German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

Public consultation on draft RTS to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions (JC 2023-67)

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Frank Trojahn
Telephone: +49 30 20225-5513
E-mail: frank.trojahn@dsgv.de

Berlin, 2024-02-27

Coordinator:
German Savings Banks Association
Charlottenstraße 47 | 10117 Berlin | Germany
Telephone: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

Comments Public consultation on draft RTS to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions (JC 2023-67)

Question 1. Are articles 1 and 2 appropriate and sufficiently clear?
No, the article is not sufficiently clear.
Art. 1 is not clear. If it is a proportionality clause that allows simplified implementation for less risky/complex subcontracted services, this should be clarified. It should be added that the scope of the respective subcontracting can be included in the consideration. A significantly simplified implementation of the requirements should be permitted for contracts with lower volumes.

Art. 1 e): please always use the level 1 terms to avoid misunderstandings:
intragroup provider instead of "part of the same group of the financial entity"

Art. 1 f): This issue and the handling of corresponding risks is sufficiently dealt with in the context of exit strategies (Art. 28 (8) DORA). The point could be omitted here.

Question 2. Is article 3 appropriate and sufficiently clear?
No, the article is not sufficiently clear.
Proportionality: No explicit proportionate and risk-based approach is applied in the RTS. The ESAs assume that: (i) all ICT services that support critical or important functions have the same level of risk (or importance) to a FE; and (ii) all subcontractors associated with an ICT service that supports a critical or important function or supports essential parts of it are considered equivalent, regardless of their role and potential impact on the provision of the services.

Proposed amendment: Introduction of a materiality threshold. FEs would then be able to identify and monitor the material risks of subcontractors whose disruption or failure could lead to a material impact on the provision of services.

Art. 3 (1)
c) The disclosure of contractual conditions to subcontractors is problematic. Proposed amendment: It should be sufficient to check whether the use of subcontractors does not impair or hinder the fulfilment of the ICT service provider's contractual obligations towards the FE.
e) We propose to delete this point: Otherwise this would lead to a disproportionately high level of complexity at the FE for sometimes very specialised tasks. Alternatively, external audit certificates from auditors or the results of pool audits should be accepted as sufficient evidence.
f) Delete the step-in-rights option, as this is misleading, or specify whether step-in risks are meant here.
g) Are we talking about geopolitical risks such as war, instability, etc. or are we essentially talking about the transfer of data to third countries? If the latter is the case, this is already dealt with in existing regulations such as Data Reg and GDPR. Cf. Art. 68d of the existing EBA outsourcing guidelines.

Question 3. Is article 4 appropriate and sufficiently clear?
No, the article is not sufficiently clear.
Art. 4: Implementation must be contractually agreed between the financial institution and the ICT TPP. In some cases, some points may not be fulfilled by the subcontractor in accordance with the contract: Termination of the contract with the ICT TPP solely due to individual problems with some subcontractors has huge consequences for the financial institution. Short-term implementation is not possible, for example, due to a lack of alternatives or very expensive exit plans. In these cases, risk assumption should be authorised on the basis of a

risk assessment.

f) A completely uninterrupted provision of services will not be possible in all cases and is not absolutely necessary. Instead of ""to ensure the continuous provision ... ", it should read "to ensure the provision of ICT services without serious disruption".

g): The plans themselves cannot and must not be passed on to the subcontractor. The service level requirements from the contingency plans relevant to the subcontractor should be passed on, see EBA Outsourcing Guidelines, 75 g, i and l

h): is the complete requirement for the highest security standards pursuant to Art. 28.5 DORA meant? The chain of references is not entirely clear, as only a general reference is made to Art. 28.10 DORA (and thus indirectly to Art. 7.1.a RTS 28.10 "Information security standard"). We recommend a risk-oriented categorisation option for the security requirements for the subcontractor.

i): The word "at least" is not comprehensible. Why should the FE require more extensive audit and access rights for the subcontractor than for the ICT service provider itself? We recommend deleting "at least".

Question 4. Is article 5 appropriate and sufficiently clear?
No, the article is not sufficiently clear.
Art. 5.1: It is unclear what the monitoring involves and how it should be carried out if the FE itself has no contractual relationship. It is also unclear what is meant by the subcontracting chain and how far this monitoring should extend - see previous comments. We do not consider a direct monitoring between the FE and the subcontractor to be practicable. In our opinion, the ICT-TPP must check compliance itself (e.g. via its own audits) and, if necessary, confirm this by means of a certificate / external audit certificate. It is unclear where the boundary/distinction to EBA-GL 2019/02 lies with regard to forwarding. The documentation requirement appears redundant with the maintenance of the information register 28.9 DORA, therefore delete or clearly refer to it.

Art. 5.2: Reviewing the subcontracting documents is difficult or impossible for various reasons:
1. legally: a contract between 2 parties (ICT-TPP and subcontractors) is an internal document of these two parties and cannot/may not be disclosed so easily (secrecy, possibly internal price agreements, confidentiality, personal data)

2. consequently, FEs would also have to have a right to inspect the contract documents throughout the entire chain (i.e. between subcontractor rank 2 and subcontractor rank 3), which seems impossible. We therefore recommend deleting Art. 5.2 from the requirement.

Question 5. Are articles 6 and 7 appropriate and sufficiently clear?
No, the article is not sufficiently clear.
Art. 6: Proposal to delete, as it would mean an overfulfilment of DORA. Art. 30.3.b DORA only requires a "notification" of ICT-TPP in the event of developments with a significant impact, but does not provide for a "veto right". In this respect, Art. 6 of the RTS would require more from subcontractors (rank >1) than

from the actual ICT-TPP (rank 1). The FE should have the right to be informed of significant changes in the subcontractor chain. However, it is unrealistic that the FE can enforce a right of veto on the appointment of a new subcontractor. The article should therefore be deleted. Alternative: Addition of opening clauses to develop other procedures for risk limitation.

6.1: Material changes to subcontracting arrangements is not a clearly defined term and is therefore very open to interpretation. The reference to Art. 1, on the other hand, is clearly defined and should be formulated as a criterion for the relevant changes. Furthermore, we recommend including a "reasonable" lead time for the period of advance notice.

6.2: The objective of this requirement is not clear. Why should the FE be obliged to inform the ICT-TPP of the result of its risk assessment? In our view, this can only make sense in individual cases, e.g. as part of a justification in the event that the FE raises objections to the use of the subcontractor.

6.3 and 6.4: A FE cannot contractually demand that a subcontractor in the chain does not carry out or modifies changes (this would be a toggle contract for the entire chain, however a subcontractor is usually obliged to several clients). Therefore, the requirement can only be interpreted in such a way that FE expresses at most its objections to changes to the subcontractor and, if necessary, makes use of its special right of cancellation in the event of non-implementation. In this respect, Art. 6.3 and 6.4 cannot be a contractual requirement. We recommend deleting this passage.

6. Do you have any further comment you would like to share?
No comments.