German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

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 *Lobby Register No R001459 EU Transparency Register No 52646912360-95*

Contact:
Berit Schimm
Telephone: +49 30 2021- 2111
E-mail: b.schimm@bvr.de

Berlin, 2023-09-08

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks.

Coordinator:
National Association of German Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-deutsche-kreditwirtschaft.de

Comments on 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

	Question	YES/ NO	Comments GBIC
Q1	Are the articles 1 and 2 regarding the application of proportionality and the level of application appropriate and sufficiently clear?	No	Not sufficiently. For credit institutions and investment firms already subject to EBA, it would have been better if the ESAs had simply given these firms the option of extending the existing EBA Outsourcing regime to ICT Services (non-outsourcing) supporting to critical and important functions. i.e. a shortcut to compliance for those who have already implemented the EBA requirements and can therefore extend this in scope. The DORA approach seems to be more prescriptive in the "how"- mandating that this is all through explicit reference in the ICT policy. Art. 1: • The provisions only refer to increased complexity or risk elements. Proportionality considerations should be added (see e. g. Art. 4 and Art 28.1 (b) DORA and Section 1 of EBA/GL/2019/02). • "whether the ICT third-party service providers are part of the same group of the financial entity". Please use the term 'ICT intra-group service provider' defined in DORA, because this definition takes into account groups in the meaning of "financial entities belonging to the same institutional protection scheme". Intra-group providers are not an element of increased risk but just a distinguishing factor in risk profile. • We don't agree with the location of TPP or its parent company as a factor of increased risk on basis DORA has considered oversight of third country CTPPs. Art. 2: • A consistent application of the policy in all group members is reasonable in principle. However, individual situations should allow for differentiation among group members. Consistent should therefore not have to mean completely identical. Furthermore subsidiaries that are not related to financial services - for example are responsible for facility management - do not have to fully implement these requirements. Amendment: Please change the phrase "parent shall ensure that" into "shall endavour" in the sentence: the parent undertaking that is responsible for providing the consolidated or sub-consolidated financial statements for the group shall endavour that the policy…" • The article should address also how EU parent undertakings that belong to a third country group could meet the requirement also by relying on groupwide arrangements of the third country group.
Q2	Is article 3 regarding the governance arrangements appropriate and sufficiently clear?	No	Generally: Requirements seems to be too high for material subcontractors. • Art. 3.5: Resources of the service provider must be adequate with the contractually agreed compliance

Comments on 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

			requirements regard to the mandated services only, not with overall compliance of the financial entity. Amendment: Delete "all" and add "regard to the mandated services" in the sentence: "… the policy referred to in paragraph 1 shall foresee that the financial entity assesses that the ICT third party service provider has sufficient resources to ensure that the financial entity complies with its legal and regulatory requirements regard to the mandated services." • Art. 3.8: It should be made clear that an independent review is not only possible by the financial institution, but that independent reviews by the service provider's internal audit department can also be used (see Article 7 (3) (c) RTS). • Art. 3.9 (c): It should also be specified how ICT service providers are to cooperate with regulatory authorities and the scope of possible cooperation. Furthermore, it should be specified how to proceed if ICT service providers do not want to agree on this contractually.
Q3	Is article 4 appropriate and sufficiently clear?	No	• Article 4.1 does not define elements to be used for the differentiation of ICT third party service providers in this context.
Q4	Is article 5 appropriate and sufficiently clear?	No	• Art 5.1: We propose to delete the word "and procedures" because it makes the policy too granular. Amendment: "The policy … shall specify requirements, including principles and responsibilities for each main phase of the lifecycle…."
Q5	Are articles 6 and 7 appropriate and sufficiently clear?	No	In practice, it might be difficult to obtain all this information before signing the contract. This could also restrict competition among service providers, as some ICT third-party service providers may withdraw from the financial market if they do not want to disclose such information. • Art. 6.2: Wording: We suggest changing the phrase "risks linked to where the location of the data is processed" in "risks linked to locations where data are processed". • The article should allow the reliance on groupwide assessments where the service recipient belongs to a third country group. In addition, it should be mentioned that EBA-outsourcing requirements expect the management of overall 3rd-Party-concentration risk by FEs. It should be clarified whether this is sufficient to comply with DORA or an ICT-subset concentration risk is needed. • Art. 7.1 (a): If the requirements are also to include arrangements with natural persons and microenterprises, compliance with all of the stated aspects could be difficult. Arrangements with a minor volume should be exempted. We propose to delete "sufficient abilities"; otherwise please provide further guidance. • Art. 7.1 (e): The financial entity will not be able to assess whether the ICT service provider always actually acts in an ethical and socially responsible manner and adheres to human and children's rights; financial entity can only be required to assess whether ICT third party service providers has established processes to ensure this; the reference to "applicable principles on environmental protection" is too broad and doesn't address the DORA

Comments on 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

			resilience aims. This requirement should be deleted, as these requirements will be contained in more detail in the European Directive 2022/0051 Corporate Sustainability Due Diligence Directive (CSDDD). • Art. 7.2: It is unclear what "level of assurance" means, please provide further guidance. • Art. 7.3: It is unclear how this paragraph interacts with Article 7.1 which requires assessment against (a) to (e) while Article 7 (3) does explicitly not. Please provide further guidance. From an internal-audit-perspektive further clarification is needed on Article 7(3)(c)(i) & (iv).
Q6	Is article 8 appropriate and sufficiently clear?	No	• Art. 8.1: It should be defined in more detail what is meant by conflicts of interest through the use of third-party providers. Please provide further guidance. • Art. 8.2: We propose to delete 8.2. There should no additional requirements for this special type of provider are made. A mandatory requirement to set intra-group conditions at arm's length within a delegated regulation is legally questionable, as this would interfere with entrepreneurial freedom of decision. We did'nt see the connection of the requirement "arm's length" to digital operational resilience questions and no conflicts of interest. The term is also unclear and compliance with this provision would be verifiable only to a limited extent. Verification can always be very complex and time-consuming e.g. assessment of fair market price.
Q7	Is article 9 appropriate and sufficiently clear?	No	Generally: We note that it is difficult for a financial entity to enforce individual contractual requirements with monopoly or oligopoly vendors such as Microsoft. Specific comments: • Article 9.1 last sentence is very vague. • Art. 9.2: The Interaction between Article 9.2 and Article 3.9 is unclear. The wording of the requirement could be misunderstood to mean that all audit types (a) and (b) must be applied to one service provider, which would be inappropriate. Furthermore, (b) could be understood to mean that the audit must necessarily include a threat-based penetration test. This goes beyond Art. 26 (1) DORA. Not all financial companies are required to conduct threat-based penetration tests. Therefore, we ask for clarification with reference to Art. 26.1 DORA or deletion of the insertion regarding penetration tests. • Art. 9.3: If the bank is satisfied corresponding to 9.3 ((a) to (h) are fulfilled), especially the internal audit function of the ICT third-party provider fulfills the requirements placed on the bank's internal audit, then the bank should be allowed to dispense with own audits. The requirements (a)-(h) can also be covered by a suitable proof of function (i.e. a third party checks the audit activity at the service provider). • Art. 9.3 (d): What is the difference to Article 9 (3) (b)? We suggest deleting (d) or provide further guidance. • Art. 9.3 (g): For multi-client service providers, these requirements are not enforceable. It is suggested that internal or external audit findings of the service provider result in an obligation to extend the scope.

Comments on 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

Q8	Is article 10 appropriate and sufficiently clear?	No	• Art. 10.1: it is unrealistic to expect a ICT third party service provider to agree to comply with the policies and procedures of each of its service recipients. We propose to delete the part of the sentence "and the compliance of the ICT third-party service providers with the financial entity's relevant policies and procedures" • Art. 10 (2) (e): The requirement for audits and independent reviews (e) is already included in (b) and should therefore be deleted. Otherwise, it needs to be clarified (which legal requirements, which policies). • Art. 10.4: The determination of measures is usually regulated on an individual service provider basis in other documents and should therefore not be a mandatory part of the Policy. We therefore request that ''appropriate measures'' be reworded as ''possible measures''.
Q9	Is article 11 appropriate and sufficiently clear?	No	The necessity of an exit strategy should not be demanded in a blanket manner but must be assessed under risk aspects. In particular, in the case of intra-group outsourcing and outsourcing within financial networks (cooperation of institutions with joint service providers), an exit strategy is generally not necessary. In this case, the ownership structure ensures compliance and continuity of service. There are no plausible alternatives in short or midterm. In the information register, the specification of an alternative provider is rightly not required for intragroup-Provider. Text proposal analogue to EBA-Guidelines on Outsourcing: "The policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers shall include requirements for a documented exit plan where such an exit is considered possible taking into account possible service interruptions or the unexpected termination of ICT services."