CHECKLIST ON ECUC POSITION PAPER 2.1 FOR CSPs

Version 1.0

14. Sep 22

Contact: consultation@ecuc.group

Document: ECUC_Checklist_Sep_2022_v1.0.xlsx

CHECKLIST ON ECUC POSITION PAPER 2.1 FOR CSPs

INTRODUCTION: A CHECKLIST FOR CLOUD SERVICE PROVIDERS

Cloud computing is fundamental to enable the digital transformation of the European financial sector. The objective of the European Cloud User Coalition (ECUC) is to provide and further develop a joint position on common legal, regulatory and technical challenges which Financial Institutions (FIs) need to tackle and solve for while progressing on their cloud adoption journey. These challenges and proposed solutions were outlined in the joint Position Paper and detailed further in the Checklist at hand.

The checklist is designed to be a self-questionnaire for CSPs to verify their own approach regarding the legal, regulatory and technical requirements mentioned in the Position Paper 2.1. It shall allow CSPs to structure their solutions in a manner that matches the legal, regulatory and technical requirements of the financial sector.

According to the Position Paper, the checklist contains the following 5 chapters:
2 - Requirements on Privacy
3 - Requirements on Security
4 - Requirements for Governance and Regulation
5 - Requirements on Contractual Clauses
6 - Requirements on Portability

The checklist is based on the folowing principles:
ECUC does not intend to assess or certify CSPs.
ECUC does not check any voluntarily given answers given by the CSPs for accuracy.
ECUC assumes no liability for any answers given by the CSPs.
ECUC does not implement any technical / automatic data exchange.
The checklist includes an extract of references to the following selected applicable laws, binding regulations and guidelines of competent European authorities.
The Position Paper 2.1 covers the most relevant requirements and these cannot be regarded as being complete. This view applies to the Checklist accordingly.

CHECKLIST ON ECUC POSITION PAPER 2.1 FOR CSPs

EXPLANATION OF COLUMNS

(B) EXCERPT FROM THE POSITION PAPER 2.1:

Copy of the respective subchapter of Position Paper 2.1.

(C) REF. ID:

This is the internal reference ID of each question in the Checklist.
Example: 3.4.1 => the first two positions refer to the chapter and subchapter in the Position Paper 2.1, third position is a follow up number of the question.

(D) QUESTIONS RELATED TO REGULATORY REFERENCE:

The questions are derived from the ECUC requirements based on Position Paper 2.1 and so matched to regulatory requirements (highlighted in column E).

(E) REGULATORY REFERENCE / RECOGNISED STANDARD (examples):

Applicable law:

- DORA: European Digital Operational Resilience Act (Provisional Agreement)
- DATA ACT: European Commission Data Act COD 2022/0047 of 23 February 2022
- ECJ Schrems 2: European Jurisdiction C-311/18 of 16 July 2020
- GDPR: General Data Protection Regulation (Regulation (EU) 2016/679)

Binding regulations and guidelines of competent European authorities:

- BCBS 239: Basel Committee on Banking Supervision´s standard number 239
- EBA/GL/2019/02 (Outsourcing): European Banking Authority revised Guidelines on outsourcing arrangements
- EBA/GL/2019/04 (ICT): European Banking Authority Guidelines on ICT and security risk management
- EDPB Sup. Mea.: European Data Protection Board Supplementary Measures
- EDPB WP 250 GL on pers. Data Breach: European Data Protection Board WP 250 Guideline 01/2021 on Personal Data Breach Notification
- Regulation (EU) 1025/2012

CHECKLIST ON ECUC POSITION PAPER 2.1 FOR CSPs

EXPLANATION OF COLUMNS

Selection of recognised standards (nonexhaustive - when answering the questions, CSP may mention equivalent standards in the comment field):
- AICPA SSAE 18: American Institute of Certified Public Accountants - Statement on Standards for Attestation Engagements no. 18
- BSI C5:2020: Bundesamt für Sicherheit und Informationstechnik (German Federal Office for Information Security) - Cloud Computing Compliance Criteria Catalogue
- CSA: Cloud Security Alliance
- CSA CCM & CAIQ: Cloud Security Alliance Cloud Control Matrix v4.0.5 23 March 2022
- CNCF: Cloud Native Computing Foundation
- ISO: International Organization for Standardization
- ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls
- ISO/IEC 27017:2015: Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019: Information technology - Security techniques - Code of priactice for protection of personally identifiable information (PII in public clouds acting as PII processors
- IEEE 2302-2021: Institute of Electrical and electronics Engineers - Standard for Intercloud Interoperability and Federaton (SIIF)
- ISAE 3402: International Standard on Assurance Engagements 3402, Assurance Reports on Controls at a Service Organization
- NIST: National Institute of Standards and Technology (U.S. Department of Commerce)
- PCI DSS: Payment Card Industry - Security Standards Council

(F) OFFERED/FULFILLED BY CSPs:

CSPs are asked to check realistically the grade of fulfillment for the individual requirement, by selecting yes, "partial" or "no".
In case of selcting "partial" or "no", any explanation including mitigating measures is helpful.

(G) CLOUD SERVICE PROVIDER COMMENT:

Please illustrate the grade of fulfillment with further comments, proofs or references. An explanation is welcomed to every question, even it is not explicitly asked for.

Chapter 2 - Privacy

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 2.1 CSP must provide Personal Data Protection in Accordance with European General Data Protection Regulations					
Data protection in public cloud environments is required to comply with the relevant European data protection regulations, in particular EU General Data Protection Regulation (EU) 2016/679 (GDPR), binding guidance of the European Data Protection Board, relevant European Court decisions, and European member state legislations. Within the EU and the European Economic Area (EU/EEA), GDPR is applicable for both, FIs (data-controller as cloud consumers) as well as for CSPs (data-processor). As data processors, CSPs are independent of their place of business, accountable to provide adequate technical and organisational security and compliance measures in the European market. Such measures should be state of the art, include data protection by design and default, and aim to even go beyond setting the benchmark. Furthermore, European citizens need to be able to trust that their FI take measures to respect and protect their privacy, including both contractual and technical aspects of such a relationship.	Ref 2.1.1	Do your customers unconditional access to documentation of your technical and organisational security and compliance measures for the European market?	GDPR: - Art. 28, 32 EBA/GL/2019/02 (Outsourcing): - Background Para. 44 - Chap. 3 Para. 16 - Chap. 4 Para. 38.b - Chap. 5 Accompanying documents, recital 8		
	Ref 2.1.2	Are these measures state of the art, including data protection by design and default?	GDPR: - Art. 25, 32 - Recital 78 ECJ Schrems 2: - Recital 108		
Subchapter 2.2 CSP should provide supplementary Measures to enable effective GDPR Compliance in 3rd Countries					
With regards to entering into contracts with CSPs established outside of the EU/EEA (3rd countries), the European Court of Justice (C-311/18 Schrems II) declared, that if applied standard contractual clauses ensure a GDPR equivalent environment for the individual, they can be an appropriate tool of transfer. Hence, the data controller (e.g. the FI) needs to ensure that the storage, transfer, and/or processing of data maintains GDPR equivalence and does not increase the risks of, for instance, unauthorised 3rd country processing. However, the outcome of adequacy evaluation and implementing contractual clauses potentially does not achieve a GDPR equivalent level of protection in the country where the CSP is established and/or where the data processing takes place. This is especially a challenge in countries where there are legislative requirements that authorizes public authorities to access data broadly beyond legitimate objective. Therefore, this may interfere with the contractually agreed confidentiality to access any personal data where the FI is the controller and is processed on its behalf by the CSP. The CSP should provide technical and organisational measures that ensure the compliance with GDPR in 3rd countries also.	Ref 2.2.1	Do technical and organisational measures of your organisation ensure an GDPR equivalent protection for personal data in 3rd countries? Please provide more details and references in the comment field.	GDPR: - Art. 44 subseq. ECJ Schrems 2: - Recital 134 EBA/GL/2019/02 (Outsourcing): - Background Para. 37 subseq. - Chap. 4 Para. 72, 83		

Chapter 2 - Privacy

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 2.3 CSPs need to implement basic Security Principles					
In case a 3rd country can request access to personal data, according to the recommendations of the European Data Protection Board (EDPB) and the Standard Contractual Clauses 2021/914 of the European Commission (EU SCC 2021/914), data controllers and data processors should implement additional measures to ensure GDPR equivalent protection in the 3rd country. These technical measures are typically based on the principles of data security, data minimisation, anonymisation or pseudo-anonymisation. In the case of pseudonymisation, the CSP should support an approach where additional information for attribution of personal data to a specific data subject shall remain under the exclusive control of the FI. All CSPs and cloud operating models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) are in scope for these requirements.	Ref 2.3.1	In the case of pseudonymisation, does your organisation support an approach where additional information for attribution of personal data to a specific data subject remains under the exclusive control of the FI?	GDPR: - Art. 28, 44, 46, 32, 25 - Recital 26, 28, 29		
Subchapter 2.4 Cloud Services should facilitate Data Sovereignty by processing Data exclusively in the EU/EEA					
With the declared invalidation of the EU-US Privacy Shield by the European Court of Justice (Schrems II decision), FIs as cloud consumers should be able to apply data localisation to a certain country or geographic region, e.g. EEA. Furthermore, all cloud services should support storing and processing of customer and individual data exclusively in a dedicated country or geographic region e.g. in the EU/EEA.	Ref 2.4.1	Do your cloud services provide data localisation to a certain country or geographic region, e.g. EEA?	GDPR: - Art. 28, 44		
	Ref 2.4.2	Does your organisation provide tools to make data transfers visible, either initiated by the FI or the CSP, for whatever reason, and whether data travel within or outside of the EEA?	GDPR: - Art. 28 Para. 2		
	Ref 2.4.3	Does your organisation provide controls to the FI for validation in case personal data leaves or is accessed outside of the EEA, either knowingly or unknowingly?	GDPR: - Art. 28 Para. 2		
Subchapter 2.5 Global and regional Cloud Services must be made transparent to FIs					
CSP must make transparent what cloud services are operated only globally (so called Global services). In addition, CSP must make transparent if a cloud service necessarily requires transfers and/or processes personal data outside the EU. This information must be publicly accessible at any time, and it must not be limited to cloud services that potentially transfer customer data outside the EU as an essential function of the service. In addition, the CSP must proactively inform their FI customers if they add or alter any privacy and data protection features and/or capabilities as well as region expansion announcements as they are released.	Ref 2.5.1	Does your organisation provide full transparency over cloud services in your system that potentially or definitely transfers and/or processes personal data outside the EEA?	GDPR: - Art. 28 Para. 2, Art. 30 Para. 2		
	Ref 2.5.2	Is this information publicly accesible, even without a contract?	GDPR: - Art. 28 Para. 3.f		
	Ref 2.5.3	Does your organisation proactively inform its customers if you add or alter any privacy / data protection compliance features and/or capabilities for the services, as well as any announcements about new region launches, as they become available to customers?	GDPR: - Art. 28 Para. 3.f		

Chapter 2 - Privacy

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 2.6 Provide robust and multi region-based Global Services					
CSP should ensure that global cloud services are hosted in multiple regions and must not rely on one region only. Alternatively, CSP must be transparent to their customers whether or not global services are localised in a single region.	Ref 2.6.1	Does your organisation provide cloud services declared a global services in multiple regions? Please describe in the comment field which of your global cloud services are hosted in one region only.	GDPR: - Art. 28, Art. 44		
Subchapter 2.7 Contractually agreed Data Processing Roles and Responsibilities must be adhered to by the CSPs					
Although CSPs aim to have differentiated approaches concerning the roles of being a data processor for the FI and a data controller for own interests (e.g. data analytics), ECUC asks CSPs to refrain from any data processing going beyond what has been contracted with respect to the data of the FI. When involving a CSP as 3rd party in the processing of customer data, the FI needs to be confident that the involvement of the additional processing party does not increase the risk of unauthorized processing/access to such data. CSPs also need to ensure that the processing of customer data remains within the limits of the contract with the FI. After contract expiration all data shall be returned and the CSP needs to certify that all data has been deleted.	Ref 2.7.1	Does your organisation offer full transparency on the role of the CSP referring to manage GDPR data (if CSP acts as a Data Processor), on the retention period of data processed, on the type of personal data processed, and if data profiling is done on data processed for each service in IaaS, PaaS or SaaS?	GDPR: - Art. 28 Para. 3, Art. 29 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 83		
	Ref 2.7.2	Does your organisation provide confirmation of customer data deletion following contract termination / expiry?	GDPR: - Art. 28 Para. 3 lit. G		
Subchapter 2.8 CSP should enable FIs to contract with EU based Legal Entities					
CSPs should offer FIs to contract with their legal entities based in the EU. Trilateral contractual relationships between FIs and both, the CSPs EU and non-EU based legal entities, contain uncertainties in terms of "Who is responsible for the control and contractual safeguarding of data transfers to countries outside the EU?" The ECUC regards the CSP EU based legal entities as the primary data processors for the personal data of the FI. If the CSP EU based legal entities send data to non-EU based CSP legal entities, the EU based legal entities are not only in breach of the contract but also act as data exporters, and thus being responsible to perform data transfer assessments and apply standard contractual clauses with their non-EU based entities.	Ref 2.8.1	Does your organisation offer FIs to contract with your legal entities based in the EU?	GDPR: - Art. 28 EBA/GL/2019/02 (Outsourcing): - Background Para. 41 - Chap. 4 Para. 67.a		
	Ref 2.8.2	Will your organisation apply Standard Contractual Clauses between your EU based and non-EU based entities?	GDPR: - Art. 28, 44, 46		
	Ref 2.8.3	When EU based legal entities of your organisation send data to your non-EU based legal entities, will you provide details of the data transfer assessments between these two parties?	GDPR: - Art. 46 EBA/GL/2019/02 (Outsourcing): - Background Para. 37, 41, 46 - Chap. 4 Para 68.d, 68.i		

Chapter 2 - Privacy

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 2.9 CSP must assess the Impact of 3rd Country Transfers					
The CSP must warrant that it has no reason to believe that the laws and practices in a 3rd country of destination, applicable to the processing of the personal data by one of its data importers, prevent such data importers from fulfilling its obligations under these clauses. This includes requirements to disclose personal data and/or measures authorising access by government authorities. It has to take due account of the specific circumstances of the transfer; the legislative requirements, practices, limitations and safeguards of countries of destination permitting data disclosure and/or access from authorities, practical experience with or knowledge of such requests and any contractual, technical or organisational supplementary safeguards put in place.	Ref 2.9.1	Does your organisation assess specific circumstances of the transfer regularly and ad hoc (the legislative requirements, practices, limitations and safeguards of countries of destination permitting data disclosure and/or access from authorities)?	GDPR: - Art. 28, 44, 46, 48 ECJ Schrems 2 EBA/GL/2019/02 (Outsourcing): - Background Para 37, 41, 46 - Chap. 4 Para 68.d, 68.i		
The CSP shall conduct this assessment regularly (at least annually) in best efforts to continuously ensure compliance with obligations and to make the outcome with supporting information available to the FI upon request. A risk deemed low or medium by the CSP could be deemed differently by the FI due to its specific requirements. If the CSP has reason to believe that it can no longer comply with its commitments it shall immediately (at least within one day) inform the FI and identify appropriate protective measures. If instructed by the FI the data exporter should suspend the transfer in accordance with EU SCC 2021/914 Recital 17.	Ref 2.9.2	Does your organisation provide the outcome of your assessment with supporting information to the FI upon request?	GDPR: - Art. 28		
	Ref 2.9.3	If your organisation can no longer comply with your commitments, will you immediately (at least within one day) inform the FI and identify appropriate protective measures?	GDPR: - Art. 28		
This CSP transfer impact assessment must be performed independently of any assessment of the FI in accordance with accountability obligations in its provider selection process.	Ref 2.9.4	If instructed by the FI, will your organisation suspend the transfer in accordance with EU SCC 2021/914 Recital 17?	GDPR: - Art. 28, 44, 46		
Subchapter 2.10 CSP should achieve holistic Effectiveness of Encryption					
In its Guideline on supplementary measures the EDPB emphasises the use of effective encryption as an adequate supplementary measure to the Standard Contractual Clauses to ensure adequate and effective protection in case of a data transfer outside of the EU/EEA or 3rd countries with established equivalence. Therefore, the ECUC encourages CSPs to seek and proceed in developing new encryption techniques and other data protection measures to protect the data adequately and effectively at any given time.	Ref 2.10.1	Does your organisation plan or is in progress of developing new encryption techniques and other data protection measures to adequately and effectively protect the data at any given time?	GDPR: - Art. 28, 32 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para 68.e		
Hence, guaranteeing encryption and ensuring that the encryption keys are kept under the full control of an EU entity is an option to legally transfer personal data e.g. data transferred to the US.	Ref 2.10.2	Will your organisation guarantee that encryption of data in transit and data at rest as well as corresponding encryption keys can be kept under the full control of an EU entity?	GDPR: - Art. 28, 32		
However, such a proposed approach may only address risks associated with data that is in transit and/or data at rest. Therefore, the EDPB questions the effectiveness of encryption regarding preventing access to data being processed (e.g. data in use). Bring-your-own-key and hold-your-own-key approaches (using HSM technologies) are valuable first steps, but the CSP need to find a holistic approach towards trusted computing giving the FI the opportunity to stay fully in control and deny technically any 3rd party and even the CSP potential access to personal data in clear text.	Ref 2.10.3	Will your organisation guarantee that encryption services for data in use and corresponding encryption keys can be kept under the full control of an EU entity?	GDPR: - Art. 28, 32		
	Ref 2.10.4	Will your organisation guarantee that FIs can choose to deny your support personnel and / or any 3rd party access customer data in clear text?	GDPR: - Art. 32, 32		

Chapter 2 - Privacy

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 2.11 Disclosure Request must be challenged by the CSP					
The CSP shall review the legality of disclosure requests and challenge them if it concludes that the request is unlawful. The CSP therefore needs to pursue possibilities of appeal, seek interim measures with an objective to suspend the request and not disclose the personal data requested but instead forward the request to the individual FI. If disclosing, the CSP shall provide the minimum amount permissible. The CSP shall notify the FI and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it receives a legally binding request or becomes aware of any direct access by public authorities. Prior information should be given as soon as the CSP is made aware to give the FI the opportunity to object or limit access (CSP should support embedding a kill switch or similar technologies or procedures to block autonomously 3rd country access as soon such is identified). Furthermore, the CSP should deny access before the affected FI was able to take actions. If the CSP is prohibited from notifying the FI and/or the data subject under the laws of the country of destination, the CSP shall ensure best efforts to obtain a waiver of the prohibition or forward the request to the FI, with the ambition to communicate as much information as possible and as soon as possible.	Ref 2.11.1	Does your organisation review the legality of disclosure requests and challenge them if you hold the request being unlawful?	GDPR: - Art. 29, 47		
	Ref 2.11.2	If in doubt, will your organisation suspend the request and not disclose the personal data requested but instead forward the request to the individual FI?	GDPR: - Art. 29, 47		
	Ref 2.11.3	If there is no choice other than to fulfil the disclosure request, will your organisation endeavour to disclose the minimum amount of data possible?	GDPR: - Art. 29, 47, 25, 28		
	Ref 2.11.4	Will your organisation notify the FI and, where possible, the data subject promptly if you receive a legally binding request or become aware of any direct access by public authorities?	GDPR: - Art. 28, 12		
	Ref 2.11.5	Will your organisation enable the FI to object or limit access to this data prior to disclosure?	GDPR: - Art. 28		
	Ref 2.11.6	Will your organisation deny access to the requestor before the affected FI is able to take action?	GDPR: - Art. 28 - Art. 44 subseq.		
	Ref 2.11.7	Does your organisation provide a kill switch or similar technology or procedure so the FI can block autonomously 3rd country access as soon such is identified?	GDPR: - Art. 28 - Art. 44 subseq.		
	Ref 2.11.8	If your organisation is prohibited from notifying the FI and/or the data subject under the laws of the country of destination, will your organisation ensure best efforts to obtain a waiver of the prohibition or forward the request to the FI, with the ambition to communicate as much information as possible and as soon as possible to the FI?	GDPR: - Art. 28 - Art. 44, 48		
Subchapter 2.12 Transparency Reports must be provided by the CSPs					
Where legally permissible in destination country, the CSP agrees to provide the FI, in regular intervals for the duration of the contract, with as much relevant information as possible on the requests received, in particular, number of requests, type of data requested, requesting authorities, whether requests have been challenged and the outcome of such challenges, etc. If the CSP acts as a data processor, it shall forward the information to the FI as data controller as quickly as possible.	Ref 2.12.1	Will your organisation fully provide the information outlined in Chapter 2.12?	GDPR: - Art. 46(1), (2c) ECJ Schrems 2: - Recital 109, 139, 143 EDPB Sup. Mea.: - marginal no. 133 subseq.		

Chapter 2 - Privacy

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 2.13 CSP should provide Warrant Canary on Request of FI					
Upon request, the CSP should provide information through a *Warrant Canary* or similar process to inform each FI on a regular basis (e.g. at least every 24 hours) that no access requests have been received from authorities acting against GDPR. This may be done e.g. by sending a cryptographically signed message informing the FI that as of a certain date and time it has received no order to disclose personal data or the like, if this is permitted by the regulation of the CSP place of business in a 3rd country. The CSP must ensure that its private key for signing the Warrant Canary is kept safe and that it cannot be forced to issue false Warrant Canaries by the regulations of the 3rd country, e.g. by appointing a person outside of the 3rd country jurisdiction. The absence of an update of this notification will indicate from FI perspective that the CSP may have received an order and enable the FI to take defence actions.	Ref 2.13.1	Does your organisation provide a Warrant Canary or similar process to inform each FI regularly (e.g. at least every 24 hours) that no access requests have been received from authorities acting against GDPR? Please specify the process and the frequency your organisation is offering in the comment field.	GDPR: - Art. 46(1), (2c) ECJ Schrems 2: - Recital 139 third sentence EDPB Sup. Mea.: - marginal no. 116.		
	Ref 2.13.2	If your organisation provides a Warrant Canary process, will your organisation ensure that the private key for signing the Warrant Canary is kept safe and that it cannot be forced to issue false Warrant Canaries by the regulations of the 3rd country?	GDPR: - Art. 46(1), (2c) ECJ Schrems 2: - Recital 139 third sentence EDPB Sup. Mea.: - marginal no. 116.		
Subchapter 2.14 Personal Data Protection Audits should be supported					
The CSP shall be able to demonstrate compliance with its contractual safeguard provisions. In particular, the CSP shall keep appropriate documentation on the processing activities carried out on behalf of the FI. The CSP shall make available all information necessary for the FI to demonstrate compliance with the obligations set out in these Clauses and at the FIs request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may consider relevant certifications held by the data importer. The FI may choose to conduct the audit by itself, mandate an independent auditor or choose to perform the audit in a pooled audit together with other FIs. Audits may include inspections at the premises or physical facilities of the CSP and shall, where appropriate, be carried out with reasonable notice.	Ref 2.14.1	Will your organisation make available all information necessary for the FI to demonstrate compliance with the contractual obligations by the means of an audit of the processing activities at reasonable intervals?	GDPR: - Art. 5, 28 (3h), 30, 46(1), (2c) EBA/GL/2019/02 (Outsourcing): - Recital Para. 85 ff.		

Chapter 2 - Privacy

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 2.15 Personal Data Breaches must be reported immediately					
In the event of a personal data breach processed for an FI including government request, the CSP shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The CSP shall also notify the FI without undue delay after having become aware of the breach and allow the FI to report the breach at the latest within 72h to the respective regulator. Such notification shall contain a description of the nature of the breach including categories and numbers of affected data subjects and personal data, the details of a data protection officer or contact point where more information can be obtained, the likely consequences of the affected breach and the measures taken or proposed to address the breach and mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, CSP shall send an initial notification containing the information then available and deliver further information as it becomes available without undue delay. The first notification of the breach must not be delayed by the CSP performing internal investigations on the question if this is a breach that needs to be notified as the assessment of this question is a prerogative of the FI as data controller.	Ref 2.15.1	In the event of a personal data breach, will your organisation notify the FI without undue delay after having become aware of the breach?	GDPR: - Art. 33 (2) EDPB WP 250 GL on pers. data breach: - p. 13		
	Ref 2.15.2	Will your organisation allow the FI to report the breach latest within 72h to the respective regulator?	GDPR: - Art. 33 Para. 2 - Recital 85 Para. 2, 87 EDPB WP 250 GL on pers. data breach: - p. 13		
	Ref 2.15.3	Will such notification contain a description of the nature of the breach including categories and numbers of affected data subjects and personal data, as well as the likely consequences of the affected breach and the measures taken or proposed to address the breach and mitigate its possible adverse effects?	GDPR: - Art. 33 Para. 3 EDPB WP 250 GL on pers. data breach: - p. 13 subseq.		
	Ref 2.15.4	If it is not possible to provide all information at the same time, will your organisation send an initial notification containing the information then available and deliver further information as it becomes available without undue delay?	GDPR: - Art. 33 Para. 4 EDPB WP 250 GL on pers. data breach: - p.15		

Chapter 2 - Privacy

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 2.16 CSP Personnel accessing Customer Data must be traceable					
In the event where CSP support personnel need access to cloud services, FIs must be able to grant access, monitor and trail access made by such personnel. The CSP must provide details to trace and protocol these support access activities. There must be no backdoor where CSP support personnel accesses customer data/cloud services without the ability to trail. Amongst others these activities include internal support networks. The CSP must provide a reliable “technical vault mechanism” including surrounding controls and processes around to prevent unauthorized (administrative) access to customer data as well as meta data by any support party, CSP support personnel and sub-contractors.	Ref 2.16.1	In the event where your organisation´s support personnel and / or sub-contractors need access to customer data in the cloud services, do you enable FIs to grant access, monitor and trail such access to customer data?	GDPR: - Art. 32 Para. 4 ECJ Schrems 2: - Recital 134		
	Ref 2.16.2	Does your organisation provide means to trace and protocol such support accesses by your support personnel and / or sub-contractors?	GDPR: - Art. 32 Para. 4 ECJ Schrems 2: - Recital 134		
	Ref 2.16.3	Will the ability to track and trace support personnel and / or subcontractor activities be applicable to your organisation´s internal management and support networks?	GDPR: - Art. 32 Para. 4 ECJ Schrems 2 Rn. 134		
	Ref 2.16.4	Does your organisation provide a reliable “technical vault mechanism” including surrounding controls and processes around to prevent unauthorized (administrative) access to customer data as well as meta data by any support party, CSP support personnel and sub-contractors?	GDPR: - Art. 32 Para. 2, 3 ECJ Schrems 2: - Recital 134		

Chapter 3 - Security

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 3.1 Strong and Transparent Data at Rest Security					
Data at Rest refers to the storing of data. To fulfil this basic need for cloud customers, transparent and strong security in the cloud is a necessity. Therefore, CSPs should provide solutions to ensure adequate security is in place.	Ref 3.1.1	Is data at rest security enabled by default, when setting up an account?	CSA CCM v4.0.5: - CEK-04		
	Ref 3.1.2	If data at rest security is enabled, can your organisation provide the details of the implemented data security measures?	CSA CCM v4.0.5: - CEK-04 ff		
	Ref 3.1.3	Does your organisation keep your data at rest security up to date with new regulations?	CSA CCM EBA/GL/2019/04 (ICT)		
	Ref 3.1.4	Does your organisation notify the customers if new security regulations are adopted? Please specify how in the comment field.	CSA CCM EBA/GL/2019/04 (ICT)		
Firstly, a data encryption methodology should be implemented in such a way that the CSP cannot be forced to disclose the keys to decrypt customer data without approval, consent or knowledge of the data owners. More precisely, a CSP should employ at least a level three, 140-2 Financial Information Processing Standard (FIPS) Hardware Security Module (HSM) which supports state of the art cryptographic processes as well as provides a scalable and managed Key Management Service (KMS) based on HSMs, including key import and re-import, rotation, re-encryption, grouping, and labelling. A CSP should also offer multiple methods for customers to encrypt data at rest, for example: - Supply Your Own Key upon each request - Bring Your Own Key into CSPs HSM - External Key Management where key encryption keys reside outside CSPs HSM - Privately hosted HSMs in a co-location.	Ref 3.1.5	Does your KMS provide the customer with exclusive control? Please specify your approach in comment field.	CSA CCM v4.0.5: - CEK-04		
	Ref 3.1.6	Does your organisation support FIPS 140-2 Level 3 HSM technology in your systems? Please specify if it is internal, external or both in the comment field.	CSA CCM v4.0.5: - CEK-06, 08, 10		
	Ref 3.1.7	If your organisation supports an external HSM, does this limit your service offering? Please specify the not supported services in the comment field.	CSA CCM v4.0.5: - CEK-06, 08, 10		
	Ref 3.1.8	Does your organisation´s KMS provide to the customer scalability?	CSA CCM v4.0.5: - CEK-06, 08, 10		
	Ref 3.1.9	Does your organisation´s KMS provide to the customer key operations?	CSA CCM v4.0.5: - CEK-06, 08, 10		
	Ref 3.1.10	Does your organisation´s KMS provide to the customer encryption?	CSA CCM v4.0.5: - CEK-06, 08, 10		
	Ref 3.1.11	Does your organisation´s KMS provide to the customer signatures?	CSA CCM v4.0.5: - CEK-06, 08, 10		
	Ref 3.1.12	Does your organisation´s KMS provide to the customer meta data?	CSA CCM v4.0.5: - CEK-06, 08, 10		

Chapter 3 - Security

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Secondly, it should be transparent to cloud customers which encryption keys are used for specific actions or on what grounds they are updated, when data assets are encrypted and by whom, thus ensuring auditability. A CSP should offer customers organisation-wide encryption policies and a central place to define Data at Rest encryption for all services. Furthermore, it should enable all services to support the cryptographic key management options mentioned above as well as provide access sovereignty and access transparency logs to justify usage of cryptographic keys and provide a holistic dashboard for all key involvement.	Ref 3.1.13	Does your organisation´s Key Management Service support different cryptographic methods? Please list them in the comment field.	CSA CCM v4.0.5: - CEK-12		
	Ref 3.1.14	Does your organisation ensure the immutability of each cryptographic key operation? Please provide the details in the commentary field.	CSA CCM v4.0.5: - CEK-12		
	Ref 3.1.15	Does your organisation provide data at rest encryption as an enforced system policy for all services?	CSA CCM v4.0.5: - CEK-04		
	Ref 3.1.16	Can your organisation provide access control and transparency of all keys access operations? Please provide in the comment field the services which are being supported by the above mentioned data at rest encryption.	CSA CCM v4.0.5: - CEK-08, 10, 12		
	Ref 3.1.17	In the case of a systemic failure of the KMS rendering our data become inaccessible, does your organisation provide support? Please provide in the comment field in which way you can provide support.	CSA CCM v4.0.5: - CEK-13		
	Ref 3.1.18	Does your organisation provide central monitoring / reporting on key management?	CSA CCM v4.0.5: - CEK-01		
	Ref 3.1.19	Does your organisation offer a single pane of glass view on the state of encryption of all encrypted data?	CSA CCM v4.0.5: - CEK-12		

Chapter 3 - Security

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 3.2 Strong and Transparent Data in Transit Security					
For FIs currently using public cloud services, it is often unclear to them where their data is transferred and how it is secured in transit. However, it should always be transparent to the FI how and where their data is being transferred, particularly the security measures in place to protect data-in-transit. The CSP should use state of the art security to secure data-in-transit, e.g., TLS version 1.3. Hence, vulnerable data security protection should be avoided.	Ref 3.2.1	Does your organisation implement technical measures to protect data-in-transit between on premise and your cloud infrastructure, within your cloud infrastructure, and towards third parties (e.g., Internet)? Please elaborate the technical measures for each data-in-transit type in the comment field.	CSA CCM v4.0.5: - CEK-03 - DSP-10 - UEM-12		
	Ref 3.2.2	Does your organisation use state-of-the-art cryptographic methods to ensure data-in-transit security? Please elaborate the details of the implemented cryptographic method ensuring data-in-transit security in the comment field.	CSA CCM v4.0.5: - CEK-03 - DSP-10 - UEM-12		
To provide clarity on the data transport architecture, the CSP should provide a consistent, central place to configure and monitor data-in-transit security, rather than only per individual service.	Ref 3.2.3	Does your organisation provide a centralized management console to configure and monitor data-in-transit security e.g. native integration of market CASB? Please provide more information in the comment field.	CSA CCM v4.0.5: - CEK-03 - DSP-10 - UEM-12		
Also, a precise description of the CSP's internal data transfer channels and applied security measures should be made transparent to the FI.	Ref 3.2.4	Can your organisation specify for your internal data transfer the details of transfer channels and applied security measures? If yes, please give specification (reference) in CSP comment field.	CSA CCM v4.0.5: - CEK-03 - DSP-10 - UEM-12		
In addition, for each cryptographic process, a clear justification should be available and included in log files, e.g., certificate renewal.	Ref 3.2.5	Can your organisation provide evidence for implemented cryptographic processes around certificates, e.g., logfiles of certificate operations?	CSA CCM v4.0.5: - CEK-03 - DSP-10 - UEM-12		

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 3.3 Fully Featured Logging and Monitoring					
To ensure full control of customer data assets, robust, and complete audit logging of all cloud application and service activity is required. This applies to both customer and CSP actions and the retention time should be defined by the customer. Logging and Monitoring includes customer service access (Access Transparency with approvals), CSP and customer admin access (Admin Activity/Read/Write), as well as data that have been accessed (Data Access/Read/Write).	Ref 3.3.1	Does your organisation provide complete audit logging of all cloud application and service activity?	CSA CCM v4.0.5: - LOG-10, 11		
	Ref 3.3.2	Does your organisation provide the logging of both customer and CSP actions?	CSA CCM v4.0.5: - LOG-01 ff		
	Ref 3.3.3	Does your organisation ensure integrity of logging?	CSA CCM v4.0.5: - LOG-01 ff		
If only the CSP accesses customer assets, the customer should be provided with functionality to effectively control the access for this specific resource before any access happens.	Ref 3.3.4	Does your organisation provide a control mechanism which requires the approval from the customer prior to any admin access being granted?	CSA CCM v4.0.5: - LOG-01 ff		
A CSP should, for all services, consistently log identity, performed action, service usage, corresponding purpose, and involved data. Cloud customers should be able to access comprehensive logs to the service related activities on the platform; this could be provided via for instance an Application Programming Interface (API), a Graphical User Interface (GUI) or some other mechanisms to integrate with their own security logging systems.	Ref 3.3.5	Does your organisation provide a centralised Security Monitoring service where all logs and alerts are generated either by user activities, service activities, data activities data, etc. and can be actively monitored and tracked?	CSA CCM v4.0.5: - LOG-03		
Furthermore, customer log data should not be shared with 3rd parties without the consent of the customer.	Ref 3.3.6	Does your organisation share logging data with any 3rd parties or subcontractors without upfront consent of the customers? Please elaborate in comment field which cases and why you need to share logging data with which 3rd parties.	CSA CCM v4.0.5: - LOG-04		
With respect to monitoring, there is a lack of standardised monitoring interfaces across CSPs. Therefore, to leverage multiple CSPs, there should be a standardised monitoring interface provided across all services.	Ref 3.3.7	Is your organisation´s monitoring approach covering all your services? Please explain in comment field.	CSA CCM v4.0.5: - LOG-07		
	Ref 3.3.8	Does your organisation´s Security Monitoring service provide an interface so that interchange between different platforms is possible (e.g. open standards)? Please provide the interchange protocols in the comment field.	CSA CCM v4.0.5: - DSC-01		
	Ref 3.3.9	Does your organisation provide a complete set of policies to achieve compliance against industry standards (e.g. CIS benchmarks) out of the box?	CSA CCM v4.0.5: - AIS-01		
	Ref 3.3.10	Does your organisation provide out of the box management of these policies?	CSA CCM v4.0.5: - AIS-01		

Chapter 3 - Security

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 3.4 Data Exfiltration and Customer Policy Enforcement					
Since data sharing is quite effortless to perform on the cloud, customers are interested in strictly controlled data sharing capabilities to prevent data exfiltration to unwanted locations.	Ref 3.4.1	Does your organisation provide a way to restrict data to be localised in a chosen region only and by doing so prevent data transfers taking place towards unwanted locations e.g. outside the EEA?	CSA CCM v4.0.5: - DSP-08		
Hence, CSP should provide consistent visibility and control of all workloads and communication flow perimeters regardless of location, size, or architecture. This also applies to communication between CSP services and 'private endpoints', including the direction of data flow (ingress/egress).	Ref 3.4.2	Can your organisation provide the detailed data flows, both ingress (inbound) / egress (outbound), of each cloud service being used by the customers?	CSA CCM v4.0.5: - DSC-09 ff.		
A CSP should also provide an effective set of KMSs to enable customers to assess security configurations at a global cloud control layer in line with their security frameworks and standards.	Ref 3.4.3	Does your organisation provide an effective set of KMSs to enable customers to assess security configurations at a centralized global cloud control layer in line with their security frameworks and standards?	CSA CCM v4.0.5: - CEK-06, 08, 10		
In addition, each configuration and policy defined for a cloud service by a customer should be automatically applied across all instances of that service run by that customer and be centrally monitored thereafter.	Ref 3.4.4	Does your organisation provide for each service an automated policy enforcement as configured by the customers so that it can be monitored and validated upon policy compliance?	CSA CCM v4.0.5		
Subchapter 3.5 Service Certifications and Evidence					
Certifications for cloud services assure an adequate level of security and therefore are one of the key requisites for all cloud users to rely upon. Hence, the services of a CSP should be independently certified by independent certification authority.	Ref 3.5.1	Can your organisation demonstrate or evidence the independent certifications provided by certified authority?	BSI C5:2020 PCI DSS CSA STAR ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 AICPA SSAE 18 ISAE 3402 type II: SOC2		
The security certifications should at least include the de facto market standards for cloud technology , as well as further certifications that are specific to the financial industry.	Ref 3.5.2	Does your organisation certify cloud products and services, with de facto market standards for cloud technology certifications? If yes, please specify in the comment field which certifications you have granted for which products and services.	BSI C5:2020 PCI DSS CSA STAR ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 AICPA SSAE 18 ISAE 3402 type II: SOC2		
A CSP should disclose evidence of certifications upon request to the customer. Furthermore, a CSP should provide its customers with the ability to conduct their own audits on the CSP.	Ref 3.5.3	Can your organisation provide (annually if possible) evidence of certifications of the services being used by the customers, so that this can be validated in an own audit?	BSI C5:2020 PCI DSS CSA STAR ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 AICPA SSAE 18 ISAE 3402 type II: SOC2		

Chapter 3 - Security

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 3.6 Separation of Identities and Contacts					
In the event an FI's identity and contact information are identical, there's a possibility that their associated contexts may get mixed up. A CSP should therefore provide the measures to associate federated and non-federated identities with valid routable contact information (e.g., email addresses) to ensure notifications are successfully delivered to the user. More precisely, identity identifier and contact information should be separated but able to be grouped by identities. For example, if an identity cannot be routed for notifications, at least a valid and routable email address should be able to be associated and used to send any notifications to and from the CSP.	Ref 3.6.1	Does your organisation provide measures to associate federated and non-federated identities with valid routable contact information (e.g., email addresses), to ensure notifications are succesfully delivered to the users? Please provide the details in the comment field.	CSA CCM v4.0.5: - LOG-08		
A CSP should provide specific communication channels for certain event types, such as critical data and service events, e.g., data breaches, security issues, or technical blockers. This should be provided, in addition to email by other channels that can be configured by the customer.	Ref 3.6.2	For specific (critical/sensitive) event types, does your organisation provide a separate communication channel (in addition to email) that can be configured by the customer? Please describe the details of a separate communication channel for communication of such critical/sensitive data in the comment field.	CSA CCM v4.0.5: - LOG-08		
Subchapter 3.7 Maturity of Data-in-Use Security					
As of now, to achieve data-in-use security, the only generic and practical method in the industry is to rely on Trusted Execution Environments as part of the computing processors. This functionality is often referred to as Confidential Computing. This feature is only offered by some CSPs for a few selected services restricted to specific hardware specifications. To enable customers to protect their data during usage, the CSP should provide Confidential Computing or similar implementations as an option for a broad set of hardware configurations as well as backends of managed services.	Ref 3.7.1	Does your organisation provide Confidential Computing or similar implementations? Please provide the list of services that you offer which support Confidential Computing as well as details on how it is implemented.	CSA CCM v4.0.5		

Chapter 3 - Security

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 3.8 Backup Functionality, High Availability, and Disaster Recovery					
A CSP should provide a geo-redundant backup solution which is independent of the service's API enablement status. The backup functionality should support service independent storage locations and should not rely on 3rd parties. Also, the backup measure should be coherent with the shared responsibility model for the cloud service models for IaaS, PaaS, SaaS	Ref 3.8.1	Does your organisation provide a geo-redundant backup solution for all cloud service models (IaaS, PaaS, SaaS) which is independent of the service's API enablement status, and support service independent of storage locations and not rely on 3rd parties? Please elaborate your answer in the comment field.	ISO/IEC 27002:20013: - Chapter 5.29, 7.5 ISO/IEC 27002:2022: - Chapter 5.29, 7.5, 8.14 ISO/IEC 27018:2019: - Chapter 5.29, 7.5		
This functionality should be provided by all services storing customer data or service configurations and be manageable through a single interface.	Ref 3.8.2	Is your organisation´s backup solution provided for all services storing customer data or service configurations, and can it be managed through a single interface?	ISO/IEC 27002:2013: - Chapter 12.3 ISO/IEC 27002:2022: - Chapter 8.13 ISO/IEC 27018:2019: - Chapter 12.3		
For business continuity reasons, cloud services should be available in both High Availability and Disaster Recovery mode, so as not to create a single point of failure for FIs. Furthermore, if the CSP performs business continuity and resilience exercises affecting customers, they should be informed of the process and able to veto.	Ref 3.8.3	Are your organisation´s cloud services available in both High Availability and Disaster Recovery mode?	ISO/IEC 27001:2013: - Chapter 17.2 ISO/IEC 27002:2022: - Chapter 8.14 ISO/IEC 27018:2019: - Chapter 17		
	Ref 3.8.4	Can customer choose to opt-out or are they able to veto when your business continuity and resilience exercises are expected to have a negative impact on customers' availability?	CSA CCM v4.0.5: - BCR-01 ff.		
Due to the central relevance of a KMS to provide cryptographic processes, a solution should be in place that enables CSP services to perform cryptographic tasks even when the main KMS is unavailable. This holds true especially for single region services.	Ref 3.8.5	Is your organisation´s KMS implemented with resilience in mind so that your cloud services continue to perform cryptographic tasks even when the main KMS is unavailable?	ISO/IEC 27002:2013: - Chapter 10.1 ISO/IEC 27002:2022: - Chapter 8.24 ISO/IEC 27018:2019: - Chapter 10.1		
Hence, a KMS should have a multi-region setup allowing the provisioning of multiple different keys to a specific service to overcome the risk of unavailability of an otherwise single point of failure KMS service.	Ref 3.8.6	Is your organisation´s KMS implemented as a multi-region setup to overcome the risk of unavailability of an otherwise single point of failure?	ISO/IEC 27002:2013: - Chapter 10.1 ISO/IEC 27002:2022: - Chapter 8.24 ISO/IEC 27018:2019: - Chapter 10.1		
While multi-regional services enable a geo-redundant setup, the set of single regions should be clearly defined for the multi-region. A CSP's customer should be able to customize a multi-region or select of several pre-defined multi-regions in the same geographical region.	Ref 3.8.7	Is the customer able to customize a multi-region or select out of several pre-defined multi-regions in the same geographical region?	ISO/IEC 27001:2013		

Chapter 3 - Security

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 3.9 Software Supply Chain Transparency					
Customer assets such as applications run on various underlying infrastructure managed by the CSP. This consists also of software, such as operating systems and management tools. Since the layer below the customer's view is only available to the CSP, the responsibility for this software stack is with the CSP. Therefore, a CSP should provide methods such as auditing processes and security evidence in order to provide transparency on its underlying software supply chain towards the customer. This helps FIs to comply with EBA requirements , where applicable CSP should provide detailed information to deliver the service chain.	Ref 3.9.1	To be able to comply with EBA-requirement, can your organisation provide methods such as auditing processes and security evidence in order to provide transparency on underlying software supply chain towards the customer?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 67-80		
Subchapter 3.10 IAM and Privilege Escalation					
Assets, such as data of customers, reside in CSP's services and access to these are controlled via Identity & Access Management (IAM). This is a core feature and should be a foundation to build upon, where user access rules are defined, controlled and managed solely by the cloud customers. However, if this is not implemented correctly, the risk of privilege escalation may emerge (with associated risks such as identity theft and data leakage), resulting in higher privileges than users should have in the first place. It should not be possible to gain access to a system without proper IAM settings. The CSP is responsible to deliver a sound IAM implementation across all its services to enable the definition, enforcement, and maintenance of IAM roles and permissions. This should result in a managed infrastructure, which is only accessible via a secured IAM system.	Ref 3.10.1	Does your organisation provide an integrated Identity & Access Management (IAM) service that allows cloud customers to configure and solely manage their user population and access? Please provide the details in the comment field.	ISO/IEC 27002:2013: - Chapter 9.2 ISO/IEC 27002:2022: - Chapter 8.24 ISO/IEC 27018:2019: - Chapter 5.2, 5.3, 5.18, 8.5 CSA CCM v4.0.5: - BCR-01 ff		
	Ref 3.10.2	Is your organisation´s Identity & Access Management (IAM) service implemented in such a way that access control is enforced and users are not able to bypass it (e.g. potentially gain access to a system without proper IAM settings)? Please provide the details in the comment field.	ISO/IEC 27002:2013: - Chapter 9.2 ISO/IEC 27002:2022: - Chapter 8.24 ISO/IEC 27018:2019: - Chapter 5.2, 5.3, 5.18, 8.5 CSA CCM v4.0.5: - BCR-01 ff.		
	Ref 3.10.3	Can your organisation´s Identity & Access Management (IAM) service prevent user privilege escalation ? Please provide the details in the comment field.	CSA CCM v4.0.5: - IAM-01 ff.		

Chapter 3 - Security

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 3.11 Workload Isolation					
Various workloads of different customers will reside at the same CSP. Therefore, it should never be possible to access any other customer's assets without explicit consent. This includes data, software, infrastructure, and containers or virtual machines.	Ref 3.11.1	Are customer's cloud deployment fully isolated in such a way that it is not possible to access any other customer's assets without explicit consent/approval? This includes data, software, infrastructure, and containers or virtual machines.	CSA CCM v4.0.5: - IVS-06		
The CSP should deliver evidence of periodic review of isolation controls that are effective including corrective measures. Updating systems and publishing reports will increase transparency.	Ref 3.11.2	Can your organisation demonstrate or provide evidence of periodic reviews of isolation controls, that they are effective and that - if necessary - corrective measures were taken?	CSA CCM v4.0.5: - IVS-05 ff.		
Subchapter 3.12 Malware Defence					
Due to the variety of services offered by a CSP, this enables different entry points for malware, such as ransomware. For the parts of the shared responsibility model the CSP is responsible for, the malware needs to be kept away from customer systems while at the same time the customers should have the possibility to use specialized tools to prevent, detect, and mitigate malware impact. Thus, the CSP should provide a threat intelligence to isolate threats without disruption and alert the customer with the option to clean infected systems.	Ref 3.12.1	Does your organisation have a threat detection service that can protect against threats to avoid disruption and alert the customer with the option to clean infected systems? Please provide the details in the comment field.	CSA CCM v4.0.5: - TVM-01,02		
For the parts of the shared responsibility model the customer is responsible for, the CSP should offer tools to prevent misuse and infection of its services.	Ref 3.12.2	Does your organisation offer tools to the customer to prevent misuse and malware infection of cloud services used by the customers? Please provide the details in the comment field.	ISO/IEC 27002:2013: - Chapter 12.2 ISO/IEC 27002:2022: - Chapter 8.7 ISO/IEC 27018:2019: - Chapter 12.2		

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 4.1 Control measures on Outsourced Services					
To control outsourced services and systems implemented on cloud platforms, the following information on outsourced services should be made available to the customer on near real-time basis (case related) or via adequate alerts with defined and transparent thresholds: - Information on geographical/regional aspects and the provider's landscape including their data center location	Ref 4.1.1	In general, does your organisation provide information or alerts on the availablity of the used services at least on a near real-time basis to monitor the performance of the outsourced arrangements? Please specify in comment field.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74, 75, 100 ff.		
- Defined, implemented and tested contingency measures for the used services and infrastructure - Adequate contingency solutions to allow instant action to keep the service running or to fix problems - Conditions upon which contingency measures can be justified when it comes to 3rd country data transfer - Contingency measures that include or risk 3rd country data transfer should be made transparent in standard contractual clauses - Supplied information should include the CSP supply chain and sub-outsourcing, where applicable.	Ref 4.1.2	Does your organisation provide contingency measures for the used services on a near times basis to monitor the performance of the outsourced arrangements, according to the EBA/GL/2019/02 (Outsourcing)?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74, 75, 100 ff.		
	Ref 4.1.3	Does your organisation break down availabilty information and contingency measures to services and regions/zones to monitor the performance of the outsourced arrangements?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74, 75, 100 ff.		
	Ref 4.1.4	Does your organisation inform about 3rd country data transfer to monitor the security & data protection of outsourced services?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74, 75, 78, 83		
	Ref 4.1.5	Is the above mentioned information provisioning referenced in your organisation´s standard contractual clauses?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75, 100 ff.		

Chapter 4 - Governance and Regulation

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 4.2 CSP should provide Information for a sound 3rd Party Risk Management					
For a sound governance of 3rd Party Risk Management, CSPs should provide FIs with the following information for the used cloud services and infrastructure, that is deemed to be sufficient for an FI specific Business Continuity and Disaster Recovery Plans: - Overview of cloud services including a detailed supply-chain service mapping of underlying dependent sub-contractors or sub-hosting services - Supply-chain information detailing the roles and responsibilities of the underlying sub-contractors for the related cloud services - Supply-chain information detailing the dataflow, data exchange and data location/region between the CSP and each sub-contractor for the related cloud services.	Ref 4.2.1	Does your organisation provide a present list of all sub-contractors relevant for FI's cloud usage to control and manage the risk of outsourced arrangement?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 76 ff.		
	Ref 4.2.2	Does your organisation inform about changes in sub-contractors to control and manage the risk of outsourced arrangement?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 76 ff.		
	Ref 4.2.3	Does your organisation provide the list of services managed by the sub contractors/sub-processors and which kind of data access are processed by them? Please provide a list or link in the comment field.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 76 ff.		
	Ref 4.2.4	Does your organisation inform about the location of customer data at rest, in transport (only if managed by the CSP) and in use (especially when subcontractors are part of the service operation) to control and manage the risk of outsourced arrangement?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 76 ff.		
	Ref 4.2.5	Does your organisation provide a due diligence for each of the sub contactors/sub-processors?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 79		

Chapter 4 - Governance and Regulation

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 4.3 Exit Strategy Requirements					
The European Banking Authority (EBA) guidelines on outsourcing arrangements require FIs as part of their risk assessment to have an exit strategy in place when outsourcing any "Critical / Important function" to CSPs. This is to cover relevant exit triggering events, e.g. bankruptcy of CSP, sanctions, or a changing legal environment. Relevant exit triggering events can be observed, and the occurrence anticipated. On that basis along with empirical data from such events, an exit and migration time slot can be defined to exit a cloud platform and migrate the bank critical service. We ask to outline feasible time slots for exit plan execution that is connected to the materiality assessment of the outsourcing.	Ref 4.3.1	Does your organisation duly inform about discontinuation of used services or contractual arrangements to prevent an unexpected interrupt of outsourced arrangements? Please specify the days in advance, like e.g. 180 days in the comment field.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 42, 76 ff., 106		
	Ref 4.3.2	Does your organisation offer a dedicated post-termination period?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 42, 76 ff., 106		
Subchapter 4.4 CSP Audits and Oversight					
We propose simplifications in audit procedures insofar as the cloud service offerings are not checked by every FI, but centrally at the CSP. We want to facilitate the implementation of regulatory requirements at CSPs: Collaborative audits organised by the financial industry should become a generally accepted approach by CSPs and free of charge. Different institutions form a collaborative team to audit one specific CSP. The audit results can be regarded valid within the respective individual institution. Collaborative audits are already supported by the EBA Guidelines on Outsourcing Arrangements (Art. 13.3.91.a). Currently CSPs are audited by European supervision along onsite inspections at Financial Institutes. On that basis a particular CSP is audited multiple times whenever Financial Institutes as CSP customers are inspected on their public outsourcing activities. National and European supervision are asked to form collaborative audit teams to audit CSPs across countries and for all Financial Institutions being customers of a CSP. Such an approach could improve consistency of observations, and additionally be more efficient. In addition, we point out that the systemic risk of the entire industry using CSP cannot be managed by individual institutions. However, the institutions specific cloud adoption is still inspected individually and resulting observations are assigned to the respective institution.	4.4.1	Does your organisation support pooled audits performed by FIs themselves to use audit resources more efficiently and to decrease organisational burden?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91		

Chapter 5 - Contractual Clauses

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 5.1 Audit Rights for Customers					
To meet industry's obligations to audit, audit rights to data centers and its services, Customers Audit Rights should be granted per standard contractual clauses. There is also a need to audit the relevant infrastructure on a regular basis. With referance to the requirements set out in the EBAs Guidelines on Outsourcing Arrangments (EBA/GL/2019/02), the written outsourcing arrangements should at least include the unrestricted right to inspect and audit the service provider especially with regards to the critical or important outsourced function. This would include but not be restricted to for instance data centers. Therefore, you are kindly asked to provide answers to the following questions.	Ref 5.1.1	Does your organisation offer rights to your customers, their auditors, and competent authorities without restricting them to inspect and audit your services with regards to the functions and services outsourced to your institution in accordanace with the written outsourcing arrangement?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.p, 85.ff		
	Ref 5.1.2	Does your organisation grant by the written outsourcing agreement: a. full access to all relevant business premises (e.g. head offices and operation centers), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors ('access and information rights'); and b. unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 87		
	Ref 5.1.3	Does your service arrangement make third party certifications, including related evidences or reports, available to the customer?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91.b		
	Ref 5.1.4	Does your service arrangement make third party audits or internal audit reports available to the customer?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91.b		
	Ref 5.1.5	Does your organisation provide the scope of certifications or audit reports which cover the systems (e.g. processes, applications, infrastructure, data centers, etc.) and key controls identified by the Financial Institutions?	EBA/GL/2019/02 (Outsourcing): - Chap. Para. 93.b		
	Ref 5.1.6	Does your organisation provide the certifications and evidences or reports on a regularly basis?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 93.c		
	Ref 5.1.7	Does your organisation ensure that key systems and controls will be covered in future versions of your certification or audit report?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 93.d		
	Ref 5.1.8	Does your organisation grant the right by contract to request expansion of the scope of the certifications or audit reports or relevant systems and controls?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 93.g		

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
	Ref 5.1.9	Does your organisation grant the contractual right to perform individual audits at banks' discretion with regard to the outsourcing of critical or important functions?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 93.h		
	Ref 5.1.10	Does your service arrangement permit pooled audits?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91 a		
	Ref 5.1.11	Concerning pooled audits, does your organisation provide full visibility on internal CSP procedures and documentation in a confidential way to permit to the EU legal entities to satisfy the inspection activities?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91.b		
Summary	Ref 5.1.12	**Has your organisation regulated all the above requirements in the standard contract or a specific contractual amendment?**			

Chapter 5 - Contractual Clauses

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 5.2 Sub-Outsourcing					
In accordance with the EBA "Guidelines on Outsourcing Arrangements" the CSP provides information regarding sub outsourcing at any time without limitations.	Ref 5.2.1	Does your organisation provide information such as a registry of sub-contractors and their potential third-country transfer of data to your customers to ensure that any risks can be identified and mitigated?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 55.g, 67		
	Ref 5.2.2	For sub-outsourcing does your organisation a. in the sub-outsourcing arrangement oversee and ensure that all contractual obligations between your institution and the customer are continuously met if sub-outsourcing takes place? and b. does your organisation ensure that the same contractual and regulatory requirements stipulated in your service arrangement also apply to these arrangements including the requirements to grant rights of access and audit in accordance with Ref 5.1.1?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 79		
	Ref 5.2.3	Does your organisation provide any information during the due diligence phase to support the Financial Institute to evaluate the potential risk?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 69		
In addition and following our experiences, we regard a prenotification of minimum 90 days as being adequate to show all changes with the right of consultation.	Ref 5.2.4	Does your organisation notify your customers in advance regarding potential changes to the outsourcing arrangement or the service provided including sub-outsourcings and the right of consultation?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 42.d.ii, 44.f, 78.e		
The CSP should ensure that the objections of FIs are examined favourably.	Ref 5.2.5	Does your organisation ensure that objections to the suboutsourcing by the FI are duly taken into account?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 78.f		
	Ref 5.2.6	Does your organisation inform customers in advance to perform a risk assessment? Please specify how many days in advance in the comment field.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 44.f, 78.d, 78.f		

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
	Ref 5.2.7	In case that your organisation does not grant the right to object, do you offer termination support in case of undue sub-outsourcing?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 78.d, 78.f		
In the event of use of unsuitable subcontractors, the FI should be granted a special right of termination including termination support.	Ref 5.2.8	Does your organisation offer the right to terminate the contract in case of undue sub-outsourcing or in any case by the customer?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 78.g		
	Ref 5.2.9	Does your organisation offer a transition period when the customer is forced to terminate the contract?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 99.b		
Summary	Ref 5.2.10	**Has your organisation regulated all the above requirements in the standard contract or a specific contractual amendment?**			

Chapter 5 - Contractual Clauses

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 5.3 Embedded URLs in Contracts and Service Level Agreements					
In Accordance with EBA Guidelines on Outsourcing, CSPs should provide clear financial obligations within the contract.	Ref 5.3.1	Does your organisation provide clear financial obligations by a written contract for your services, including clear rules on price increases according to periods with price guarantee/fixed price.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.d		
Unilateral changes by the CSPs using embedded URLs in contract should not affect the agreed Terms and Conditions during the contract period. This prevents a sudden increase in cost which can occur after offering an attractive price model for the initial contract phase.	Ref 5.3.2	Does your organisation provide stable Terms and Conditions for your services for an agreed contract period?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.i DORA: - Art. 25.9		
Likewise, the CSP should only change the service in a way that guarantees all cloud customers at least equal or improved services in terms of function, security, technology and data protection,	Ref 5.3.3	Does your organisation provide backward compatibility for any service change?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 DORA: - Art. 25.9		
	Ref 5.3.4	In the event of a service change(s), is there a gurantee that are overall security standards and data protection are kept at least at the previous level?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 DORA: - Art. 25.9		
or that a change or termination of the service will be announced with a prenotification period and without undue delay.	Ref 5.3.5	Does your organisation offer prenotification periodes in case of major changes or termination of services? Please provide more details in the comment field.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 DORA: - Art. 25.9		
In addition to availability, the Service Level Agreements (SLA) should also include performance metrics and reporting thereof. Both values require permanent monitoring and automation for reporting deviations.	Ref 5.3.6	Does your SLA include performance metrics and permanent monitoring and reporting?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.h, 75.i, 75.p, 82, 85, 87, 88, 90, 91b, 92, 93		

Chapter 5 - Contractual Clauses

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference**	**Reg. reference**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
The CSP should offer additional communication channels to transmit critical event and service level information (e.g. on data breaches, penetration test findings, logfiles for problem analysis) besides email and a definition of which channels are to be used for different types of information, e.g., via phone. All such events should be available to the customer regardless if the CSP has concluded that the customer is impacted or not. The customer must have the possibility to assess impact and not only rely on the CSP impact analysis.	Ref 5.3.7	Does your organisation offer dedicated communication channels and competent contacts for critical events, breaches, penetration tests and logfile issues?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.j, 98, 92		
	Ref 5.3.8	Does your organisation inform the customer about events in any case, not only if the customer is impacted?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.j, 85, 87, 88		
	Ref 5.3.9	Does your organisation offer Financial Institutions impact analyses in addition to your own?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.h, 75.i, 75.p, 93.g		
All terms, changes, and level of information should apply without exception to all consumers and not only to individual consumers.	Ref 5.3.10	Does your organisation state all terms/prenotification periods, communication channels tests etc. in a standard contract or a standard FSA?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74		
Any changes to product terms (incl. FSA, DPA and SLA) should be highlighted on paragraph level in order to facilitate FI identification of the exact change and subsequent impact analysis. Documentation of changes should be logged by the CSP to allow for back-tracking what changes have happened over time.	Ref 5.3.11	Does your organisation offer a version management with the ability to track changes for all contracts and SLA?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.i DORA: - Art. 25.9		
Subchapter 5.4 Insurance					
The contracts between CSPs and FIs should have an insurance clause that needs to increase with the number of assets on the cloud.	Ref 5.4.1	Does your organisation provide an insurance against risks for cloud usage?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.k		
	Ref 5.4.2	Does your organisation provide, if applicable, the level of insurance cover requested?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.k		
Summary	**Ref 5.4.3**	**Has your organisation regulated all the above requirements in the standard contract or a specific contractual amendment?**			

Chapter 6 - Portability

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 6.1 CSP should apply Technology Standards					
CSP should make sure to apply technology standards of internationally recognised institutes to their services. These include: - NIST (National Institute of Standards and Technology) - ISO (International Organization for Standardization) - CNCF (Cloud Native Computing Foundation) - an institute that implements the general requirements for the EU Cybersecurity Act (EUCA) e.g. BSI (Bundesamt für Sicherheit in der Informationstechnik): C5 (Cloud Computing Compliance Criteria Catalogue) - CSA (Cloud Security Alliance): STAR (Security, Trust, Assurance, and Risk) In order to prove the certification of the standards of these bodies, the adherence to these standards should be publicly documented by the CSP.	Ref 6.1.1	Does your organisation in general apply technology standards of international institutes to ensure interoperability and compatibility?	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4		
	Ref 6.1.2	Does your organisation apply NIST to ensure interoperability and compatibility?	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4		
	Ref 6.1.3	Does your organisation apply ISO to ensure interoperability and compatibility?	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4		
	Ref 6.1.4	Does your organisation apply CNCF to ensure interoperability and compatibility?	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4		
	Ref 6.1.5	Does your organisation apply CSA to ensure interoperability and compatibility?	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4		
	Ref 6.1.6	Does your organisation apply standards of other institutes which leverage interoperability and compatibility? Please specify in comment field which one.	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4		
	Ref 6.1.7	Does your organisation publicly document the compliance with the confirmed standards to ensure interoperability and compatibility?	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4		
Subchapter 6.2 CSP should offer Open-Source Technology and Standards					
CSP should embrace open-source technology and provide such components as software stacks, interfaces, and APIs. The provided services should build upon or be efficiently referable to open-source solutions from the open-source community. Effective pre-checks as part of the system lifecycle management should be in place before using open-source technology. This especially holds for standards in software, data, communication, and processes, which should be preferred in comparison to proprietary solutions.	Ref 6.2.1.	Does your organisation provide opensource technology in general as part of your product strategy to support the transfer of outsourced services to alternative providers ? Please specify your organisation´s strategy for open source and list in extracts the components being offered in the comment field.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		

Chapter 6 - Portability

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 6.3 CSP should provide methods and tools to allow Workload Portability					
CSPs should strongly support FIs to perform their exit plans for their workloads, services and applications as required by European Banking Authority (EBA) guidelines on outsourcing arrangements. CSPs should provide methods and tools to help migrate IaaS and PaaS to other IT service providers quickly and securely: - The methods and tools provided should enable a seamless migration to the most widely used commercial and open-source infrastructures, networks, platforms, and databases (state of the art technologies). Tools provided should enable homogeneous and heterogeneous migrations from any supported source within the CSP environment to a state-of-the-art technology target environment. - CSPs should provide tools to create infrastructure as a code-artifacts that describe existing resources and their properties in order to prepare for automated implementation in target environments. - Licenses for on-premises (or equivalent) solutions for a fair price to ensure clients have the option to return to an on-premises solution should an exit scenario occur. - For SaaS, the CSPs should offer a version/installation which is compatible with other cloud platforms or provides other alternatives, such as licenses for desktop installations. The exception here would be SaaS CSP proprietary solutions that needs cloud-native capabilities to provide the service(s) to the customer. Alternatives are especially relevant for Office products and should ensure that a migration during an exit is realistic and economically possible. CSPs should respect the requirement for FIs to have an exit plan.	Ref 6.3.1	Does your organisation supply methods and tools that enable customers a seamless migration to the most widely used commercial and open-source infrastructures, networks, platforms, and databases (state of the art technologies) to support the transfer of outsourced services to alternative providers?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.3.2	Does your organisation supply tools to create infrastructure as code-artifacts that describe existing resources and their properties in order to prepare for automated implementation in target environments to support the transfer of outsourced services to alternative providers?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.3.3	Does your organisation support clients in returning existing licenses to an alternative solution if an exit scenario should occur to support the transfer of outsourced services to a different infrastructure?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.3.4	Does your organisation offer a version/installation which is compatible with other cloud platforms or provides other alternatives for the transfer of your SaaS offerings to alternative providers?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.3.5	Does your organisation have APIs or connectors for migration to other cloud platforms or provide alternatives?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		

Chapter 6 - Portability

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 6.4 CSP should provide standardised Data Formats and Export Processes					
CSP should provide standardised data formats and processes for data extraction and transport to other environments and platforms. The paragraph will only cover data portability and export requirements not already covered in other chapters, e.g. chapter 2 Requirements on Privacy: - CSP should establish bi-directional data portability by providing contract/service contract/SLA, processes, products, data formats, metadata and professional services to customers for all data owned as intellectual property by the customer.	Ref 6.4.1	To support the transfer of outsourced services to alternative providers, is data portability (information transfer, being export and import of data to and from other CSP) part of the standard contract?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.2	To facilitate the transfer of oursourced services and related data, is data portability part of the standard offered SLA?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para 107, 108		
	Ref 6.4.3	To facilitate the transfer of oursourced services and related data, is data portability supported by internal processes of your organisation?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.4	To facilitate the transfer of oursourced services and related data, is data portability supported by an information transfer registry?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		

Chapter 6 - Portability

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
	Ref 6.4.5	To facilitate the transfer of oursourced services and related data, is data portability supported via different (common) data formats (e.g; JSON, XML)?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.6	To facilitate the transfer of oursourced services and related data, is data portability supported by means of appropriate physical data transfer media for different data volumes (small to very large)?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.7	To facilitate the transfer of oursourced services and related data, is the exported data accompanied by its relevant meta-data and is this part of the above mentioned data formats?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.8	To facilitate the transfer of outsourced services and related data, are professional services offered to support the customer in his data portability process and implementation?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		

Chapter 6 - Portability

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
- Data portability includes both data and meta-data which give the data its meaning. Amongst others these are operational data, secrets, metadata and their backups as well.	Ref 6.4.9	To support the transfer of outsourced services and data to alternative providers is the provided data export containing operational meta-data (e.g. creation date & time)?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.10	To support the transfer of outsourced services and data to alternative providers, is the provided data export containing (in the same or separate export file) the secrets to decrypt the data?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.11	To support the transfer of outsourced services and data to alternative providers, is the provided data export containing the meta-data of the meta-data itself (e.g. in order to understand if a date is a creation date or date of update)?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.12	To support the transfer of outsourced services and data to alternative providers, is the provided data export containing a set of backup snap-shots?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.13	To support the transfer of outsourced services and data from other providers to your organisation, can your organisation import a data file containing operational meta-data (e.g. creation date & time)?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
	Ref 6.4.14	To support the transfer of outsourced services and data from other providers to your organisation, can your organisation import a data file containing (in the same or separate export file) the secrets to decrypt the data?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.15	To support the transfer of outsourced services and data from other providers to your organisation, can your organisation import a data file containing the meta-data of the meta-data itself (e.g. in order to understand if a date is a creation date or date of update)?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.16	To support the transfer of outsourced services and data from other providers to your organisation, can your organisation import a data file containing a set of backup snap-shots?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		

Chapter 6 - Portability

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
- CSPs should establish processes that support the customer to execute data portability and export. - CSPs should offer products and services that support the customer to execute bi-directional (in and out) online and offline (bulk) data portability. Data at rest and in transit should be secured and privacy needs to be ensured. - Customers must be able to choose data portability products and services depending on the urgency, the data volume to exchange, different data querying (e.g. SQL) and representation (e.g. JSON) formats and cost.	Ref 6.4.17	To support the transfer of outsourced services and data, does your organisation have a service to support customers to execute the data import/export processes?	ISO/IEC 27018:2019: - Control 16.11 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.18	To support the transfer of outsourced services and data, is data portability supported by means of appropriate physical data transfer media for different data volumes (small to very large)?	ISO/IEC 27018:2019: - Control 13.2 GDPR: - Art. 20 EU Data Act: - Art. 29 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.19	Does your organisation provide an secure transfer of outsourced services and data? Please specify how the physical data transfer media ist protected at rest and in transit.	ISO/IEC 27018:2019: - Control 13.2 GDPR: - Art. 20 EU Data Act: - Art. 29 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
-CSPs should enable open market standards (cf. “The Open Data Institute”) (additional requirements in paragraph on “Technology Standards”) for: - Shared vocabulary (meta-data): Words, Models, Taxonomies & Identifiers - Data exchange: File formats, Schemas, Data types & Data transfer methods - Guidance: Codes of practice, how to collect data & Units and measures	Ref 6.4.20	To support the transfer of outsourced services and data, is data portability supported via different data formats (e.g; JSON, XML)?	GDPR: - Art. 20 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.21	To support the transfer of outsourced services and data, is data portability supported via different technical means: API based, file exchange (online and offline)?	GDPR: - Art. 20 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.4.22	To facilitate the transfer of outsourced services and data, is data portability supported with guidance codes of practice to support the customer in his data portability journey?	GDPR: - Art. 20 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		

Chapter 6 - Portability

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Example open standards to comply with: - Egeria: opensource metadata standard, maintained by the LF AI & Data Foundation	Ref 6.4.23	To facilitate the transfer of outsourced services and data with open technical standards, is your organisation supporting integration with open standard adoption?	BCBS 239: - Principle 2 Art. 33 BSI: - Clause 21, 52 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4 EU Data Act: - Art. 29		
	Ref 6.4.24	Is your organisation adhering to any standard/Code of Conduct to facilitate the transfer of outsourced services and data with open technical standards?	BCBS 239: - Principle 2 Art. 33 BSI: - Clause 21, 52 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4 EU Data Act: - Art. 29		
	Ref 6.4.25	Is your organisation adhering to any standard/IaaS Code of Conduct Transparency Statement to facilitate the transfer of outsourced services and data with open technical standards?	BCBS 239: - Principle 2 Art. 33 BSI: - Clause 21, 52 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4 EU Data Act: - Art. 29		

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
	Ref 6.4.26	Is your organisation adhering to any standard/SaaS Code of Conduct to facilitate the transfer of outsourced services and data with open technical standards?	BCBS 239: - Principle 2 Art. 33 BSI: - Clause 21, 52 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4 EU Data Act: - Art. 29		
	Ref 6.4.27	Is your organisation able to provide any Adherence Declaration Form to facilitate the transfer of outsourced services and data with open technical standards ?	BCBS 239: Principle 2 Art. 33 BSI: - Clause 21, 52 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4 EU Data Act: - Art. 29		
- Where requested by the customer, the CSP should offer professional services in support of data portability and export.	Ref 6.4.28	To facilitate the transfer of outsourced services and data with open technical standards, are professional services offered to support the customer in his data portability process and implementation? (overlap with Q6.4.3-1)	BCBS 239: - Principle 2 Art. 33 BSI: - Clause 21, 52 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4 EU Data Act: - Art. 29		

Chapter 6 - Portability

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 6.5 CSP should be transparent with Ingress and Egress Costs					
CSPs charge customers when they export data (so called egress cost) from the cloud to anywhere else. Compared to importing data exporting data is usually more expensive. Portability of applications and data is required in certain scenarios and in most cases part of the required exit strategy. FIs must have an exit strategy in place. The cost of leaving a cloud infrastructure or a service due to substantial egress cost is in contrast to this requirement: CSPs should provide ways for temporary and agreed exceptions to the costs and be transparent about the pricing. That in case an exit is required it can be achieved in an economical way.	Ref 6.5.1	Does your organisation document ingress and egress costs at a comparable level for the respective services to asses the financial resources of exits plan?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107, 108		
	Ref 6.5.2	Does your organisation provide ways or plans that egress costs can be temporary lower or fixed to maintain the feasibility of exit plans?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107, 108		
	Ref 6.5.3	Does your organisation specify and document ingress and egress on a contract level to support business plans and to maintain the feasibility of exit plans?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107, 108		
Subchapter 6.6 CSP should provide detailed Information on Data Center Location					
FIs should know CSPs' data center physical locations to ensure proper planning for resilience and portability. Data Center information within every availability zone or region needs to be provided in a standardised format and made available directly to FIs as part of contractual obligations. Information is needed to support: - Mitigation of risks of CSP data center outages and impacts of regional disaster events impacting multiple CSP data centers - A clear understanding that each data center has access to separate power supplies and utility services as well as redundant paths that are isolated from the other data centers (in the same location / region).	Ref 6.6.1	Does your organisation provide information within zones and regions upon assigned data centers and their respective locations?	EBA/GL/2019/04 (ICT): - 3.2.3. Art. 8		
	Ref 6.6.2	Does your organisation in principle add this information to the contracts and service level agreements with FIs?	EBA/GL/2019/04 (ICT): - 3.2.3. Art. 8		
	Ref 6.6.3	Does your organisation document and make available the seperation criteria of regions/zones/data centers to ensure the effectiveness of the risk-mitigating measures of exit plans?	EBA/GL/2019/04 (ICT): - 3.2.3. Art. 8		
Subchapter 6.7 CSP should safeguard Interoperability of selected Data Centers					
It is common to establish at least two interoperable but independent data center locations, meeting national localisation requirements for redundant implementation to shift workload and to allow disaster recovery. Examples of standards to be implemented in the CSP Data Center migration solution: - Service modelling: Open-SCA (Software Composition and Analysis), USDL/SoaML/CloudML (multi-view services), EMML (mashups) - Service interfaces: OCCI (infrastructure management), CIMI (infrastructure management), EC2 (de-facto standard), TOSCA (portability), CDMI (data management) - Infrastructure: OVF (Open Virtualization Format for software on virtual machines) - CSPs should provide a managed and supported data center migration option leveraging existing standards according to the related domains.	Ref 6.7.1	Does your organisation provide supporting modules like SCA, USDL/SoaML/CloudML, EMML or equivalent solutions to facilitate undue disruption of business activities? Please specify in the comment field.	IEEE 2302-2021 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107, 108		
	Ref 6.7.2	Does your organisation provide OCCI, CIMI, EC2, TOSCA, CDMI or equivalent solutions to facilitate undue disruption of business activities? Please specify in the comment field.	IEEE 2302-2021 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107, 108		
	Ref 6.7.3	Does your organisation provide OVF for software packaging and distribution, or equivalent solutions to facilitate undue disruption of business activities? Please specify in the comment field.	IEEE 2302-2021 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107, 108		

Chapter 6 - Portability

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	**Ref. ID**	**Questions related to reg. reference / recognised standard (examples)**	**Reg. reference / recog. stand. (examples)**	**Offered / fulfilled by CSPs**	**Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.**
Subchapter 6.8 CSP should run independent Network Connections					
CSPs should establish and provide multiple independent network connection options to ensure that communication and applications, are still available in the chosen data centers/regions when (hazardous) incidents occur. Also, operational and scheduled maintenance of these network connection must be independent and respect clients' configuration, ensuring that no back-up connection is unintentionally stopped. In more detail, it should be ensured that at least one stable connection is provided by the CSP at all times and that backup and main connections are not in maintenance mode at the same time.	Ref 6.8.1	Does your organisation provide and establish multiple independent network connections for a proper ICT operations management? Please specify your approach or refer to public documentation in comment field.	EBA/GL/2019/04 (ICT): - 3.5 ff, 3.4.4. Art. 36 ISO/IEC 27001:2013		
	Ref 6.8.2	Does your organisation operate and maintain (FI's) network connection indepent for a proper ICT operations management?	EBA/GL/2019/04 (ICT): - 3.5 ff, 3.4.4. Art. 36 ISO/IEC 27001:2013		

GLOSSARY

API: Application Programming Interface
CSA: Cloud Security Alliance
CCM: Cloud Control Matrix
CSP: Cloud Service Provider
DORA: Digital Operational Resilience Act
EBA: European Banking Authority
ECB: European Central Bank
ECUC: European Cloud User Coalition
EDPB: European Data Protection Board
EEA: European Economic Area
EC: European Commission
EU: European Union
FI: Financial Institution
FIPS: Financial Information Processing Standard
GDPR: General Data Protection Regulation
HSM: Hardware Security Module
IaaS: Infrastructure as a Service
ICT: Information & Communication Technology
PaaS: Platform as a Service
SLA: Service Level Agreement
TPP: 3rd Party Provider