German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

Consultation on Draft Implementing Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers

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 Implementing Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers

	Question	Comments GBIC
Q1	Can you identify any significant operational obstacles to providing a Legal Entity Identifier (LEI) for third-party ICT service providers that are legal entities, excluding individuals acting in a business capacity?	Legal Entity Identifier (LEI) goes beyond current industry requirements and practices. The proposed approach does not reflect existing limitations of LEIs in the supply chain and overstates the general usefulness of LEIs to firms' TPO programs. The collection of the LEI code causes additional work for both the institution and the service providers. The LEI code should not be the only possibility for the identification of a service provider that is a legal entity. An LEI should therefore not be mandatory for all companies. For smaller legal entities or unincorporated firms, the ID number of the national commercial register number should be sufficient. We therefore recommend that Article 4(7) of the ITS be revised to: "Financial entities shall use a valid and active legal entity identifier (LEI) to identify their ICT third-party service providers, if available. If LEI isn't available financial entities should use another unique code to identify the ICT third-party service providers (i.e. Corporate registration number, VAT number, Passport Number, National Identity Number)." Analogue Article 4(8) (and delete "and maintain"): "When an ICT service provided by a direct ICT third-party service provider is supporting a critical or important function of the financial entities, financial entities shall ensure through the direct ICT third-party service provider, that, all the material subcontractors, with exception of those who are individuals acting in a business capacity, shall procure a valid and active legal entity identifier (LEI), if available or another unique code."
Q2	Do you agree with Article 4(1)b that reads 'the Register of Information includes information on all the material subcontractors when an ICT service provided by a direct ICT third-party service provider that is supporting a critical or important function of the financial entities.'? If not, could you please explain why you disagree and possible solutions, if available?	We see significant obstacles, as currently this high transparency on specific data (outsourcings excluded) does not reflect a risk-based approach to third-party risk management. We suggest a more detailed definition of the term material subcontractor. In particular, to ensure a uniform understanding and application of the term. Otherwise it could result to an overly broad scope of subcontractors considered material and the application of unnecessary data requirements to these entities, which provide limited value to practical risk management. Amendment: The term material subcontractor should be defined in article 2 or the term should be revised in article 4(1)b and 4 (8) of the ITS as followed: "Material subcontractor – a subcontractor providing a material part of an ICT service provided by a direct ICT third-party service provider supporting a critical or important function and whose disruption or failure could lead to a material impact to service provision." We also see a challenge in practice that this information can be validly presented or collected for the whole chain of material subcontractors. FE's might not have contact / contract to sub-contractors of their providers, hence they would may have to draft new contracts and align them with their service providers to ensure future compliance with requirements for sub-contractors from DORA. In order to limit the application of unnecessary data fields that provide limited risk management or supervisory benefits, it should be assessed whether all detailed information are essential for subcontractors. Only the information that is already required in the outsourcing register para. 54 and para. 55 EBA Guidelines on Outsourcing (EBA/GL/2019/02) should be mandatory. It should be noted that a "transition phase" is needed for existing contracts / providers. In consideration of review phases of existing contracts, a grandfathering of at least 3 years is required. In addition, we propose to apply DORA-requirements for new or re-negotiated contracts from Jan. 2025 onwards.

Comments on Consultation on Draft Implementing Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers

Q3	Are there any significant operational issues to consider when implementing the Register of Information for the first time? Please elaborate.	Maintaining the information in the register to account for all changes to contractual arrangements and all new contractual arrangements is a significant undertaking without clarity on the benefit. Data must first be obtained, existing contracts have not taken this into account, especially since all ICT services (not just for critical and important functions) must be covered. Formal requirements for contracts exist so far only for outsourcing critical and important functions (beyond general contract law). Nevertheless the scope and content of the information register differs considerably from the information in the outsourcing register. That's why it also causes considerable additional work for outsourcing contracts that are at the same time ICT-third party contracts. (see also our comments to Question 12 and 14). ESAs need to give financial entities sufficient time to secure ~~net~~ the new information from third-parties and establish the first version of the register after 1/17/2025 and submit it no earlier than January 2026. If the ESAs/ the Oversight Forum later needs the register information in a~~n~~ uniform electronically format, the corresponding formats would have to be provided as soon as possible. This would ensure that the processes currently being developed would not have to be adapted subsequently on the basis of the formats later determined by the competent authorities. We also encourage the ESAs and NCAs to limit register submissions to an annual cadence; a more frequent submission would provide minimal supervisory benefit given the time needed to aggregate, analyze and action firms' submissions. In case the electronic submission will be executed like for the outsourcing register submission, then based on our experience the tools of ECB or national authorities needs to be completely reviewed since they are currently not tailormade to allow a submission of such large files with many different attributes. The submission template should allow normal excel functionalities (such as filtering and sorting) to enable data quality checks on our provider side. Harmonisation of registers and reporting procedures are absolutely necessary. • Art. 3.1 (b): The provision is not comprehensible. The use of checkboxes with multiple selection options should be possible. • Art. 4.5 The audit trail requirement needs clarification since it is unlikely that any Financial Entity will have a register in this structure. The information will need to collated from multiple sources and reported. In that context, what would be captured as 'significant' within the audit trail, please explain?
Q4	Have you identified any significant operational obstacles for keeping information regarding contractual arrangements that have been terminated for five years in the Register of Information?	This historic information is not relevant for the ongoing monitoring of ICT third party risks in the institution. Similar to the requirements for the outsourcing register, terminated contracts should still be kept for a maximum of one year after termination. The display of terminated contracts of the last 5 years leads to a high complexity of the register and impairs the overall overview. We also request clarification that contracts terminated before 17.1.2025 do not have to be subsequently recorded in the information register.
Q5	Is Article 6 sufficiently clear regarding the assignment of responsibilities for maintaining and updating the register of information at sub-consolidated and consolidated level?	It is not clear what is meant by "sub-consolidated" and "consolidated level" and what requirement is attached to it. In addition, it is not clearly described which information belongs to the two "types" - the "detailed register" at group company level and a register at group level and why the in many parts redundant two registers are needed. It is also not clear whether the supervisor wants to get the group register or the group company register. The responsibility to maintain and update the register of information at sub-consolidated and consolidated level lies with the respective parent undertaking. <u>Therefore the requirement in Art. 6.3 for all subsidiaries is neither necessary nor practicable and should be deleted.</u> Instead, it could be recommended to grant financial entities at subsidiary level a right to insight into parent registers.

Comments on Consultation on Draft Implementing Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers

Q6	Do you see significant operational issues to consider when each financial entity shall maintain and update the register of information at sub-consolidated and consolidated level in addition to the register of information at entity level?	We see "significant operational issues" in the case of keeping an information register and a register for outsourcing with different rules for consolidation (see also comments on question 5 and 14). Such a requirement is neither necessary nor practicable and should be deleted. The division of two registers into legal entity level and consolidated level is very cumbersome. We would expect the supervisory authority to be able to create such a consolidation– if needed - itself - that way we would also avoid any misunderstandings / misinterpretation on duplicated values.
Q7	Do you agree with the inclusion of columns RT.02.01.0041 (Annual expense or estimated cost of the contractual arrangement for the past year) and RT.02.01.0042 (Budget of the contractual arrangement for the upcoming year) in the template RT.02.01 on general information on the contractual arrangements? If not, could you please provide a clear rationale and suggest any alternatives if available?	It is not clear, why the supervisor the information in the context of digital operational resilience needs. In our view, the costs do not represent an ICT risk. Linking the information register with cost and financial data means in many cases extensive efforts. The general risk management processes do not primarily provide for the retrospective determination and maintenance of costs for a past year. This is part of financial controlling. From the Institute's perspective, the aim should therefore dispense the information on costs or limit it (optional fields). Contracts are often not limited to ICT-services only, the costs may contain costs that belong to other kind of services. If kept, this information should only be mandatory for standalone and/or overarching arrangements (but not for subcontractors) and limited to RT.02.01.0041 “budget for past year”. The “budget for the upcoming year” can be increased or adjusted by special projects at any time.
Q8	Do you agree that template RT.05.02 on ICT service supply chain enables financial entities and supervisors to properly capture the full (material) ICT value chain? If not, which aspects are missing?	Nothing is missing, on contrary we are concerned about the proportionality principle and how this is risk based. We would like to point out that it can be difficult to obtain the required information from rank 2 onwards. There is no legal claim for this on the part of the financial service provider against the subcontractors from rank 2. In the event of non-compliance with DORA in these points, this should not result in any negative consequences for the financial service provider. As per our response to question 2, the focus on a service provider’s supply chain should be on material subcontractors, taking into account the actual role they play and potential impact of their disruption. For our first level of providers we have to list nearly everyone (including consultants working in projects, who barely generate any material risk, neither at bank nor industry wide). For the sub-providers we are allowed to leverage on the material ones. Why is this differentiation not applied already on the first level of providers, which would dramatically decrease the number of data sets and would enable FEs and Competent Authorities to focus on the risk facing relationships instead of administration of a data base to full fill formal duties? We also see the starting point in 2025 for the collection of the mentioned information. We request that the formulation of the requirements be guided by paragraph 54 and paragraph 55 of the EBA Guidelines on Outsourcing (EBA/GL/2019/02).
Q9	Do you support the proposed taxonomy for ICT services in Annex IV? If not, please explain and provide alternative suggestions, if available?	General remarks In principle, we welcome a classification of ICT services~~,~~; however, the Annex IV taxonomy is too detailed and partially redundant. The result will be the inclusion of services that do not present the type of risks DORA is intended to address and forces an inappropriate taxonomy on financial institutions. We miss a restriction to those ICT services that are relevant from the core idea of digital operational resilience, see Art. 3 No. 1 DORA. In the strict sense, this relates to ICT systems that either potentially jeopardize the security of network and information systems or that jeopardize the continuous provision of financial services and their quality, including in the event of disruptions. ICT services that do not meet either of these criteria should not fall within the scope of DORA, and thus of this RTS. If the RTS did not make a negative delimitation in this respect, this would lead to an unequal and inappropriate administrative effort, which at the same time would not serve the purpose of DORA. Some ICT services are included in Annex IV that do not represent a digital service provided through ICT systems or are not on an ongoing basis. Management-/ Controlfunctions and pure consulting services, are in principal no ICT Services. Short-term services should be excluded. The taxonomy also lacks a distinction between services provided by ICT service providers and in-house ICT services.

Comments on Consultation on Draft Implementing Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers

		Details to the ICT service Identifiers: • S2/ S3 / S16 / S17 ICT project management / ICT development / ICT-Consulting / ICT risk management and auditing does not constitute ICT services according to the definition in Art 3.21 (DORA / definition of ICT services). • S4 ICT help desk and ICT incident management. A more differentiated view of whether the service supports 1*st*-, 2*nd*- or 3*rd*-level support is recommended. • S7 Data analysis does not constitute an ICT service as defined in DORA. • S8- S10 ICT facilities, Computation and Non-Cloud storage - The definitions should be specified/ the content should be more distinguished. How does S8 differ from S9 – S11. S9 should be also covered by specified S18 to S20; also Hardware related providers (S12). It might be on different level as it is on rental not on providing services of Equipment. • S11 Please clarify which ICT services are meant by "telecom carriers". • S13 Rental of servers is already covered by S9, S10, S12, S8. Transitions Physical devices for rent without support services do not constitute ICT services in the sense of the legal definition of DORA. The definition should be clarified here. • S 14 Please clarify the definition here, pure configuration of hardware does not constitute a digital ICT service. What is meant by business continuity management here? • S1 Software licencing (excluding SaaS) - The use of licensed software "on premises" should be excluded. There is a significant difference and significant deviation in comparison to software operated by an third party-service provider. • S18-S20 Cloud services: The content should be more distinguished. Where are (SaaS)-services provided by conventional full-service providers that do not constitute cloud services in a narrow sense included?
Q10	Do you agree with the instructions provided in Annex V on how to report the total value of assets and the value of other financial indicator for each type of financial entity? If not, please explain and provide alternative suggestions?	Regarding credit institutions, competent authorities already know the indicator via COREP. An additional reporting should not be necessary. It is not clear, why the supervisor needs the information in the context of digital operational resilience. Linking the information register with cost and financial data means in many cases extensive efforts.
Q11	Is the structure of the Register of Information clear? If not, please explain what aspects are unclear and suggest any alternatives, if available?	We already have a requirement to create an outsourcing register. It would be good to align the requirements for outsourcing register based on EBA with the DORA requirements. If not, we need to maintain two different registers as the requirements are not the same. Moreover, splitting the data in so many templates (for the DORA register) is very error prone as it is difficult to ensure consistency of the population. The register is too complex. A merging of templates would facilitate filling (and later provision to the responsible supervisor). For example, general and specific details of contracts should be combined in one template. A simpler solution should be possible, which also allows to indicate multiple services for one service provider (e.g. multiple checkboxes). Function-related information should be kept to a minimum. It should be taken into account that certain contracts e.g. core banking systems can often refer to many functions (or also licensed activities), it does not make sense to repeat contract details for each function. The structure for the sub-consolidated and consolidated level is very difficult to understand. See also our answer to Question 3 and the detailed comments in the separate attachment to ESA's Consultation Feedback DORA RegisterInformation EntityLevel and ConsLevel.

Comments on Consultation on Draft Implementing Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers

Q12	Do you agree with the level of information requested in the Register of Information templates? Do you think that the minimum level of information requested is sufficient to fulfill the three purposes of the Register of Information, while also considering the varying levels of granularity and maturity among different financial entities?	The proposed 108 attributes of the register go far above and beyond a pragmatic approach and the value add is unclear in multiple cases. It is not in line with the proportionality principle that so many data points are required for lower risk procurements. It is much more than what is requested for the EBA outsourcing register. The implementation of the proposed DORA register will require significant FTE resources to i) initially populate it and ii) maintain it on an ongoing basis as well as IT budget to create the correct template pulling data from various sources. For services that didn't support critical or important functions there are much to many details to be reported. We suggest to reduce details in this case to a minimum (see our comments to the register in detail). The purposes of the Register of Information can also be fulfilled with less details. As it has to include all (even smallest) relationships (in projects which high turnover rates), it does not focus on the overall aim - risk and resilience as it is creating to much "noise" in the data. The data points should also be aligned with the purpose of the DORA. The register should only contain data that are relevant to technical stability monitoring and do not disregard the principle of proportionality. Redundancies should also be avoided (such as the EBA outsourcing register mentioned above), because these lead to increased effort and do not offer any added value. Recital (4) 2nd sentence should be reworded. Instead of the blanket wording "financial undertakings should ... supplement'', we propose the wording ''financial undertakings should check for the need to supplement ... ". Furthermore, the goal of achieving a “minimal level of content or harmonisation” is inappropriate and counter to the core objectives of DORA, in terms of harmonising regulatory and supervisory requirements across the single market. Existing outsourcing registers are already prone to divergence and have caused significant resources of financial institutions to be diverted to administrative tasks, including updating different national registers. The result is less time and resources available to address and mature actual risk management and oversight of third parties. We strongly encourage the ESAs to help avoid such divergence in the DORA register, by explicitly restricting any additional data fields to the DORA template by national authorities. Any changes should be agreed to at the EU level and be implemented equally across Member States.
Q13	Do you agree with the principle of used to draft the ITS? If not, please explain why you disagree and which alternative approach you would suggest.	There are not yet sufficient requirements for the reporting format, which is particularly relevant for electronic reporting. Harmonisation of registers and reporting procedures is absolutely necessary. To enhance proportionality, simplifications and streamlining of the register requirements should be considered. Importantly, the principle of proportionality is not adequately applied when its comes to application of enhanced data requirements of ICT services supporting critical or important functions. As currently drafted in RT.06.01.0061, any ICT service supporting a critical or important function is to be treated equally, without reflection on the actual materiality of that ICT service. Without consideration of materiality of the ICT service itself, the register does not apply a risk-based approach. We therefore recommend that a “Yes/No” field is added to template RT.02.02 which will require the financial institution to identify whether the ICT service arrangement is material to the critical or important function. ICT services that indicate “Yes” would then be subject to the enhanced requirements for critical or important functions in the register. Such a design would align with a risk-based approach and specifically with the Level 1 DORA text which notes that a financial institution should focus on the elements such as the criticality or importance of the services supported by the envisioned ICT contract.

Comments on Consultation on Draft Implementing Technical Standards to establish the templates composing the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers

Q14	Do you agree with the impact assessment and the main conclusions stemming from it?	1) The effort is considerable and not cost-neutral to implement. 2) The usual facilitations for LSIs are omitted. 3) The amount of information to be collected exceeds the established procedure, without the added value being apparent. Benefits compared to the effort at the instituts are not recognizable for such extensive templates. With regard to the outsourcing supervisory processes, there should be a regular supervisory review of the type and scope of the register data required. From the Institute's point of view, the parallel maintenance of an outsourcing register and an information register focused exclusively on ITC third-party-services involves a great deal of additional administrative work. Merging the two registers would make things easier. In addition, there should only be one way to submit the registers to the supervisory authority. Otherwise existing systems would have to be extensively and cost-intensively adapted. For example the cost of maintenance of LEI are not considered. Even if these are only 100 EUR per year for the external fees, it has to be handled, updated in registers etc. All providers (ebven smallest ones) will need some, thus this will bring additonal cost to the fianncial ecosystems in millons. This is not in line with proportionality principle: the proposed 108 attributes of the register go far above and beyond a meaningful need to know principle, the proposed approach to the ‘proportionate’ application of the register is flawed / not actually risk-based. This proposed approach overlooks other essential risk-based factors such as the size and complexity of the legal entity or the criticality of the ICT third-party service provided that impact the risk level of the ICT third-party provider portfolio.