DORA: public consultation on the second batch of policy products.

Deadline: 4th of March

Background: Cboe Europe B.V. (CEBV) is pleased to be able to respond to these consultations as they relate to the proposed technical standards specifying:

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

ii) the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents as well as draft Implementing Technical Standards on the standard forms, templates and procedures for FE to report a major incident and to notify a significant cyber threat (RTS and ITS on major incidents).

We note that the majority policy products related to the second batch are highly prescriptive in nature and provide valuable input in support of the level one requirements of DORA. However, we find the level of specificity set out in the RTS on subcontracting problematic as it does not appear to allow firms to apply proportionality when considering how to address and comply with the obligations set out in the technical standards. The RTS and ITS on major incidents also provide challenges in terms of timeliness on the reporting of major incidents. We believe that these requirements might interfere with incident management & resolution, while adding little value in terms of risk management. In addition, CEBV invites ESAs to consider higher flexibility in the deadline of the application of DORA and associated technical standards given the level of prescription of the policy drafts and the introduction of multiple requirements outside the FE's direct control.

Contents

RTS on subcontracting ICT services

General observations

To enhance coherence and promote clarity in interpreting the RTS on subcontracting ICT services, CEBV considers it advisable to incorporate explicit references throughout the text underscoring that the RTS pertains solely to the subcontracting arrangements concerning ICT services that directly support critical or significant operational functions, or material parts thereof, in full alignment with the mandate provided under Article 30(2)(a) DORA.

Across various provisions, the RTS call for a high degree of oversight by FE in regard to their relationships with ICT third-party service providers (ICT TP). While engagement by FE with ICT TPs is a key element of maintaining the relationship with a third party, the requirements related to the relationship between FE and ICT TP - and subsequently their sub-outsourcing partners, appear overly broad. Compliance with such requirements would impose a significant operational burden on FE, and may cause potential conflicts between FE and ICT TP.

Recital 10 of the RTS is confusing as to how it is applicable in practice: it is mentioned under Article 3 (*risk assessment regarding the use of subcontractor)* that risk assessments are to be performed by the FE), but it is to be addressed via a standard clause to be included in the contract between the third party provider and the subcontractor (and not mentioned in article 4 which is about the contractual clauses). In addition, Recital 10 is problematic when it imposes how third parties should assess subcontractors' risk via a contractual clause. Apart from this not being proportional, Recital 10 seems to be referenced in Article 3 (regarding the risk assessment of the use of subcontractor) instead of Article 4 (that establishes the conditions for the contractual agreements when there is subcontracting for critical or important functions). This is unclear and prone to different interpretations.

Overall, the draft RTS are highly prescriptive leaving little room for FE to apply proportionality when considering how to address and comply with the obligations set out in the technical standards. In addition, there is no specific reference within the Articles as to when the financial entities can exercise and interpret requirements in a proportionate manner. In our view, Article 4 of DORA is not sufficient to clarify the application of proportionality.

Question 1: Are articles 1 and 2 appropriate and sufficiently clear?

CEBV believes it is advisable to introduce an initial provision (e.g. another first article) including a clear reference to the subject matter and the overarching scope of the RTS, to ensure a comprehensive understanding of the scope of the RTS.

With regard to Article 1, clarifications as to the necessity to carry out the risk assessments prior to entering into contractual arrangements with an ICT TP on the use of subcontracted ICT services would be welcomed. It could be desirable to specify that the FE bear the responsibility of assessing these requirements. Additionally, the possibility to merge the requirements set out under this Article with the ones mandated under Article 3 of the same RTS should be considered, to ensure FE have a clear understanding of all applicable requirements.

Moreover, we would request not to include in the definition of subcontracting those cases when ICT services supporting critical or important functions are provided from the parent company to a

subsidiary or the reverse. We consider that requesting a parent company to fulfil the requirements included in points from (a) to (i) of paragraph 1 – as well as to conduct the periodic review defined in paragraph 2 – when subcontracting a subsidiary, or the reverse, would represent an unnecessary and disproportionate administrative burden and is inappropriate for entities which are belonging to the same group.

Question 2: Is article 3 appropriate and sufficiently clear?

Concerning Article 3 overall, CEBV observes that the blending of different requirements, related not only to risk assessment criteria, but also to due diligence requirements and contractual provisions, results in a lack of clarity and coherence. As this may potentially hinder the effective implementation of the prescribed risk assessment process, it could result in FE finding it more difficult to establish the mandated measures to verify suitability and reliability of subcontractors.

CEBV suggests examining the possibility to incorporate under Article 3(1) the criteria delineated under Article 1, to ensure clarity for FE as to their obligations.

Moreover, providing a clear framework where contractual provisions are considered separately from risk assessment consideration would be desirable. CEBV specifically notes that the considerations included under letters b), c), and i) of Article 3(1) RTS may be best included under Article 4 as they describe provisions to be addressed within the context of contractual determinations.

As mentioned within the "General Remarks and Observations," it is essential to clarify that the assessment pertains specifically to subcontracted ICT services supporting critical or important functions, avoiding ambiguity in interpretation.

It is often the case that ICT TP are not FE subject to DORA compliance (or other financial regulations) and therefore are not necessarily subject to due diligence and risk assessment requirements vis-a'-vis their own service provider. Further consideration of proportionality should be given to letters a), c), and d) of Article 3(1) RTS with the purposes of addressing this disparity, whilst keeping into consideration that FE's lack regulatory authority to demand compliance with these requirements from ICT TPs regarding their subcontractors.

With regard to Article 3(1) a), last sentence, the participation of ICT TP supporting critical of important functions in FEs' operational reporting and testing may be separated as an independent criterion, to ensure clarity and specificity.

With regard to Article 3(1) b), CEBV would like to note that it may be very complex for FE to have such a degree of influence and/or involvement on the decision-making process of any third party that the FE be involved in decision-making related to subcontracting. This requirement raises concerns about external interference, as it does not reflect actual decision-making processes within either FE nor service providers (both ICT TP and their sub-outsourcing partners). Therefore, CEBV strongly recommends reviewing this requirement with a focus on its practical implement ability. In the same light, with regard to Article 3(1) c), CEBV questions whether FEs do have the possibility to influence materially the contractual arrangements between ICT TP and their own contractors – as well as the proportionality of this requirement. A notification duty for ICT TP to FE regarding changes in subcontracting arrangements supporting critical or important functions would be a suggested alternative solution.

With regard to Article 3(1) d) and e), CEBV considers these to be duplicative of requirements already covered under Article 28(4) DORA and therefore potentially redundant but otherwise introducing

unnecessary complexity. As simplicity and proportionality should be prioritised to facilitate comprehension and implementation, CEBV recommends avoiding the inclusion of these criteria in the final draft RTS.

Question 3: Is article 4 appropriate and sufficiently clear?

CEBV generally understands and supports the provisions included under Article 4. However, the following considerations are noted.

With regard to Article 4 a), the current wording requires ICT TP to monitor all their subcontracted ICT services supporting critical or important functions. However, the language included in Article 1 suggests that this would remain an obligation of the FE. Clarification is sought regarding the division of responsibilities to ensure consistency and avoid ambiguity but also to ensure proportionality. It is questionable whether verifications carried out by both the FE and ICT TP would be necessary. With reference to Article 4 in general, but also specifically to the provisions set under letter c), and e), CEBV would like to remark that FE lack regulatory authority to require ICT TP to create internal procedures and processes to assess risks related to their own sub-contractors.

With regard to Article 4(e), CEBV anticipates that further clarity may be sought by ICT TP as to the expected manner in implementation monitoring and reporting requirements and thus queries the usefulness of this requirement.

With regard to Art. 4(f): From a commercial perspective, the acceptance of this proposition (to ensure the continuous provision of the ICT services supporting critical or important functions, even in case of failure by a subcontractor to meet its service levels o to ensure the continuous provision of the ICT services supporting critical or important functions, even in case of failure by a subcontractor to meet its service levels) is unrealistic and poses a very high degree of difficulty for third-party ICT service providers from a practical perspective, necessitating substantial financial costs on their behalf even if continuous provision of services could be guaranteed (which we doubt). We believe the costs incurred would be passed through to the financial entity and would be materially impactful to the viability of engaging the service provider in the first place. Implementation of this clause would therefore be inappropriate and unrealistic leaving aside how it might actually be complied with in practice.

With regard to Art. 4(i): From a commercial perspective, requiring subcontractors to grant audit and access rights to the financial entity equivalent to those of the ICT third party service provider is unrealistic. It is highly unlikely that subcontractors will accept this proposition, which is burdensome, and potentially conflicting with their existing confidentiality obligations to the ICT TP. CEBV suggest a more proportionate approach, focusing on cooperation and oversight mechanisms which may facilitate agreement.

With regard to Art. 4(j): The acceptance of termination rights in case the provision of services fails to meet required service levels by subcontractors presents a considerable challenge for third-party service providers and is an inappropriate remedy for most types of service level breaches. Financial entities will already have termination rights for breach of contract which would be triggered by material, repeated and large-scale service levels breaches. This point is also commercially unviable as service providers will either reduce service level coverage and/or raise prices to cover the additional risk. Accordingly, the termination rights should be limited to those outlined in Article 7.

Question 4: Is article 5 appropriate and sufficiently clear?

Beyond observing certain ambiguities, overall CEBV questions the proportionality of Article 5 and whether these requirements will be able to support the creation of implementable standards.

Article 5(1) stipulates that FE must "fully monitor the ICT subcontracting chain and shall document it." Whist CEBV notes that the mandate set under DORA is not complied with as the reference to *subcontracting supporting only critical or important functions* is missing, the extent of monitoring and documentation necessary for compliance remains uncertain. For instance, it is unclear whether merely identifying the entities involved in the subcontracting chain of relevant critical and important functions would suffice, or if there is an obligation to monitor and document the operational aspects and dependencies within the chain comprehensively. CEBV considers this requirement very difficult to correctly understand but also not lending itself to concretely useful purposes: understanding the reasons for criticality concerns and concentration risks is a sufficient exercise. We do not consider this clause to have sufficient clarity and is an inappropriate obligation. The concept of “fully monitor” is ambiguous and the obligation to document is also undefined. We do not believe financial entities can legally or in practice fully monitor a subcontracting chain and interpose themselves in the any existing contractual relationships to which they are not party.

Moreover, the wording used causes interpretative issues as it refers to monitoring, which normally takes place after third party relationships have been established, and documenting, which instead is a process carried out both during the due diligence phase and throughout the monitoring. Clear delineation of how Article 5 interacts with existing regulatory requirements under this RTS (referring to Article 1, 3, and 4 specifically) would enhance coherence and facilitate compliance efforts for FE.

Regarding Article 5(2), CEBV notes that the requirement to track and review (directly or indirectly) the performance of sub-contractors (even via ICT TP) lacks proportionality and requires the mandated entity/entities to increase their number of staff to unrealistic levels for practical implementation. CEBV further emphasizes that incidents or other indicator of unsatisfactory service provision should be solely managed between service provider and service recipient. While CEBV acknowledges the usefulness of KPIs as essential metrics for assessing performance, identifying potential risks, and ensuring compliance with contractual obligations, it remains very questionable whether FE should be subject to an obligation to practically align their monitoring and oversight practices, incorporating these requirements into their processes also vis-a’-vis service providers of ICT TP. This is deemed as disproportionate, also to the potential advantages available to FE.

The way the financial entity may effectively review contractual documentation between ICT third-party service providers and subcontractors lacks adequate clarity and is inappropriate given the financial entity is not a party to that agreement. Moreover, due regard must be given to privity of contract and confidentiality considerations integral in such contractual arrangements between the contracting parties. For these reasons this clause is inappropriate and potentially may place the service provider in breach of confidentiality obligations it owes to its sub-contractor.

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

CEBV notes again that it would be beneficial to clarify whether the expectations outlined in Article 6 exclusively concern subcontracting arrangements supporting critical or important functions of ICT TP.

With regard to Article 6, CEBV questions whether it is practically feasible for FE to retain such a level of interference in the affairs of ICT TP (or any third-party entity for that matter): this appears to be a substantial issue and will encounter resistance from the industry. While CEBV appreciates it is essential for FE to safeguard against risks, it is extremely important to recognize certain boundaries. Article 6(3)

entails significant control over the TP's business operations by potentially various FEs, which not only does not align with the authority granted to FE and is anticipated to encounter resistance. CEBV also invites the ESAs to assess the compatibility of the proposed Article 6(4) with local contractual civil law rules, including with non-disclosure agreement and confidentiality provisions. Certain aspects, particularly those pertaining to subcontracting changes, may need to be reviewed to ensure alignment with existing frameworks and practices.

As mentioned, each ICT TP may engage with multiple FEs, each with distinct requirements and preferences. This diversity in expectations could pose challenges in reconciling conflicting demands placed on ICT TP. Therefore, Article 6(4) may not be practicable in addressing the complexities arising from multi-partner engagements. Given the complexities highlighted above, it is advisable to retain only the provisions related to information rights following changes in the relationships between ICT TP and their service providers as well as the conditions outlined in Article 7 concerning termination of the contractual arrangement. This approach would streamline the regulatory requirements and focus on critical aspects pertaining to subcontracting and termination.

RTS and ITS on major incidents

Question 1: Do you agree with the proposed timelines for reporting of major incidents? If not, please provide your reasoning and suggested changes.

Timelines are on the short side, which potentially puts pressure on classifying incidents as major, due to reporting requirements. When a major incident applies, the reporting requirement might hinder the process of solving the issue, as the focus is shifted to documenting and explaining, rather than resolving the issue. Hence, we suggest that the proposed timelines for reporting of major incidents are extended with the aim to remove the four-hour initial report requirement. Alignment with NIS 2 and GDPR's incident reporting frameworks is deemed appropriate in our opinion. This implies that the requirement to provide an initial report within four hours is replaced by the requirement to submit this report without undue delay from the moment of classification of the incident as major, but no later than 24 hours from the time of detection of the incident becoming aware of the major incident.

Question 6 – Do you agree with the proposed reporting requirements set out in the draft ITS? If not, please provide your reasoning and suggested changes.

We acknowledge that the ESAs has arrived at the view that the reporting should be on solo basis only (para. 29 of the consultation paper), which is fully in line with Article 18(1) of DORA (Regulation (EU) 2022/2554). We also appreciate that financial entities will be allowed to submit all notifications and reports in 'one' submission with a more streamline environment (as per Article 2 of the draft ITS).

However, we would like to highlight a potential 'dual' submission scenario where, according to Article 27b of MiFIR, an investment firm or a market operator operating a trading venue may also provide the DRSP services. Once a major incident happens, a financial entity may need to submit two incident reports to two competent authorities (namely, one to NCA and another one to ESMA).