German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

ECB Guide on outsourcing cloud services to cloud service providers

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

Contact:
Christina Pfaff
Telefon: +49 30 20225-5427
Telefax: +49 30 20225-5404
E-mail: christina.pfaff@dsgv.de

Berlin, July 12, 2024

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

EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Institution/Company
German Banking Industry Committee (GBIC)

Contact person

Mr/Ms
Ms

First name
Christina

Surname
Pfaff

Email address
christina.pfaff@dsgv.de

Telephone number
+49 30 20225-5427

☐ Please tick here if you do not wish your personal data to be published.

General comments
Regarding the facts that DORA and the supplementary ESA standards lay down extensive and stringent requirements for all entities in the financial sector, which also include cloud services and were developed with the involvement of supervisory authorities, IT and outsourcing experts, etc., we miss a clear statement that the additional expectations in the ECB guide can be implemented in a risk-oriented manner. Proportionality should also apply in this context.

Template for comments

ECB Guide on outsourcing cloud services to cloud service providers

Please enter all your feedback in this list.
When entering feedback, please make sure that:
- each comment deals with a single issue only;
- you indicate the relevant article/chapter/paragraph, where appropriate;
- you indicate whether your comment is a proposed amendment, clarification or deletion.

Deadline:	15.07.2024

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
1	1. Introduction 1.1. Purpose		2	Amendment	The definition of a “critical or important function” differs significantly from the definition as outlined in the EBA Guidelines on outsourcing arrangements as well as under DORA (Art. 3 Sec. 22). According to the draft ECB Guide, critical/important shall be more or less seen from a macro perspective and not just from an individual financial institution’s impact. We do not consider such a different definition to be useful, not least because an institution's risk management can ultimately only take its own perspective. Instead, reference should be made to the DORA definition. The macro perspective is under the remit of the supervisory authorities.	A deviating definition of a “critical or important function” does not make sense, DORA definition should be used.	Pfaff, Christina	Publish
2	1. Introduction 1.1. Purpose		2	Clarification	The definition of an „ICT Asset“ also slightly differs from DORA. Whilst the ECB guide is using "... that is found in the business environment", DORA defines ICT assets as software or hardware assets "in the network and information systems used by the financial entity". If the intended meaning does not differ between the two, we suggest to relate to the existing DORA definition.	The wording should be aligned with DORA in order to avoid extending the current scope of the guide unnecessarily.	Pfaff, Christina	Publish
3	1. Introduction 1.1. Purpose		2	Clarification	The definition of “cloud“, “hybrid cloud“ and „hybrid cloud“ differ from EBA/REC/2017/03 as of 20.12.2017.	The wording should be aligned with EBA/REC/2017/03 in order to avoid extending the current scope of the guide.	Pfaff, Christina	Publish

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
4	Chapter 2.1 Governance of Cloud Services 2.1.1. Full responsibility continues to lie within the institution in question		4	Amendment	For the ECB, Article 28(1)(a) DORA means that institutions that choose to outsource must have the same controls, processes and risk management in place as institutions that choose to retain these services internally. While equivalent controls should be established in principle, for example, an appropriate level of detail should be applied when monitoring the external service provider. Particularly in the case of cloud outsourcing, the level of detail is naturally limited, including with regard to the infrastructure used (server level). Only controls such as access controls or monitoring of system activities should be established. External controls, which are assumed by the cloud service provider, would be physical security, availability of services, data backup and recovery, as well as compliance with data protection regulations, etc.		Pfaff, Christina	Publish
5	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis		4	Clarification	“Under Art. 28 (4) DORA, institutions are required to conduct risk analysis...prior to entering into a new outsourcing arrangement with a CSP. In order to adequately identify ... the institutions should ...” We suggest to replace “institutions should” by “best practice shows ...”	Background to this is the following: Within the framework of the requirements care must be taken to ensure that the institutions do not always conclude contracts with service providers who have already implemented such controls. Normally, service providers set up such controls once they want to work with us. In these cases, the institutions cannot check whether the controls are functional and suitable as part of the pre-outsourcing audit. Therefore, an audit of the controls before outsourcing should not end up on the mandatory agenda of the auditors, and only be considered “best practice”.	Pfaff, Christina	Publish
6	Chapter 2.1 Governance of Cloud Services 2.1.2. Pre-outsourcing analysis		5	Amendment	"vendor lock-in and potential challenges that could arise in the course of identifying an alternative provider if an exit is required"	We suggest to amend the wording as follows: "vendor lock-in and potential challenges that could arise in the course of identifying an alternative provider if an exit is required and possible"	Pfaff, Christina	Publish

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
7	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions		5,6	Deletion	The guide contains several references to the NIS2 Directive, although DORA has been confirmed as lex specialis to NIS2, which could lead to interpretation issues. References in 2.2.1, 2.2.3 and 2.3 (business continuity measures, disaster recovery strategy, ICT security and risk management) are included and all refer to requirements in NIS2 that are set out in more detail in DORA. The Risk Management section in Chapter 6; Articles 24-26 DORA deals with Business Continuity Plans and Disaster Recovery Plans, while the references to Incident Response and Recovery are an integral part of the overall RTS. It is unclear what further regulatory guidance will be added by the inclusion of NIS2 and to what extent this could lead to interpretation issues due to its lack of applicability to financial services. There is a risk that the inclusion of NIS2 could lead to confusion in the financial sector regarding the lex specialis provision. We therefore recommend removing references to NIS2.		Pfaff, Christina	Publish
8	Chapter 2.2. Availability and resilience of cloud services 2.2.1 Holistic perspective on business continuity measures for cloud solutions		5,6	Amendment	The ECB states that a financial company should not use the same cloud service providers for data backup. Furthermore, the ECB states that financial institutions should have backup and recovery procedures in place by default and limit losses int the event of severe disruptions to its business... Instead, we suggest a risk-based approach, which takes any impacting developments (including e.g. changes in the geopolitical landscape) into a broad view. Concerning an exit without cooperation from the CSPs we suggest taking into account that contracted CSPs are legally bound to support an ongoing exit-procedure for the duration of a full year. Negating any support would constitute a breach of contract that would likely jeopardize any given CSP‘s business model, and therefore appears to be highly unlikely. The interpretations go far beyond the DORA and should therefore be deleted or formulated as "may".		Pfaff, Christina	Publish

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
9	Chapter 2.2. Availability and resilience of cloud services 2.2.2 Proportionate requirements for critical or important functions		7	Deletion	The interpretations regarding the ability to bring data back on-prem and regarding portability go far beyond the DORA and should therefore be deleted or formulated as "may".	Smaller banks may not have data centers or on-prem is very expensive, it would make more sense to refer to another technical area (no on-prem) or rather the bank's own risk assessment as a recommendation	Pfaff, Christina	Publish
10	Chapter 2.2. Availability and resilience of cloud services 2.2.3 Oversight over the planning, establishment, testing and implementation of a disaster recovery strategy		7	Deletion	There are a number of assumptions about how a financial institution can test a cloud service provider. The ECB states that financial institutions should carry out spot checks on CSPs (cloud service providers), which would not be proportionate to do for all cloud service providers and where we see challenges in implementation		Pfaff, Christina	Publish
11	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks		8	Clarification	C.f. our comments regarding the definition of critical or important functions (ID #1): How does this relate to the more „institution-focussed“ definition within DORA?		Pfaff, Christina	Publish
12	Chapter 2.2. Availability and resilience of cloud services 2.2.4 Assessment of concentration and provider lock-in risks		8	Deletion	The aspect of scalability should be deleted and rephrased by: "In particular, concentration risks should be assessed not only on the basis of the number and nature of outsourced functions, but an integrated approach of concentration risk which may among others take into account the scalability of the cloud (which allows it to be gradually extended to encompass new functions, with potential effects on concentration risks)"	Scalability cannot be checked in an abstract way if the underlying functions are not clear yet. Therefore, we propose an integrated approach to address the topic holistically, but avoid a lack of clarity by aspects which cannot be adhered to during the assessment	Pfaff, Christina	Publish

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
13	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.1 Establishment of adequate data security measures, such as encryption and cryptographic key management processes		9,10	Amendment	The level of "best practice" is inadequately high especially with regards to cryptographic keys, especially in the light that there are additional means of a similar level of security. "Best practice" should be replaced by “examplary measures“	Some institutions do not use cryptography entirely, but different means like network segmentation to obtain the same level of security.	Pfaff, Christina	Publish
14	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.2 Risks stemming from the location and processing of data		10	Clarification	"Furthermore, the ECB also considers it good practice for institutions to assess additional risks if a sub-contractor relevant for the cloud services is located in a different country from the CSP, while taking into account any risks associated with complex sub-outsourcing chains as outlined in paragraph 25 of the EBA Guidelines on outsourcing arrangements." should be clarified in order to consider risk-orientation and proportionality.	2.3.2 refers to all sub-contractors, although DORA differentiates between subcontractor for critical or important function and others. Especially for non-critical or important functions 2.3.2 para. 3 does not reflect the principles of proportionality. Many banks have more than 100 subcontractors of a CSP which they would then have to assess. In addition there is a discrepancy with data protection laws - so far from a data protection point of view the assessment obligation is only given for the subcontractor in scope, and not holistically for the entire subcontractor-chain.	Pfaff, Christina	Publish
15	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.3 Consistent inclusion of outsourcing assets in an institution’s inventory of ICT assets		10	Clarification	"Classification of all ICT assets" in an up-to-date inventory does not reflect the criticality enough and creates an inappropriate burden. We suggest to include a risk-based approach.	The inclusion of all ICT assets is an immense burden for the reporting entities and does not reflect the rationale behind of identifying the CCSP.	Pfaff, Christina	Publish

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
16	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements		11	Amendment	Risk mitigation of any deviations within this context appears to be a level of scrutiny that exceeds previous expectations, therefore we suggest limiting this to necessary instances.		Pfaff, Christina	Publish
17	Chapter 2.3. ICT security, data confidentiality and integrity 2.3.4 Identity and access management (IAM) policies for cloud outsourcing arrangements		11	Amendment	It may be viable to compare this requirement to standard privileged access management procedures.It should be sufficient that the IAM policy is reflecting cloud outsourcing and is regularly reviewed in the outsourcing agreement	Given the complexity and frequent changes of IAM policies, the reflection ot the exact content in the outsourcing agreement would go beyond the DORA framework. Therefore, only the existence and regular review of the IAM policy should be stated.	Pfaff, Christina	Publish
18	2.4 Exit strategy and termination rights 2.4.1 Termination rights		12	Clarification	C.f. our comments regarding the definition of critical or important functions (ID #1): How does this relate to the more „institution-focussed“ definition within DORA?	Institution focussed: While the DORA definition of ‘critical or important function’ focusses on importance for the operation of an institution, the definition given in the draft ECB Guide refers to ‘services that are essential to the real economy’, therefore setting a much bigger scope. We suggest to refer to the DORA definition only.	Pfaff, Christina	Publish

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
19	2.4 Exit strategy and termination rights 2.4.1 Termination rights		12	Amendment	2.4.1 (2) describes other changes that could also lead to such a reason for terminating for termination, including in particular (iv) relocation... and (vi) change in the regulations applicable... We suggest to add "unless the data is immediately transferred to a host country that also otherwise meets the requirements of the outsourcing agreement".	Background to this is the following: None of these points are within the CSP's sphere of influence. Such clauses must give the CSP an opportunity to perform the contract correctly. Therefore the institutions may not be able to enshrine a corresponding clause in the context of general terms and conditions in a legally effective manner unless at the same time a remedy for the CSP is agreed (e.g. by moving) In a case of doubt it should be sufficient that a service will then be provided by another CSP and not by the institution itself.	Pfaff, Christina	Publish
20	2.4 Exit strategy and termination rights 2.4.1 Termination rights		12	Deletion	Point (iii) ("an excessive increase in expenses under the contractual arrangements that are attributable to the CSP") should be deleted, as it goes beyond DORA and could not be implemented with legal certainty. Extraordinary termination rights in the event of an unreasonable price increase by the service provider should generally be covered by civil law.	delete, as this would constitute an impracticable expectation	Pfaff, Christina	Publish
21	2.4 Exit strategy and termination rights 2.4.2 Components of the exit strategy and alignment with the exit plan		13	Deletion	These expectations go far beyond DORA and should be deleted, as they are neither necessary nor practible. Acc. to Art. 28 (8) DORA: For ICT services supporting critical or important functions, financial entities shall put in place exit strategies. The exit strategies shall take into account risks that may emerge at the level of ICT third-party service providers, in particular a possible failure on their part, a deterioration of the quality of the ICT services provided, any business disruption due to inappropriate or failed provision of ICT services or any material risk arising in relation to the appropriate and continuous deployment of the respective ICT service, or the termination of contractual arrangements with ICT third-party service providers under any of the circumstances listed in paragraph 7.	Art. 28 (8) DORA does not outline a principle-based exit strategy with granular technical exit plans for individual cloud outsourcing arrangements: The exit plan should follow the risk-based approach as outlined in the overall framework of DORA. It has to be realistic and feasible, based on plausible scenarios and reasonable assumptions incl. a timeline which corresponds to the exit and termination conditions.	Pfaff, Christina	Publish

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
22	2.4 Exit strategy and termination rights 2.4.3 Granularity of exit plans		13,14	Amendment	We suggest the following wording (part1): "A dedicated exit plan as referred to in Article 28(8) of DORA should ensure that a supervised entity is able to react quickly to any deterioration in the service provided by a CSP. It is good practice for exit plans to include, as a target, the critical milestones, a description of the tasks or steps and general skill sets that are necessary to perform the exit, and a rough estimate of the time required and the costs involved. Exit plans should be reviewed and tested on a regular basis, bearing in mind the principle of proportionality as described in Article 28(1)(b) of DORA. Supervised entities should at least perform an in-depth desktop review, ensuring that such reviews are conducted by staff who are sufficiently knowledgeable about cloud technologies. Institutions should also review the amount of data and the complexity of the applications that would need to be migrated, thinking about the potential data transfer method, in order to produce meaningful estimates of the time required. Institutions should check that they have the personnel required for their exit plans, allowing for the impromptu allocation of external resources if necessary and, by conducting a walkthrough of the tasks involved, ensure that the proposed tasks outlined in the exit plan can be performed within the previously described bounds."		Pfaff, Christina	Publish

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
23	2.4 Exit strategy and termination rights 2.4.3 Granularity of exit plans		13,14	Amendment	We suggest the following wording (part 2): "For the most critical steps in the migration process, employees' ability to perform their assigned roles in the allotted time should be considered when performing reviews. Supervised entities should check, on a regular basis, to what extent the general skill sets required to perform the tasks set out in their exit plans are represented among staff members, or whether the support of external consultants would generally be needed in order to exit a cloud outsourcing arrangement. The feasibility of each exit plan should be independently verified (i.e. checked by someone who, possibly while still being part of the institution, is not responsible for drafting the plan in question, comparable to in internal audit process)."		Pfaff, Christina	Publish
24	2.4 Exit strategy and termination rights 2.4.4 Exiting under stress		14	Deletion	Conflicting legislation is unlikely to happen without a transitionary grace period. The scenario outlined here appears to be the legal counterpart to the extinction level event described above. Given the legal (and contractual) transitionary periods, it appears prudent to limit the expectations to cautioning institutions against this kind of threat.		Pfaff, Christina	Publish
25	2.4 Exit strategy and termination rights 2.4.4 Exiting under stress		14	Deletion	It should be noted that any kind of outsourcing retains the risk of a contractual party not fulfilling their duties in this way. However, a provision that necessitates a more or less seamless transition away from any outsourced service may put in question the use of cloud services as a concept. We therefore suggest to delete these interpretations because they go far beyond DORA.		Pfaff, Christina	Publish
26	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs		14,15	Clarification	In 2.5, "An institution's internal audit function should ensure that risk assessments are not based solely on narratives and certifications provided by the CSP without independent assessments/reviews and the incorporation of input provided by third parties (e.g. security analysts)." should be clarified.	Audits of hyperscalers should be replaced by regular neutral and independent certification for the services concerned initiated by the hyperscaler and confirmed by the supervisory authorities.	Pfaff, Christina	Publish

ID	Chapter	Paragraph	Page	Type of comment	Detailed comment	Concise statement as to why your comment should be taken on board	Name of commenter	Personal data
27	2.5 Oversight, monitoring and internal audits 2.5.1 Need for independent expert monitoring of CSPs		15	Clarification	Given that the institutions and CSPs work closely together, we suggest limiting additional monitoring to cases in which the institution has reason to believe manipulation has taken place. In addition to this, joint audits should stay on a voluntary basis.		Pfaff, Christina	Publish
28								
29								
30								