CHECKLIST ON ECUC POSITION PAPER 3.0 FOR CSPs

Version 2.0

02/26/2025

Contact: info@ecuc.group

Document: ECUC_Checklist_Feb_2025_v2.0xlsx

CHECKLIST ON ECUC POSITION PAPER 3.0 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 3.0. 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 Organisation
5 - Requirements on Contractual Clauses
6 - Requirements on Portability, Resilience and Exit

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 3.0 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 3.0 FOR CSPs

EXPLANATION OF COLUMNS

(B) EXCERPT FROM THE POSITION PAPER 3.0:
Copy of the respective subchapter of Position Paper 3.0.

(C) REF. ID V 1.0:
This is the internal reference ID of each question of the Checklist version 1.0.
Example: Ref. 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) REF. ID V 2.0:
This is the internal reference ID of each question of the Checklist version 2.0.
Example: V 2.0 Ref. ID 3.4.1 => the first two positions refer to the chapter and subchapter in the Position Paper 3.0, third position is a follow up number of the question.

(E) 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).

(F) REGULATORY REFERENCE / RECOGNISED STANDARD (examples):
Applicable law:
- DORA: European Digital Operational Resilience Act (Regulation (EU) 2022/2554)
- DATA ACT: Regulation (EU) 2023/2854 of 13 December 2023
- 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

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

(G) 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.

(H) 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 - Requirements on Privacy

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 CSPs are required to provide Personal Data Protection in Accordance with European General Data Protection Regulation (GDPR)						
Data protection in public cloud environments is required to ensure compliance with European data protection regulations as set out in GDPR (EU 2016/679), binding guidance of the European Data Protection Board (EDPB), relevant European Court rulings, and national requirements on member state level. Within the European Economic Area (EEA), GDPR is applicable for both, FIs (data-controller as cloud consumers) as well as for the CSPs (in their role as data-processors). Natural persons residing in the EU should be able to trust that their FIs take measures to respect and protect their privacy. This includes both contractual and technical aspects of such a relationship even when non-European service providers are used. As data processors, CSPs are independent of their place of business, accountable for the provision of 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.	Ref 2.1.1	V 2.0 Ref 2.1.1	Do your customers have unconditional access to documentation of your technical and organisational security and compliance measures for the European market?	EBA/GL/2019/02 (Outsourcing): - Background Para. 44 - Chap. 3 Para. 16 - Chap. 4 Para. 38.b - Chap. 5 Accompanying documents, recital 8 GDPR: - Art. 28, 32		
	Ref 2.1.2	V 2.0 Ref 2.1.2	Are these measures state of the art, including data protection by design and default?	ECJ Schrems II: - Recital 108 GDPR: - Art. 25, 32 - Recital 78		
Subchapter 2.2 CSPs should provide supplementary Measures to enable effective GDPR Compliance in 3rd Countries						
When entering into contracts with CSPs established headquartered outside of the EU/EEA (3rd countries), and under consideration of the European Court of Justice (C-311/18 Schrems II) states, contracts can be only an appropriate tool of transfer if the (standard) contractual clauses ensure a GDPR equivalent environment for the individual. 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, for instance, risk unauthorised 3rd country processing – this is however not always the case especially in countries where public authorities can access data beyond deviating legitimate objectives of the EU/EEA. This goes against the contractually agreed confidentiality prohibiting access to any personal data where the FI is the controller, and the data is processed on its behalf by the CSPs. The CSPs should therefore ensure technical and organisational measures to ensure compliance with GDPR in 3rd countries.	Ref 2.2.1	V 2.0 Ref 2.2.1	Do technical and organisational measures of your organisation ensure a GDPR equivalent protection for personal data in 3rd countries? Please provide more details and references in the comment field.	EBA/GL/2019/02 (Outsourcing): - Background Para. 37 subseq. - Chap. 4 Para. 72, 83 ECJ Schrems II: - Recital 134 GDPR: - Art. 44 subseq.		

Chapter 2 - Requirements on Privacy

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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						
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 a 3rd country. Hence, in the case a 3rd country can request access to personal data because the CSPs are domiciled in that country measures are required to be taken to restrict such access to ensure equivalent grounds as in the EU – normally requiring a formal Mutual Legal Assistance Treaty (MLAT) request. These measures are typically based on the principles of data security, data minimisation, anonymization or pseudonymization. In the case of pseudonymization, the CSPs 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	V 2.0 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 offering Services processing Data exclusively in the EU/EEA						
Although the EU-US Data Privacy Framework has been acknowledged to provide a level of data protection adequate to European requirements, 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 the storing and processing of customer and individual data exclusively in a dedicated country or geographic region e.g. in the EU/EEA. CSPs should ensure that global cloud services are hosted in multiple regions and that customers are not forced to rely on one region only when commissioning the services. Alternatively, CSPs must be transparent to their customers as to whether or not global services are localised in a single region.	Ref 2.4.1	V 2.0 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	V 2.0 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	V 2.0 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						
CSPs therefore must be fully transparent about cloud services that are only operated globally (so called Global services). In addition, CSPs must be fully transparent as to whether a cloud service requires transfers and/or processes personal data outside the EU. This information must be publicly accessible at any time. In addition, the CSPs 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	V 2.0 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	V 2.0 Ref 2.5.2	Is this information publicly accesible, even without a contract?	GDPR: - Art. 28 Para. 3.f		
	Ref 2.5.3	V 2.0 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 - Requirements on Privacy

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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.**
Removed from version 1.0 **Subchapter 2.6 Provide robust and multi region-based Global Services**	Ref 2.6.1		The deletion of subchapters does not allow any conclusion to be drawn that a legal or regulatory requirement has ceased to exist. It is simply to be understood as meaning that the ECUC currently sees no urgency of an explicit demand or query, or overlaps were removed.			
Subchapter 2.6 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 CSPs as 3rd party in the processing of customer data, the FI needs to be confident that the involvement of any 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 must be returned to the FI and the CSPs must certify that all data has been deleted.	Ref 2.7.1	V 2.0 Ref 2.6.1	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?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 83 GDPR: - Art. 28 Para. 3, Art. 29		
	Ref 2.7.2	V 2.0 Ref 2.6.2	Does your organisation provide confirmation of customer data deletion following contract termination/expiry?	GDPR: - Art. 28 Para. 3 lit. G		
Subchapter 2.7 CSPs should enable FIs to contract with EEA based Legal Entities						
CSPs should offer FIs to contract with their legal entities based in the EEA. Trilateral contractual relationships between FIs and which include both the CSPs EEA and non-EEA based legal entities may contain uncertainties in terms of "Who is responsible for the control and contractual safeguarding of data transfers to countries outside the EEA." The ECUC regards the CSPs EU based legal entities as the primary data processors for the personal data of the FI. If the CSPs EU based legal entities send data to non-EEA based CSPs legal entities, the EEA based legal entities act as data exporters, and thus are responsible for the performance of data transfer assessments and for the application of standard contractual clauses with their non-EEA based entities.	Ref 2.8.1	V 2.0 Ref 2.7.1	- revised - Does your organisation offer FIs to contract with your legal entities based in the EEA ?	EBA/GL/2019/02 (Outsourcing): - Background Para. 41 - Chap. 4 Para. 67.a GDPR: - Art. 28		
	Ref 2.8.2	V 2.0 Ref 2.7.2	- revised - Will your organisation apply Standard Contractual Clauses or EU acknowledged safeguards between your EEA based and non-EEA based entities?	GDPR: - Art. 28, 44, 46		
	Ref 2.8.3	V 2.0 Ref 2.7.3	- revised - When EEA based legal entities of your organisation send data to your non-EEA based legal entities, will you provide details of the data transfer assessments between these two parties?	EBA/GL/2019/02 (Outsourcing): - Background Para. 37, 41, 46 - Chap. 4 Para 68.d, 68.i GDPR: - Art. 46		

Chapter 2 - Requirements on Privacy

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 2.8 CSPs must assess the Impact of 3rd Country Transfers						
CSPs 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 any of its data importers or sub-processors where applicable 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. CSPs must 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. CSPs 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 CSPs could be deemed differently by the FI due to their specific requirements. If a CSP has reasons 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. 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 2.9.1	V 2.0 Ref 2.8.1	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)?	EBA/GL/2019/02 (Outsourcing): - Background Para 37, 41, 46 - Chap. 4 Para 68.d, 68.i ECJ Schrems 2 GDPR: - Art. 28, 44, 46, 48		
	Ref 2.9.2	V 2.0 Ref 2.8.2	Does your organisation provide the outcome of your assessment with supporting information to the FI upon request?	GDPR: - Art. 28		
	Ref 2.9.3	V 2.0 Ref 2.8.3	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		
	Ref 2.9.4	V 2.0 Ref 2.8.4	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 2.9 CSPs 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 requires CSPs to apply industry standard encryption techniques and procedures. The ECUC also encourages CSPs to be actively involved in new developments (post quantum computing etc.) to protect data adequately and effectively throughout its lifecycle. Hence, guaranteeing encryption and ensuring that the encryption keys are kept under the full control of an EU entity (of the CSP) is an option to legally transfer personal data e.g. data transferred to the US. 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 CSPs need to maintain a holistic approach towards trusted computing giving the FI the opportunity to stay fully in control and deny technically any 3rd parties, including the CSP from potentially accessing personal data in clear text.	Ref 2.10.1	V 2.0 Ref 2.9.1	Is your organisation involved or does it plan to be involved in developing of new encryption techniques, such as post quantum computing. 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?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para 68.e GDPR: - Art. 28, 32		
		V 2.0 Ref 2.9.2	- new - Is your organisation involved or does it plan to be involved in developing new encryption techniques, such as post quantum computing?	DORA 2022/2554: - Art. 9 (2)		
	Ref 2.10.2	V 2.0 Ref 2.9.3	- revised - 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 (of the CSP)?	GDPR: - Art. 28, 32		
	Ref 2.10.3	V 2.0 Ref 2.9.4	- revised - Will your organisation - upon customer request - guarantee that encryption services for data in use and corresponding encryption keys can be kept under the full control of an EU entity (of the CSP)?	DORA 2022/2554: - Art. 6 (2) - Art. 15, lit. a GDPR: - Art. 28, 32		
	Ref 2.10.4	V 2.0 Ref 2.9.5	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. 29, 32		

Chapter 2 - Requirements on Privacy

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 2.10 Disclosure Request must be challenged by the CSPs						
CSPs shall review the legality of disclosure requests and challenge them if it concludes that the request is unlawful. CSPs therefore need to pursue possibilities of appeal, seek interim measures with an objective of suspending the request and not disclose the personal data requested but instead forward the request to the individual FI. If disclosing, CSPs shall provide the minimum amount permissible. CSPs shall notify the FIs 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 CSPs are made aware to give the FIs an opportunity to object or limit access (CSPs should support embedding a kill switch or similar technologies or procedures to autonomously block 3rd country access as-soon as an access request is detected or identified). Furthermore, the CSP should deny access until the affected FI is able to take actions. If the CSPs are prohibited from notifying the FIs and/or the data subject under the laws of the country of destination, CSPs shall ensure best efforts to obtain a waiver of the prohibition or forward the request to the FIs, with the ambition to communicate as much information as possible and as soon as possible.	Ref 2.11.1	V 2.0 Ref 2.10.1	Does your organisation review the legality of disclosure requests and challenge them if you hold the request being unlawful?	GDPR: - Art. 29, 48		
	Ref 2.11.2	V 2.0 Ref 2.10.2	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, 48		
	Ref 2.11.3	V 2.0 Ref 2.10.3	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, 48, 25, 28		
	Ref 2.11.4	V 2.0 Ref 2.10.4	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	V 2.0 Ref 2.10.5	Will your organisation enable the FI to object or limit access to this data prior to disclosure?	GDPR: - Art. 28		
	Ref 2.11.6	V 2.0 Ref 2.10.6	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	V 2.0 Ref 2.10.7	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	V 2.0 Ref 2.10.8	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 2.11 Transparency Reports must be provided by the CSPs						
Where legally permissible in destination country, CSPs agree to provide the FIs, in regular intervals for the duration of the contract, with as much relevant information as possible on the requests received, 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	V 2.0 Ref 2.11.1	Will your organisation fully provide the information outlined in Chapter 2.11?	ECJ Schrems 2: - Recital 109, 139, 143 EDPB Sup. Mea.: - marginal no. 133 subseq. GDPR: - Art. 46(1), (2c)		

Chapter 2 - Requirements on Privacy

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 2.12 CSPs should provide Warrant Canary on Request of FI						
Upon request, the CSPs shall 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 CSPs place of business in a 3rd country. The CSPs 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 CSPs may have received an order and enable the FI to take mitigating actions.	Ref 2.13.1	V 2.0 Ref 2.12.1	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.	ECJ Schrems 2: - Recital 139 third sentence EDPB Sup. Mea.: - marginal no. 116. GDPR: - Art. 46(1), (2c)		
	Ref 2.13.2	V 2.0 Ref 2.12.2	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?	ECJ Schrems 2: - Recital 139 third sentence EDPB Sup. Mea.: - marginal no. 116. GDPR: - Art. 46(1), (2c)		
Subchapter 2.13 Personal Data Protection Audits should be supported						
CSPs shall be able to demonstrate compliance with its contractual safeguard provisions. In particular, CSPs shall keep appropriate documentation on the processing activities carried out on behalf of the FIs. CSPs shall make available all information necessary for the FIs 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 CSPs and shall, where appropriate, be carried out with reasonable notice.	Ref 2.14.1	V 2.0 Ref 2.13.1	- revised - Will your organisation make available all information necessary for the FI to demonstrate compliance with the contractual obligations by the means of an audit or collaborative audit (i.e. CCAG) of the processing activities at reasonable intervals?	EBA/GL/2019/02 (Outsourcing): - Recital Para. 85 ff. GDPR: - Art. 5, 28 (3h), 30, 46(1), (2c)		

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 2.14 Personal Data Breaches must be reported immediately						
In the event of a personal data breach processed for an FI regardless of whether this was government request or not, CSPs shall take appropriate measures to address the breach, including measures to mitigate their adverse effects. CSPs shall also notify the FIs without undue delay after having become aware of the breach and to allow the FIs to report the breach at the latest within 72h to the respective authority. 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, CSPs 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 CSPs performing internal investigations as to whether the breach is notifiable, as this assessment is a prerogative of the FI as data controller.	Ref 2.15.1	V 2.0 Ref 2.14.1	In the event of a personal data breach, will your organisation notify the FI without undue delay after having become aware of the breach?	EDPB WP 250 GL on pers. data breach: - p. 13 GDPR: - Art. 33 Para 2		
	Ref 2.15.2	V 2.0 Ref 2.14.2	Will your organisation allow the FI to report the breach latest within 72h to the respective regulator?	EDPB WP 250 GL on pers. data breach: - p. 13 GDPR: - Art. 33 Para. 2 - Recital 85 Para. 2, 87		
	Ref 2.15.3	V 2.0 Ref 2.14.3	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?	EDPB WP 250 GL on pers. data breach: - p. 13 subseq. GDPR: - Art. 33 Para. 3		
	Ref 2.15.4	V 2.0 Ref 2.14.4	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?	EDPB WP 250 GL on pers. data breach: - p.15 GDPR: - Art. 33 Para. 4		

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 CSPs personnel Accessing Customer Data must be traceable						
In the event where CSPs support personnel need access to cloud services, FIs must be able to grant, monitor and trail access made by such personnel. CSPs must provide details to trace and protocol these support access activities. There must be no backdoors where CSPs support personnel can access customer data/cloud services without the ability to have this access logged and monitored in an audit trail, as we explain in sub-chapter 3.3. Amongst others these activities include internal support networks. CSPs must provide a reliable "technical vault mechanism" which includes surrounding controls and processes to prevent unauthorized (administrative) access to customer data as well as meta data by any support party, CSPs support personnel or sub-contractors.	Ref 2.16.1	V 2.0 Ref 2.15.1	- revised - 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 have this access logged and monitored in an audit trail?	ECJ Schrems 2: - Recital 134 GDPR: - Art. 32 Para. 4		
	Ref 2.16.2	V 2.0 Ref 2.15.2	Does your organisation provide means to trace and protocol such support accesses by your support personnel and / or sub-contractors?	ECJ Schrems 2: - Recital 134 GDPR: - Art. 32 Para. 4		
	Ref 2.16.3	V 2.0 Ref 2.15.3	Will the ability to track and trace support personnel and/or subcontractor activities be applicable to your organisation´s internal management and support networks?	ECJ Schrems 2 Rn. 134 GDPR: - Art. 32 Para. 4		
	Ref 2.16.4	V 2.0 Ref 2.15.4	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?	ECJ Schrems 2: - Recital 134 GDPR: - Art. 32 Para. 2, 3		

Chapter 3 - Requirements on Security

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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, we believe that CSPs should provide solutions to ensure adequate security is in place.	Ref 3.1.1	V 2.0 Ref 3.1.1	Is data at rest security enabled by default, when setting up an account?	CSA CCM v4.0.5: - CEK-04 DORA 2022/2554: - Art. 9 (2)(3)		
	Ref 3.1.2	V 2.0 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 DORA 2022/2554: - Art. 9(2)(3)		
	Ref 3.1.3	V 2.0 Ref 3.1.3	Does your organisation keep your data at rest security up to date with new regulations?	CSA CCM DORA 2022/2554: - Art. 9(2)(3) EBA/GL/2019/04 (ICT)		
	Ref 3.1.4	V 2.0 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 CSPs cannot be forced to disclose the keys used to decrypt customer data without approval, consent or knowledge of the data owners. More precisely, CSPs 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 providing a scalable and managed Key Management Service (KMS) based on HSMs, including key generation, storage, exchange, rotation, re-encryption, grouping, and labelling. CSPs 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	V 2.0 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 DORA 2022/2554: - Art. 9(4), lit. d		
	Ref 3.1.6	V 2.0 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 DORA 2022/2554: - Art. 9(4), lit. D		
	Ref 3.1.7	V 2.0 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	V 2.0 Ref 3.1.8	- revised - Does your organisation´s KMS provide scalability?	CSA CCM v4.0.5: - CEK-06, 08, 10		
	Ref 3.1.9	V 2.0 Ref 3.1.9	- revised - Does your organisation´s KMS provide key operations?	CSA CCM v4.0.5: - CEK-06, 08, 10		
	Ref 3.1.10	V 2.0 Ref 3.1.10	- revised - Does your organisation´s KMS provide encryption?	CSA CCM v4.0.5: - CEK-06, 08, 10		
	Ref 3.1.11	V 2.0 Ref 3.1.11	- revised - Does your organisation´s KMS provide signatures?	CSA CCM v4.0.5: - CEK-06, 08, 10		
	Ref 3.1.12	V 2.0 Ref 3.1.12	- revised - Does your organisation´s KMS provide meta data?	CSA CCM v4.0.5: - CEK-06, 08, 10		

Chapter 3 - Requirements on Security

ECUC SECTION

CLOUD SERVICE PROVIDER SECTION

Excerpt from the Position Paper 3.0	Ref. ID V 1.0	Ref. ID V 2.0	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. CSPs should offer customers organisation-wide encryption policies and a central place to define Data at Rest encryption for all services. In general, for supported cloud services the CSPs should activate data at rest encryption by default. Furthermore, CSPs 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	V 2.0 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 DORA 2022/2554: - Art. 9(3)(4)		
	Ref 3.1.14	V 2.0 Ref 3.1.14	Does your organisation ensure the immutability of each cryptographic key operation? Please provide the details in the comment field.	CSA CCM v4.0.5: - CEK-12 DORA 2022/2554: - Art. 9(3)(4)		
	Ref 3.1.15	V 2.0 Ref 3.1.15	- revised - Does your organisation provide data at rest encryption as an enforced system policy for all services by default?	CSA CCM v4.0.5: - CEK-04 DORA 2022/2554: - Art. 9(3)(4)		
	Ref 3.1.16	V 2.0 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 DORA 2022/2554: - Art. 9(3)(4)		
	Ref 3.1.17	V 2.0 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 DORA 2022/2554: - Art. 11(2), lit.s a - c		
	Ref 3.1.18	V 2.0 Ref 3.1.18	Does your organisation provide central monitoring/reporting on key management?	CSA CCM v4.0.5: - CEK-01 DORA 2022/2554: - Art. 10		
	Ref 3.1.19	V 2.0 Ref 3.1.19	- revised - Does your organisation offer an overall view on the state of encryption of all encrypted data?	CSA CCM v4.0.5: - CEK-12 DORA 2022/2554: - Art. 9		

Chapter 3 - Requirements on Security

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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. It is the ECUC's position that it should always be transparent to the FI how and where their data is being transferred and security measures in place to protect data-in-transit (in accordance with subchapter 2.4 and 2.8). CSPs should use state-of-the-art security to secure data-in-transit, e.g., TLS version 1.3. Hence, vulnerable data security protection mechanisms should be avoided.	Ref 3.2.1	V 2.0 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 DORA 2022/2554: - Art. 9(2)(3)		
	Ref 3.2.2	V 2.0 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 DORA 2022/2554: - Art. 9(2)(3)		
To provide clarity on the data transport architecture, CSPs should provide a consistent, central place to configure and monitor data-in-transit security, rather than only per individual service.	Ref 3.2.3	V 2.0 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 CSPs internal data transfer channels and applied security measures should be made transparent to the FI.	Ref 3.2.4	V 2.0 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 DORA 2022/2554: - Art. 9(3), lit. a		
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	V 2.0 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 DORA 2022/2554: - Art. 9(3), lit. b		

Chapter 3 - Requirements on Security

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 customers and CSPs actions and the retention time should be defined by the customer. Logging and monitoring include customer service access (Access Transparency with approvals), CSP´s and customers admin access (Admin Activity/Read/Write), as well as data that has been accessed (Data Access/Read/Write).	Ref 3.3.1	V 2.0 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 DORA 2022/2554: - Art. 10		
	Ref 3.3.2	V 2.0 Ref 3.3.2	Does your organisation provide the logging of both customer and CSP actions?	CSA CCM v4.0.5: - LOG-01 ff DORA 2022/2554: - Art. 10		
	Ref 3.3.3	V 2.0 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 occurs.	Ref 3.3.4	V 2.0 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		
CSPs 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 for the service-related activities on the platform; these 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	Ref 3.3.5	V 2.0 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 DORA 2022/2554: - Art. 10		
Furthermore, customer log data should not be shared with 3rd parties without the explicit consent of the customer.	Ref 3.3.6	V 2.0 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 DORA 2022/2554: - Art. 9(3), lit.s b and d		
With respect to monitoring, there is a lack of standardised monitoring interfaces across CSPs. The ECUC encourages CSPs to provide a standard format for processing alerts and security monitoring solutions with third-party tools (e.g. Sentinel).	Ref 3.3.7	V 2.0 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 DORA 2022/2554: - Art. 10		
	Ref 3.3.8	V 2.0 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 DORA 2022/2554: - Art. 10		
	Ref 3.3.9	V 2.0 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 DORA 2022/2554: - Art. 10		
	Ref 3.3.10	V 2.0 Ref 3.3.10	Does your organisation provide out of the box management of these policies?	CSA CCM v4.0.5: - AIS-01 DORA 2022/2554: - Art. 10		

Chapter 3 - Requirements on Security

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 in the cloud, customers are interested in strictly controlled data sharing capabilities to prevent among other things data being located in unwanted locations.	Ref 3.4.1	V 2.0 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 DORA 2022/2554: - Art. 30 (2)		
CSPs 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 CSPs services and 'private endpoints', including the direction of data flow (ingress/egress).	Ref 3.4.2	V 2.0 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.		
	Ref 3.4.3 removed		The deletion of subchapters or questions does not allow any conclusion to be drawn that a legal or regulatory requirement has ceased to exist. It is simply to be understood as meaning that the ECUC currently sees no urgency of an explicit demand or query, or overlaps were removed.			
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	V 2.0 Ref 3.4.3	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 may assure an acceptable level of security and are key artifacts for cloud users when conducting assessments. For this reason, the services of CSPs should be independently certified by an accredited certification authority.	Ref 3.5.1	V 2.0 Ref 3.5.1	Can your organisation demonstrate or evidence the independent certifications provided by certified authority?	AICPA SSAE 18 BSI C5:2020 CSA STAR ISAE 3402 type II: SOC2 ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 PCI DSS		
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	V 2.0 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.	AICPA SSAE 18 BSI C5:2020 CSA STAR ISAE 3402 type II: SOC2 ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 PCI DSS		
CSPs should disclose evidence of certifications upon request by the customer. Furthermore, CSPs should provide their customers with the ability to conduct their own audits of the CSPs, alone or within the Collaborative Cloud Audit Group (CCAG). The CCAG is an initiative that aims to achieve this goal by combining the audit efforts of multiple FI's to reduce the audit burden on CSPs. Please see also subchapter 4.3 and 5.3.	Ref 3.5.3	V 2.0 Ref 3.5.3	- revised - Which of the mentioned certificates from column F do you provide. Please add additional in the comment field.	AICPA SSAE 18 BSI C5:2020 CSA STAR ISAE 3402 type II: SOC2 ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 PCI DSS		

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 (such as an user ID) and contact information (such as an email address) are identical, there's a possibility that their associated contexts may get mixed up. CSPs should therefore provide measures to associate both 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, the identity identifier and contact information should be kept separated but it should be able for them to be associated with each other. For example, if an identity cannot be used for notifications, it should be possible to associate a valid and routable email address with the identity for the use of sending notifications to and from the CSPs.	Ref 3.6.1	V 2.0 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		
CSPs 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. These should be provided, in addition to secure email using other channels that can be configured by the customer.	Ref 3.6.2	V 2.0 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, CSPs 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	V 2.0 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 - Requirements on Security

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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						
CSPs 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 cloud service models.	Ref 3.8.1	V 2.0 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.	DORA 2022/2554: - Art. 12 (5) 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 for all services storing customer data or service configurations and be manageable through a single interface.	Ref 3.8.2	V 2.0 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.	Ref 3.8.3	V 2.0 Ref 3.8.3	Are your organisation´s cloud services available in both High Availability and Disaster Recovery mode?	DORA 2022/2554: - Art. 9 (2)(3) ISO/IEC 27001:2013: - Chapter 17.2 ISO/IEC 27002:2022: - Chapter 8.14 ISO/IEC 27018:2019: - Chapter 17		
Furthermore, if CSPs perform business continuity and resilience exercises affecting customers, the customers should be informed of the process and have the ability to veto.	Ref 3.8.4	V 2.0 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 a CSP´s services to perform cryptographic tasks even when the main KMS is unavailable. This holds true especially for single region services.	Ref 3.8.5	V 2.0 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?	DORA 2022/2554: - Art. 9 (2)(3) - Art. 12 (4) 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	V 2.0 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?	DORA 2022/2554: - Art. 12 (4)(5) 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. CSPs customers should be able to customize a multi-region or select from several pre-defined multi-regions in the same geographical region.	Ref 3.8.7	V 2.0 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 - Requirements on Security

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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						
Depending on the chosen cloud deployment model, customer assets such as applications run on various underlying infrastructures managed by the CSPs. These infrastructures consist also of software, such as operating systems and management tools. Since the layer below the customer's view is only available to CSPs, the responsibility for this software stack is with the CSPs. Therefore, CSPs should provide information to allow the auditing of processes and security events in order to provide transparency to the FIs. This helps FIs to comply with EBA and DORA requirements. Where applicable CSPs should also provide detailed information related to the delivery of its service chain.	Ref 3.9.1	V 2.0 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?	DORA 2022/2554: - Art. 24 (3) - Art. 25 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 67-80		
Subchapter 3.10 IAM and Privilege Escalation						
Assets, such as the data of customers, reside in CSPs´ 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 CSPs are responsible for the delivery of a sound IAM implementation across all of their 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	V 2.0 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.	CSA CCM v4.0.5: - BCR-01 ff DORA 2022/2554: - Art. 9 (4), lit. c 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		
	Ref 3.10.2	V 2.0 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.	CSA CCM v4.0.5: - BCR-01 ff. DORA 2022/2554: - Art. 9 (4), lit. c 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		
	Ref 3.10.3	V 2.0 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. DORA 2022/2554: - Art. 9 (4), lit. c		

Chapter 3 - Requirements on Security

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 CSPs. Therefore, it should never be possible to access any other customer's assets without its explicit consent. This includes data, software, infrastructure, and containers or virtual machines. CSPs must manage adequate workload isolation controls.	Ref 3.11.1	V 2.0 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 CSPs 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	V 2.0 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 CSPs, there are different entry points for malware, such as ransomware. For the parts of the shared responsibility model the CSPs are responsible for, malware needs to be kept away from customer systems while at the same time the customers should have the ability to use specialized tools to prevent, detect, and mitigate malware impact. Thus, CSPs should provide defence mechanisms to isolate threats without disruption and alert the customer with the option to clean infected systems.	Ref 3.12.1	V 2.0 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 DORA 2022/2554: - Art. 10 (1)		
For the parts of the shared responsibility model the customers are responsible for, the CSPs should offer tools to prevent misuse and infection of its services.	Ref 3.12.2	V 2.0 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		

Chapter 4 - Requirements on Governance and Organisation

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 centre location	Ref 4.1.1	V 2.0 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.	DORA 2022/2554 : - Art. 28 (8) 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	Ref 4.1.2	V 2.0 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?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74, 75, 100 ff.		
• Contingency measures that include or risk 3rd country data transfer should be made transparent in standard contractual clauses and • Supplied information should include the CSPs´ supply chain and sub-outsourcing, where applicable.	Ref 4.1.3	V 2.0 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?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74, 75, 100 ff.		
	Ref 4.1.4	V 2.0 Ref 4.1.4	Does your organisation inform about 3rd country data transfer to monitor the security & data protection of outsourced services?	DORA 2022/2554: - Art. 6 (2) - Art 30 (2), lit. b EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74, 75, 78, 83		
	Ref 4.1.5	V 2.0 Ref 4.1.5	Is the above mentioned information provisioning referenced in your organisation´s standard contractual clauses?	DORA 2022/2554: - Art. 30 (3), lit. c EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75, 100 ff.		

Chapter 4 - Requirements on Governance and Organisation

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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						
To ensure 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 and • Supply-chain information detailing the dataflow, data exchange and data location/region between the CSPs and each sub-contractor for the related cloud services.	Ref 4.2.1	V 2.0 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?	DORA 2022/2554: - Art. 29 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 76 ff.		
	Ref 4.2.2	V 2.0 Ref 4.2.2	Does your organisation inform about changes in sub-contractors to control and manage the risk of outsourced arrangement?	DORA 2022/2554: - Art. 29 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 76 ff.		
	Ref 4.2.3	V 2.0 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	V 2.0 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	V 2.0 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 - Requirements on Governance and Organisation

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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.**
Old Subchapter 4.3 Exit Strategy Requirements moved to Subchapter 6.1	Ref 4.3.1 Ref 4.3.2					
Subchapter 4.3 CSP Audits and Oversight						
The ECUC propose simplifications in audit procedures insofar as the cloud service offerings are not checked or audited by every FI, but centrally at the CSPs. Collaborative audits organised by the financial industry should become a generally accepted approach by CSPs and be free of charge. Different institutions form a collaborative team to audit one specific CSP. Audit results can be regarded valid within the respective individual institution. Collaborative audits are already supported by the EBA Guidelines on Outsourcing Arrangements (chapter 13.3, Para. 91.a). If a CSP is not designated as critical per definition under DORA, they will not be under direct oversight by European Supervisory Authorities. As a consequence, those CSPs will only be audited as part of an audit conducted at an FI. On this basis a particular CSP is audited multiple times whenever FIs as CSP customers are inspected on their public outsourcing activities. Therefore, we suggest national and European supervisors should form collaborative audit teams to audit CSPs across countries and for all FIs being customers of CSPs. Such an approach could improve consistency of observations and additionally would be more efficient. However, the institutions specific cloud adoption is still inspected individually and resulting observations are assigned to the respective institution (please see also subchapter 5.3).	Ref 4.4.1	V 2.0 Ref 4.3.1	Does your organisation support pooled audits performed by FIs themselves to use audit resources more efficiently and to decrease organisational burden?	DORA 2022/2554: - Art. 30 (3), lit. i EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91		

Chapter 5 - Requirements on Contractual Clauses

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 Data						
The contract must set out the locations where ICT Services will be provided and where data will be stored and processed. Also, it must set out that the CSPs will inform the FI of any changes to these locations. The contract must also include provisions on the availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data. Where relevant, the contract must also contain provisions needed to comply with banking secrecy requirements. The contract must also set out how access, recovery and return of data, in an easily accessible format, is ensured in case of termination of the contract or insolvency, resolution or discontinuation of business processes of the CSPs.		V 2.0 Ref. 5.1.1	- new - Does your contract set out the location where your services are provided from and where data will be processed?	DORA 2022/2554: - Art. 30 (2), lit. b EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75f		
		V 2.0 Ref. 5.1.2	- new - Do you notify the FI if the location where your services are provided from or the data processing location change?	DORA 2022/2554: - Art. 30 (2), lit. b EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75f		
		V 2.0 Ref. 5.1.3	- new - Does your contract include provisions of the avialability, integrity and confidentiality in relation to the protection of data?	DORA 2022/2554: - Art. 30 (2), lit. c EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75g		
		V 2.0 Ref. 5.1.4	- new - Do you offer specific clauses regarding banking secrecy requirements?	DORA 2022/2554: - Art. 30 (2), lit. C		
		V 2.0 Ref. 5.1.5	- new - Do you provide dedicate legal language how access, recovery and return of data will be managed?	DORA 2022/2554: - Art. 30 (2), lit. d EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75m, 99		
		V 2.0 Ref. 5.1.6	- new - Do you provide solutions for insolvency or in case of discontinuation of your business processes?	DORA 2022/2554: - Art. 30 (2), lit. D		
Summary		V 2.0 Ref. 5.1.7	- new - **Has your organisation regulated all the above requirements in the standard contract or a specific contractual amendment?**			

Chapter 5 - Requirements on Contractual Clauses

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 Resilience						
The contract must set out that the CSPs provide assistance to the FI, at no additional cost or at a cost determined beforehand, in case of ICT incidents. Next to that, the contract must set out the conditions for the CSPs participating in the resilience training of the FI. Contracts for ICT Services that support critical or important functions must oblige the CSPs to implement and test business contingency plans and appropriate ICT security measures, tools and policies. CSPs must also be obliged to participate in the FIs TLPT where relevant.	-	V 2.0 Ref. 5.2.1	- new - What type of ICT incidents do you inform FIs about?	DORA 2022/2554: - Art. 10 (1)(2)(3)		
		V 2.0 Ref. 5.2.2	- new - Do you provide assistance to the FI in case of ICT incidents?	DORA 2022/2554: - Art. 30 (2), lit. F		
		V 2.0 Ref. 5.2.3	- new - Will customer be charged in case of assistance regarding ICT incidents? If yes, please specify if your contract sets out the conditions.	DORA 2022/2554: - Art. 30 (2), lit. f		
		V 2.0 Ref. 5.2.4	- new - Do you agree to participate in the FI's security awareness programmes and digital operation resilience training?	DORA 2022/2554: - Art. 30 (2), lit. i		
		V 2.0 Ref. 5.2.5	- new - Do you implement and test BCM plans and appropriate security measures?	DORA 2022/2554: - Art. 30 (3), lit. c		
		V 2.0 Ref. 5.2.6	- new - Do you agree to participate and fully coopearte in the FI's TLPT as required under DORA? If you indicate that you only partially or not meet the requirements, please provide more information in the comment field.	DORA 2022/2554: - Art. 30 (3), lit. d		
Summary		V 2.0 Ref. 5.2.7	- new - **Has your organisation regulated all the above requirements in the standard contract or a specific contractual amendment?**			

Chapter 5 - Requirements on Contractual Clauses

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 Audit Rights						
To meet industry's obligations to audit and be audited, audit rights should be granted per standard contractual clauses. These audit rights include any service, infrastructure, etc. involved in fulfilling the cloud services offered to the FIs. In addition, these audit rights must be cascaded to sub-contractors in scope. With reference to the requirements set out in the EBA Guidelines on Outsourcing Arrangements (EBA/GL/2019/02, paragraph 13.3) and DORA (Article 30.2.g, 30.3.e), the written outsourcing arrangements should at least include the unrestricted right to inspect and audit CSPs, especially with regard to the critical or important outsourced function. This would include but not be restricted to data centres. The auditors also must be allowed to take copies of relevant documentation (please see also subchapter 3.5 and 4.3).	Ref 5.1.1	V 2.0 Ref 5.3.1	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?	DORA 2022/2554: - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.p, 85.ff		
	Ref 5.1.2	V 2.0 Ref 5.3.2	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?	DORA 2022/2554: - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 87		
	Ref 5.1.3	V 2.0 Ref 5.3.3	Does your service arrangement make third party certifications, including related evidences or reports, available to the customer?	DORA 2022/2554: - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91.b		
	Ref 5.1.4	V 2.0 Ref 5.3.4	Does your service arrangement make third party audits or internal audit reports available to the customer?	DORA 2022/2554: - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91.b		
	Ref 5.1.5	V 2.0 Ref 5.3.5	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?	DORA 2022/2554: - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. Para. 93.b		
	Ref 5.1.6	V 2.0 Ref 5.3.6	Does your organisation provide the certifications and evidences or reports on a regularly basis?	DORA 2022/2554: - Art. 28 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 93.c		

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 5.1.7	V 2.0 Ref 5.3.7	Does your organisation ensure that key systems and controls will be covered in future versions of your certification or audit report?	DORA 2022/2554: - Art. 28 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 93.d		
	Ref 5.1.8	V 2.0 Ref 5.3.8	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?	DORA 2022/2554: - Art. 28 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 93.g		
	Ref 5.1.9	V 2.0 Ref 5.3.9	Does your organisation grant the contractual right to perform individual audits at banks' discretion with regard to the outsourcing of critical or important functions?	DORA 2022/2554: - Art. 28 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 93.h		
	Ref 5.1.10	V 2.0 Ref 5.3.10	Does your service arrangement permit pooled audits?	DORA 2022/2554: - Art. 28 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91 a		
	Ref 5.1.11	V 2.0 Ref 5.3.11	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?	DORA 2022/2554: - Art. 28 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91.b		
Summary	Ref 5.1.12	V 2.0 Ref 5.3.12	**Has your organisation regulated all the above requirements in the standard contract or a specific contractual amendment?**			

Chapter 5 - Requirements on Contractual Clauses

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 5.4 Sub-Contracting						
In accordance with DORA Article 29 and 30 of regulation (EU) 2022/2554 CSPs provide information regarding sub outsourcing at any time without limitations, to perform its risk assessment and to decide whether subcontracting is allowed for the FI, also in case of material changes to subcontracting arrangements. If a CSP decides to subcontract its ICT Services that support critical or important functions for a FI, the CSP should allow the FI to conduct appropriate due diligence on the CSP's subcontracting capabilities. The CSP should enable the FI to review the processes it uses to select and assess subcontractors, and keep the FI informed about all subcontractors involved. Additionally, the CSP should ensure that the FI can verify that all relevant terms and conditions are included in the contracts with subcontractors. The CSP must also allow the FI to evaluate the CSP's ability to effectively monitor its subcontractors. This includes ensuring the CSP has the necessary skills, resources, and expertise, adheres to proper information security standards, and maintains an appropriate organizational structure with risk management, internal controls, and procedures for incident reporting and response.	Ref 5.2.1	V 2.0 Ref 5.4.1	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?	DORA 2022/2554: - Art. 29 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 55.g, 67		
	Ref 5.2.2	V 2.0 Ref 5.4.2	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?	DORA 2022/2554: - Art. 29 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 79		
	Ref 5.2.3	V 2.0 Ref 5.4.3	Does your organisation provide any information during the due diligence phase to support the Financial Institute to evaluate the potential risk?	DORA 2022/2554: - Art. 28 - Art. 29 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 69		

Chapter 5 - Requirements on Contractual Clauses

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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.**
If the CSP wishes to appoint a new subcontractor or intends to make any changes concerning the addition or replacement of any subcontractor, it should notify the FIs in advance (at least 90 days), in writing, to provide the FI with the opportunity to object to any such changes. If the changes to subcontracting cannot be agreed by the FI, the FI should be granted a special right of termination, including termination exit support.	Ref 5.2.4	V 2.0 Ref 5.4.4	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?	DORA 2022/2554: - Art. 29 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 42.d.ii, 44.f, 78.e		
	Ref 5.2.5	V 2.0 Ref 5.4.5	Does your organisation ensure that objections to the suboutsourcing by the FI are duly taken into account?	DORA 2022/2554: - Art. 28 - Art. 29 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 78.f		
	Ref 5.2.6	V 2.0 Ref 5.4.6	Does your organisation inform customers in advance to perform a risk assessment? Please specify how many days in advance in the comment field.	DORA 2022/2554: - Art. 28 - Art. 29 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 44.f, 78.d, 78.f		
	Ref 5.2.7	V 2.0 Ref 5.4.7	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		
	Ref 5.2.8	V 2.0 Ref 5.4.8	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	V 2.0 Ref 5.4.9	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		
CSPs must have appropriate due diligence processes implemented to select and assess its subcontractors, must assess all risks, and involve the FI in the decision-making. CSPs must ensure that the relevant terms and conditions of the services contract with the FI are replicated in the contract with the subcontractor. The CSP must publish an overview of subcontractors to FIs so they can assess any risks that subcontracting by the CSP might cause. CSPs must monitor the subcontracted services. The contract with the subcontractor must set out security standards, any additional security features, the service levels, incident response plans and business continuity plans applicable to the subcontractors. The subcontractor must also grant the FI and the regulators the same audit, inspection, and information rights as the CSPs. Subcontracting does not absolve the CSPs from their obligations to ensure continuous provision of services, even in case of a failure by the subcontractor.		V 2.0 Ref 5.4.10	- new - Does your organisation have appropriate due diligence processes implemented to select and assess its subcontractors?	DORA 2022/2554: - Art.28 - Art. 29 - Art. 30		
		V 2.0 Ref 5.4.11	- new - Does your organisation provide transparency on subcontractors and subcontracting chains to enable FIs to effectively monitor ICT services? Please provide details or references in the comment field, which mechanisms you use to publish an overview of your subcontractors/subcontracting chains (e.g., publication on the website, upon request).	DORA 2022/2554: - Art. 29 (2) - Art. 30		
		V 2.0 Ref 5.4.12	- new - Does your organisation monitor the subcontracted services?	DORA 2022/2554: - Art. 29 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 78.c., 80		
			- new - Does your organization provide a contractual commitment that you remain fully liable for continuous provision of services, even in case of failure by the subcontractor?	DORA 2022/2554: - Art. 29 - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 78.c., 80		
Summary	Ref 5.2.10	V 2.0 Ref 5.4.13	**Has your organisation regulated all the above requirements in the standard contract or a specific contractual amendment?**			

Chapter 5 - Requirements on Contractual Clauses

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 5.5 Service Descriptions and Service Level Agreements						
The contract must provide for a clear description of the ICT services, including service levels and updates and revisions thereof. For ICT services supporting critical or important functions these must include precise quantitative and qualitative performance targets to enable effective monitoring and must include that appropriate corrective actions must be taken when service levels are not met. The contract must also provide for reporting of any development that may have a material impact on the CSPs´ ability to meet the service levels.		V 2.0 Ref 5.5.1	- new - Does your organisation provide a clear description of ICT Services in accordance with DORA?	DORA 2022/2554: - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.i		
In accordance with EBA Guidelines on Outsourcing and DORA, CSPs should provide clear financial obligations within the contract.	Ref 5.3.1	V 2.0 Ref 5.5.2	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.	DORA 2022/2554: - Art. 30 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	V 2.0 Ref 5.5.3	Does your organisation provide stable Terms and Conditions for your services for an agreed contract period?	DORA 2022/2554: - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.i		
Likewise, the CSPs should only change the services 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	V 2.0 Ref 5.5.4	Does your organisation provide backward compatibility for any service change?	DORA 2022/2554: - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 5.3.4	V 2.0 Ref 5.5.5	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?	DORA 2022/2554: - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
or that a change or termination of the service will be announced with a prenotification period and without undue delay.	Ref 5.3.5	V 2.0 Ref 5.5.6	Does your organisation offer prenotification periodes in case of major changes or termination of services? Please provide more details in the comment field.	DORA 2022/2554: - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
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. Clear communication channels at both CSPs as well as FIs should be included to discuss SLA performance, and to escalate SLA performance issues to appropriate management levels when necessary.	Ref 5.3.6	V 2.0 Ref 5.5.7	Does your SLA include performance metrics and permanent monitoring and reporting?	DORA 2022/2554: - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.h, 75.i, 75.p, 82, 85, 87, 88, 90, 91b, 92, 93		

Chapter 5 - Requirements on Contractual Clauses

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 CSPs should offer additional communication channels to transmit critical event and service level information (e.g. on data breaches, security incidents, 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 of whether the CSPs have concluded that the customers are impacted or not. The FIs must have the ability to assess impact and not only rely on the CSPs´ impact analysis.	Ref 5.3.7	V 2.0 Ref 5.5.8	- revised - Does your organisation offer dedicated communication channels and competent contacts for critical events, breaches, security incidents, penetration tests and logfile issues?	DORA 2022/2554: - Art. 30 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.j, 98, 92		
	Ref 5.3.8	V 2.0 Ref 5.5.9	Does your organisation inform the customer about events in any case, not only if the customer is impacted?	DORA 2022/2554: - Art. 30 (2) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.j, 85, 87, 88		
	Ref 5.3.9	V 2.0 Ref 5.5.10	Does your organisation offer Financial Institutions impact analyses in addition to your own?	DORA 2022/2554: - Article 30 (2) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.h, 75.i, 75.p, 93.g		
	Ref 5.3.10 removed		The deletion of subchapters or questions does not allow any conclusion to be drawn that a legal or regulatory requirement has ceased to exist. It is simply to be understood as meaning that the ECUC currently sees no urgency of an explicit demand or query, or overlaps were removed.			
Any changes to product terms (incl. Financial Service Amendments, Data Processing Agreements and Service Level Agreements) should be highlighted at paragraph level in order to facilitate FI identification of the exact change and subsequent impact analysis. Documentation of changes should be logged by the CSPs to allow for back-tracking any changes that have happened over time.	Ref 5.3.10	V 2.0 Ref 5.5.11	Does your organisation offer a version management with the ability to track changes for all contracts and SLA?	DORA 2022/2554: - Art. 30 (2), lit. e EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.i		
All terms, changes, and level of information should apply without exception to all FIs and not only to individual institutions.	Ref 5.3.11	V 2.0 Ref 5.5.12	Does your organisation state all terms/prenotification periods, communication channels tests etc. in a standard contract or a standard FSA?	DORA 2022/2554: - Art. 30 (2) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74		
Summary		V 2.0 Ref 5.5.13	- new - **Has your organisation regulated all the above requirements in the standard contract or a specific contractual amendment?**	DORA 2022/2554: - Art. 30 (2)		

Chapter 5 - Requirements on Contractual Clauses

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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.**
Removed from version 1.0 **Subchapter 5.4 Insurance**	Ref 5.4.1 Ref 5.4.2 Ref 5.4.3		The deletion of subchapters does not allow any conclusion to be drawn that a legal or regulatory requirement has ceased to exist. It is simply to be understood as meaning that the ECUC currently sees no urgency of an explicit demand or query, or overlaps were removed.			
Subchapter 5.6 Termination						
The contract must clarify the termination rights and notice periods in accordance with the expectations of the regulators. According to the Draft ECB Cloud Guide, under DORA FIs must at least be able to terminate in case of ongoing inadequate performance, serious breaches of the contract or applicable laws and regulations or if the CSPs decide to excessively increase the price of the ICT Services. Next to that, FIs must be able to terminate in case of: • merger or sale of the CSPs • a material change to the subcontracting chain • relocation of CSPs headquarters or data centre to another jurisdiction • significant change to the host country's social, political or economic climate • a change in laws affecting the ICT Services, data location or data processing • significant changes to the management of cybersecurity risk by CSPs or in the subcontracting chain • continuous failure to achieve service levels or substantial loss of service or • failures to successfully execute exit tests. In case of termination, the contract for ICT Services supporting critical or important functions of the FI must provide for an adequate transition period during which the CSPs will continue to provide the required ICT Services to reduce the risk of disruption in the FI or to ensure its effective resolution and restructuring and allowing the FI to migrate to other CSPs or move the services back in-house.		V 2.0 Ref 5.6.1	- new - Do you support termination rights in case of inadequate performance, serious breaches or applicable laws or excessively increasing prices?	DORA 2022/2554: - Art. 28 (7)(10) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 98a		
		V 2.0 Ref 5.6.2	- new - Does you contract or amandement contain notice periods? Please specify the periods you are offering to you customers.	DORA 2022/2554: - Art. 28 (7)(10)		
		V 2.0 Ref 5.6.3	- new - Do you support termination rights in case of merger or sale ? (CSP side)	DORA 2022/2554: - Art. 28 (7)(10)		
		V 2.0 Ref 5.6.4	- new - Do you support termination rights in case of material change of subcontracting chains?	DORA 2022/2554: - Art. 28 (7)(10) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 98c		
		V 2.0 Ref 5.6.5	- new - Do you support termination rights in case of relocation of headquarters or DCs to another jurisdinction?	DORA 2022/2554: - Art. 28 (7)(10)		
		V 2.0 Ref 5.6.6	- new - Do you support termination rights in case of continuous failure to achieve service levels or substancial loss of services?	DORA 2022/2554: - Art. 28 (7)(10) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 98b		
		V 2.0 Ref 5.6.7	- new - Do you support termination rights in case of failure to succesfully execute exit tests?	DORA 2022/2554: - Art. 28 (7)(10)		
		V 2.0 Ref 5.6.8	- new - Do you offer an adequate transition period? Please specify how long.	DORA 2022/2554: - Art. 28 (7)(10)		
Summary		V 2.0 Ref 5.6.9	- new - **Has your organisation regulated all the above requirements in the standard contract or a specific contractual amendment?**			

Chapter 6 - Requirements on Portability, Resilience and Exit

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 Exit Strategy Requirements						
The EBA Guidelines on Outsourcing Arrangements and DORA require FIs as part of their risk assessment to have an exit strategy in place when outsourcing any "critical or important function" to CSPs. This is to cover relevant exit triggering events, e.g. bankruptcy of CSP, sanctions, a changing legal environment, and/or a commercial decision by a FI. Relevant exit triggering events must be observable, 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. The ECUC therefore asks to outline a feasible period of time for an exit plan execution that is connected to the materiality assessment of the outsourcing. For an adequate transition period the CSPs should: • Continue to provide the contracted cloud services with a view to reduce the risk of disruption at the financial entity or to ensure the FI's effective resolution and restructuring • Allow the financial institution to migrate to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided.	Ref 4.3.1	V 2.0 Ref 6.1.1	Does your organisation duly inform about discontinuation of used services or contractual arrangements to prevent an unexpected interruption of outsourced arrangements? Please specify the days in advance, like e.g. 180 days in the comment field.	DORA 2022/2554: - Art. 28 (8) - Art. 30 (2), lit.s d and h EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 42, 76 ff., 106		
	Ref 4.3.2	V 2.0 Ref 6.1.2	Does your organisation offer a dedicated post-termination period?	DORA 2022/2554: - Art. 28 (8) - Art. 30 (2), lit.s d and h EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 42, 76 ff., 106		
Subchapter 6.2 CSPs should apply internationally recognized Standards						
CSPs should make sure to apply internationally recognized 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), ANSSI (Agence nationale de la sécurité des systèmes d'information): SecNumCloud • CSA (Cloud Security Alliance): STAR (Security, Trust, Assurance, and Risk) In order to demonstrate certification to standards from these bodies, adherence to these standards should be publicly documented by CSPs.	Ref 6.1.1	V 2.0 Ref 6.2.1	- revised - Does your organisation in general apply internationally recognized 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	V 2.0 Ref 6.2.2	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	V 2.0 Ref 6.2.3	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	V 2.0 Ref 6.2.4	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	V 2.0 Ref 6.2.5	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	V 2.0 Ref 6.2.6	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	V 2.0 Ref 6.2.7	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		

Chapter 6 - Requirements on Portability, Resilience and Exit

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 CSPs should offer Open-Source Technology and Standards						
CSPs should embrace open-source technologies and provide services based on such 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.	V 2.0 Ref 6.3.1	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		
Subchapter 6.4 CSPs should work towards creating Portability Standards for Commodity Services						
CSPs should support the emergence of commodity services, i.e. services that are provided by each CSP without functional differentiators, by establishing portability standards for such services. Being able to prove that commodity services can be ported quickly and reliably from CSP to CSP will allow FIs to shift focus to building up risk and resilience management for non-commodity services. This will enable FIs to build new value generating use cases and likely increase usage of non-commodity services.		V 2.0 Ref 6.4.1	- new - Which technical and/or organisational mechanisms does your organisation have in place to support data/application portability?	DORA 2022/2554: - Art. 33 (3), lit. f		
		V 2.0 Ref 6.4.2	- new - Does your organisation perform regular interoperability tests with other CSPs?	DORA 2022/2554: - Art. 33 (3), lit. f		
Subchapter 6.5 CSPs should provide Methods and Tools to allow Workload Portability						
CSPs should strongly support FIs in the performance of their exit plans for their workloads, data, services and applications as required by EBA Guidelines on Outsourcing Arrangements, DORA and Data Act. 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 migration to the most widely used commercial and open-source infrastructures, networks, platforms, and databases. Tools, provided e.g. interfaces, should enable uniform and diverse migrations from any supported source within the CSPs environment to a target environment. • CSPs should provide or support industry standard tools to create infrastructure as 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 or interoperable with other cloud platforms or provide other alternatives, such as licenses for desktop installations. The exception here would be SaaS CSP proprietary solutions that require cloud-native capabilities to provide the service(s) to the customer. Alternatives are especially relevant for productivity, communication and collaboration 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	V 2.0 Ref 6.5.1	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?	Data Act - Art. 25 - Art. 30 DORA 2022/2554: - Art. 33 (3), lit. (f) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.3.2	V 2.0 Ref 6.5.2	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?	DORA 2022/2554: - Art. 33 (3), lit. (f) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.3.3	V 2.0 Ref 6.5.3	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?	DORA 2022/2554: - Art. 33 (3), lit. (f) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.3.4	V 2.0 Ref 6.5.4	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?	DORA 2022/2554: - Art. 33 (3), lit. (f) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		
	Ref 6.3.5	V 2.0 Ref 6.5.5	Does your organisation have APIs or connectors for migration to other cloud platforms or provide alternatives?	DORA 2022/2554: - Art. 33 (3), lit. (f) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107		

Chapter 6 - Requirements on Portability, Resilience and Exit

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 6.6 CSPs should provide Standardised Data Formats and Export Processes						
CSPs should provide standardised data formats and processes for data extraction and transport to other environments and platforms. The following list requirements only covers data portability and export requirements not already covered in previous chapters, e.g. Chapter 2 Requirements on Privacy: • CSPs 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	V 2.0 Ref 6.6.1	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?	DORA 2022/2554: EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 - Art. 28 (8) EU Data Act: - Art. 24, 26 GDPR: - Art. 20 ISO/IEC 27018:2019: - Control 18.1		
	Ref 6.4.2	V 2.0 Ref 6.6.2	To facilitate the transfer of oursourced services and related data, is data portability part of the standard offered SLA?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para 107, 108 EU Data Act: - Art. 24, 26 GDPR: - Art. 20 ISO/IEC 27018:2019: - Control 18.1		
	Ref 6.4.3	V 2.0 Ref 6.6.3	To facilitate the transfer of oursourced services and related data, is data portability supported by internal processes of your organisation?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para 107, 108 EU Data Act: - Art. 24, 26 GDPR: - Art. 20 ISO/IEC 27018:2019: - Control 18.1		
	Ref 6.4.4	V 2.0 Ref 6.6.4	To facilitate the transfer of oursourced services and related data, is data portability supported by an information transfer registry?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para 107 EU Data Act: - Art. 24, 26 GDPR: - Art. 20 ISO/IEC 27018:2019: - Control 18.1		
	Ref 6.4.5 removed	pleas see V 2.0 Ref 6.6.18				

Chapter 6 - Requirements on Portability, Resilience and Exit

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 6.4.6 removed	pleas see V 2.0 Ref 6.6.16				
	Ref 6.4.7	V 2.0 Ref 6.6.5	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?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 24, 26 GDPR: - Art. 20 ISO/IEC 27018:2019: - Control 18.1		
	Ref 6.4.8	V 2.0 Ref 6.6.6	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?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 24, 26 GDPR: - Art. 20 ISO/IEC 27018:2019: - Control 18.1		
• Data portability includes both data and meta-data which gives the data its meaning. Amongst others these are operational data, secrets, cryptographic material, metadata, confidentiality, and their backups as well.	Ref 6.4.9	V 2.0 Ref 6.6.7	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)?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 24, 26 GDPR: - Art. 20 ISO/IEC 27018:2019: - Control 18.1		
	Ref 6.4.10	V 2.0 Ref 6.6.8	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?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 24, 26 GDPR: - Art. 20		

Chapter 6 - Requirements on Portability, Resilience and Exit

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 6.4.11	V 2.0 Ref 6.6.9	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)?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 24, 26 GDPR: - Art. 20		
	Ref 6.4.12	V 2.0 Ref 6.6.10	To support the transfer of outsourced services and data to alternative providers, is the provided data export containing a set of backup snap-shots?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 24, 26 GDPR: - Art. 20		
	Ref 6.4.13	V 2.0 Ref 6.6.11	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)?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 24, 26 GDPR: - Art. 20		
	Ref 6.4.14	V 2.0 Ref 6.6.12	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?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 24, 26 GDPR: - Art. 20		
	Ref 6.4.15	V 2.0 Ref 6.6.13	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)?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 24, 26 GDPR: - Art. 20		
	Ref 6.4.16	V 2.0 Ref 6.6.14	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?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 24, 26 GDPR: - Art. 20		

Chapter 6 - Requirements on Portability, Resilience and Exit

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 data integrity, availability and privacy need to be ensured. • Customers must be able to execute data portability and export encrypted data in a cost-effective way. • 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	V 2.0 Ref 6.6.15	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?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 24, 26 GDPR: - Art. 20 ISO/IEC 27018:2019: - Control 16.11		
	Ref 6.4.18	V 2.0 Ref 6.6.16	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)?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 24, 26, 29 GDPR: - Art. 20 ISO/IEC 27018:2019: - Control 13.2, 18.1		
	Ref 6.4.19	V 2.0 Ref 6.6.17	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.	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 29 GDPR: - Art. 20 ISO/IEC 27018:2019: - Control 13.2		
• 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	V 2.0 Ref 6.6.18	To support the transfer of outsourced services and data, is data portability supported via different data formats (e.g; JSON, XML)?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 EU Data Act: - Art. 24, 26 GDPR: - Art. 20 ISO/IEC 27018:2019: - Control 18.1		
	Ref 6.4.21	V 2.0 Ref 6.6.19	To support the transfer of outsourced services and data, is data portability supported via different technical means: API based, file exchange (online and offline)?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 GDPR: - Art. 20		
	Ref 6.4.22	V 2.0 Ref 6.6.20	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?	DORA 2022/2554: - Art. 28 (8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 GDPR: - Art. 20		

Chapter 6 - Requirements on Portability, Resilience and Exit

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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	V 2.0 Ref 6.6.21	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 DORA 2022/2554: - Art. 28 (8) EU Data Act: - Art. 29 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4		
	Ref 6.4.24	V 2.0 Ref 6.6.22	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 DORA 2022/2554: - Art. 28 (8) EU Data Act: - Art. 29 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4		
	Ref 6.4.25	V 2.0 Ref 6.6.23	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 DORA 2022/2554: - Art. 28 (8) EU Data Act: - Art. 29 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4		

Chapter 6 - Requirements on Portability, Resilience and Exit

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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	V 2.0 Ref 6.6.24	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 DORA 2022/2554: - Art. 28 (8) EU Data Act: - Art. 29 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4		
	Ref 6.4.27	V 2.0 Ref 6.6.25	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 DORA 2022/2554: - Art. 28 (8) EU Data Act: - Art. 29 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4		
• Where requested by the customer, the CSPs should offer professional services in support of data portability and export.	Ref 6.4.28	V 2.0 Ref 6.6.26	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?	BCBS 239: - Principle 2 Art. 33 BSI: - Clause 21, 52 DORA 2022/2554: - Art. 28 (8) EU Data Act: - Art. 29 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4		

Chapter 6 - Requirements on Portability, Resilience and Exit

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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.**
Removed from version 1.0 **Subchapter 6.7 CSP should safeguard Interoperability of selected Data Centers**	Ref 6.7.1 Ref 6.7.2 Ref 6.7.3		The deletion of subchapters does not allow any conclusion to be drawn that a legal or regulatory requirement has ceased to exist. It is simply to be understood as meaning that the ECUC currently sees no urgency of an explicit demand or query, or overlaps were removed.			
Subchapter 6.7 CSPs should be transparent about Ingress and Egress Costs						
CSPs may 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 conflict with this requirement. To avoid a vendor lock-in, we ask CSPs to be fully transparent about egress costs when leaving the CSPs´ cloud environments.	Ref 6.5.1	V 2.0 Ref 6.7.1	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	V 2.0 Ref 6.7.2	- revised - Does your organisation provide ways or plans that egress costs can be fully removed to maintain the feasibility of exit plans?	DORA 2022/2554: - Art. 28 (4)(8) EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107, 108		
	Ref 6.5.3	V 2.0 Ref 6.7.3	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 6.8 CSPs should provide detailed Information on Data Center Location						
FIs need to know CSPs data center physical locations including subcontracted data centers to ensure proper risk assessment and consequently to allow adequate 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. Such information must be shared pro-actively by CSPs to FIs whenever changes occur. Information is needed to support: • Mitigation of risks of CSPs data center outages and impacts of regional disaster events impacting multiple CSPs data centers • A clear understanding that each data center is resilient on its own. For example, 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	V 2.0 Ref 6.8.1	- revised - Does your organisation provide information with regards to the location of the data centers within zones and regions?	DORA 2022/2554: - Art. 30 (2), lit. (b) EBA/GL/2019/04 (ICT): - 3.2.3. Art. 8		
	Ref 6.6.2	V 2.0 Ref 6.8.2	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	V 2.0 Ref 6.8.3	- revised - Does your organisation document and provide 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		

Chapter 6 - Requirements on Portability, Resilience and Exit

ECUC SECTION					CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 3.0	**Ref. ID V 1.0**	**Ref. ID V 2.0**	**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 6.9 CSPs should run independent Network Connections						
CSPs should establish and provide multiple independent and physically segregated network connection options using diverse paths to ensure that communication and applications, are still available in the chosen data centers/regions when incidents occur. Also, operational and scheduled maintenance of these network connections 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 CSPs at all times and that backup and main connections are not in maintenance mode at the same time.	Ref 6.8.1	V 2.0 Ref 6.9.1	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.	DORA 2022/2554: - Art. 11 (5) EBA/GL/2019/04 (ICT): - 3.5 ff, 3.4.4. Art. 36 ISO/IEC 27001:2013		
	Ref 6.8.2	V 2.0 Ref 6.9.2	Does your organisation operate and maintain (FI's) network connection indepent for a proper ICT operations management?	DORA 2022/2554: - Art. 11 (5) EBA/GL/2019/04 (ICT): - 3.5 ff, 3.4.4. Art. 36 ISO/IEC 27001:2013		
Subchapter 6.10 Routing of Data in Transit						
If applicable, CSPs should provide capabilities to prevent data in transit from flowing through countries that are considered high-risk for FI's from a geo-political perspective.				GDPR - Art. 28 Para. 3 - Art. 32 - Art. 44-46		

GLOSSARY

Abbreviation	Definition
API	Application Programming Interface
CER	Critical Entities Directive
CNCF	Cloud Native Computing Foundation
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
CTPPs	Critical Third Party Providers
ECUC	European Cloud User Coalition
EDPB	European Data Protection Board
EEA	European Economic Area
ESA	European Supervisory Authorities
EU	European Union
FI	Financial Institution
FIPS	Financial Information Processing Standard
FSA	Financial Service Addendum
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HSM	Hardware Security Module
IaaS	Infrastructure as a Service
IAM	Identity & Access Management
ISO	International Organization for Standardization
ITS	Implementing Technical Standards
JSON	JavaScript Object Notation
KMS	Key Management Service
LF AI & Data Foundation	Linux Foundation Artificial Intelligence & Data Foundation
MLAT	Mutual Legal Assistance Treaty
NCAs	National Competent Authorities
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
PSD2	revised Payment Services Directive
RTS	Regulatory Technical Standards
SaaS	Software as a Service
SLA	Service Level Agreement
SQL	Structured Query Language
TIBER	Threat Intelligence-based Ethical Red Teaming
TLS	Transport Layer Security