes.

In our point of view, an intragroup due diligence has no added value. Pension service providers are subject to strict supervision by the pension funds and NCAs. Pension funds and pension service providers also have contractual agreements about the performance of ISAE 3000a and 3402 audits by external third parties. We therefore request to remove the internal due diligence obligation.

We understand the thinking behind Article 7, paragraph 1(e) and supports the intention of ethical and socially responsible business practices. We do however not see the relevance of this due diligence check to the operational resilience of ICT services and its providers. We therefore find it inappropriate for this due diligence requirement to be enforced under DORA.

Question 6: Is article 8 appropriate and sufficiently clear?

- ◉ Yes
- ○ No

6a. Please provide additional comments (if any).

Article 8 is clear and appropriate. (Regulatory) measures to prevent Conflict of Interest are common practice within the pension sector.

Question 7: Is article 9 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

* 7b. If not, please provide your reasoning and suggested changes.

We appreciate that the subjects of the articles to be added to contracts with ICT third-party service providers are clear. Nevertheless, the interpretation of how the subjects of Article 30 (2) and (3) DORA should be incorporated into clauses is likely to give rise to complicated discussions between the financial entity and its ICT third-party service providers.

We therefore suggest, just as the European Commission has done regarding data processing agreements, to draw up standard provisions for DORA Article 30 (2) and (3). This can save financial entities a lot of negotiating time and effort as it is not necessary to discuss each clause separately with an ICT third-party service provider. It will thereby also save costs.

Experience shows that, in certain cases, IT suppliers refuse the right to audit and only agree to provide information about their certification. This is contrary to Article 9 paragraph 3 (h). In such cases, we consider certification by an external independent professional should be sufficient. As a small customer, it can be hard to include the requirement from Article 9 paragraph 3 sub h in the contracts of a ICT third-party services provider. In that case, it is impossible to become DORA compliant.

The ESAs require an independent audit report to select ICT third-party service providers. While the use of independent sources is a good practice that pension funds try to use in most cases, it is not always possible to find publicly available independent assessments. In such cases it would cost extra resources to get an independent review. We point at the possibility of financial entities to perform a review inhouse. We therefore suggest to make independent audit voluntary.

Pension funds outsource most of their core activities. DORA Recital 21 points at this practice. That means that pension service providers perform a review of ICT third-party service providers. In our view, they are able to provide a sufficient level of assurance.

Question 8: Is article 10 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

* 8b. Please provide your reasoning and suggested changes.

Article 10 is clear and relatively appropriate. Monitoring compliance with contractual agreements is already a common practice within the pension sector. However, as mentioned with regards to Article 5, pension funds often outsource managing ICT third-party providers to their main processor/ICT provider. It would therefore be helpful if this could be delegated to the main processor. Implementing alternative measures for DORA compliance purposes would result in unnecessary administrative overhead and adversely impact the legal relation between pension funds and the main processors.

The ESAs require the use of independent sources to assess the ICT third-party service provider. While the use of independent sources is a good practice that pension funds try to use in most cases, it is not always possible to find publicly available independent assessments. In such cases it would cost extra resources to get an independent review. We point at the possibility of financial entities to perform a review inhouse. We therefore suggest to make independent review voluntary.

Pension funds outsource most of their core activities. DORA Recital 21 points at this practice. That means that pension service providers perform a review of ICT third-party service providers. In our view, they are able to provide a sufficient level of assurance

Question 9: Is article 11 appropriate and sufficiently clear?

- ○ Yes
- ◉ No

* 9b. Please provide your reasoning and suggested changes.

Article 11 is clear and partially appropriate. This is considered good practice to be implemented. However, as mentioned with regards to Article 5, pension funds often outsource managing ICT third-party providers to their main processor/ICT provider. It would therefore be helpful if this could be delegated to the main processor. Implementing alternative measures for DORA compliance purposes would result in unnecessary administrative overhead and adversely impact the legal relation between pension funds and the main processors.

Contact

Contact Form