Position Paper

Requirements for standardisation

of compliant use of public cloud technology

in regulated European financial institutions

Version 2.0

22nd of February 2022

Contact: consultation@ecuc.group

Content

Glossary

API: Application Programming Interface

CSA: Cloud Security Alliance

CSP: Cloud Service Provider

DORA: Digital Operational Resilience Act

EBA: European Banking Authority

ECB: European Central Bank

ECUC: European Cloud User Coalition

EDPB: European Data Protection Board

EEA: European Economic Area

EC: European Commission

EU: European Union

FI: Financial Institution

FIPS: Financial Information Processing Standard

GDPR: General Data Protection Regulation

HSM: Hardware Security Module

IaaS: Infrastructure as a Service

ICT: Information & Communication Technology

PaaS: Platform as a Service

SLA: Service Level Agreement

TPP: 3rd Party Provider

1 Introduction

Cloud computing is fundamental to enable the digital transformation of the European financial sector. Founded in 2021, the European Cloud User Coalition (ECUC) seeks to support this transformation and enable compliant use of public cloud technology in European Financial Institutions (FI). Its primary objective is to develop a joint position on common challenges and solutions posed by Cloud Service Providers (CSP) and regulations.

Following the first Position Paper, published in May 2021, the aim of this second version is to address requirements to additional challenges experienced by the FIs, represented by the ECUC members, to ensure compliant and safe application of cloud technology. Solutions for our requirements are yet to be provided off-the-shelf by CSPs. Consequently, FIs currently need to implement resource demanding custom workarounds, thus hampering effective cloud implementations.

The positions outlined in this paper are an aggregated view of the ECUC members; derived from their experiences in public cloud adoption and focus on the following areas:

- Challenges with outsourcing to cloud services and meeting the related regulatory requirements
- Implications of upcoming policies such as Digital Operation Resilience Act (DORA) and recent rulings (like European Court of Justice ruling *Schrems II*)
- Considerable administrative efforts for all FIs engaging with CSPs on an individual basis, e.g. custom contractual agreements and cloud set-up

The Position Paper consists of six different sections addressing requirements regarding Privacy, Security, Governance & Regulation, Standard Contractual Clauses and Portability, Resilience and Exit-Strategy. In addition there is also our view on the Digital Operational Resilience Act (DORA).

This paper is addressed to the following audience:

- CSPs in their responsibility for offers to FIs
- Supervisors and policy makers such as the EBA, ECB and the EC

At this point, we may thank all partners for the fruitful discussions on the first Position Paper and looking forward continuing the dialogue to this updated Position Paper. To facilitate the implementation of our requirements, which may be regarded as an open standard for public cloud adoption, ECUC will publish a check list in 2022.

The ECUC Position Paper is subject to updates. Position Paper 2.0 replaces Position Paper 1.0. In comparison to Position Paper 1.0 it has major changes and additions. Please refer to the ECUC website (https://ecuc.group) for the most recent version.

Overall 22 European FIs are members of the ECUC.

Amongst others these are:

- *Allied Irish Bank Group*
- *Bank of Ireland Group*
- *BAWAG Group*
- *Belfius Bank*
- *Commerzbank AG*
- *Deutsche Börse AG*
- *DNB Bank ASA*
- *Deutsche Kreditbank AG*
- *EFG Bank AG*
- *Erste Group Bank AG*
- *Euroclear*
- *Gothaer Finanzholding AG*
- *ING Group N.V.*
- *KBC Bank NV*
- *Landesbank Saar*
- *Permanent TSB*
- *Raiffeisen Bank International*
- *Swedbank AB*
- *UniCredit S.p.A.*

2 Requirements on Privacy

Responsibility CSP

Personal data protection or privacy is about the protection of individuals with regards to the processing of personal data. This section specifies the requirements for privacy of individuals' data, both for employees and customers.

2.1 CSP must provide Personal Data Protection in Accordance with European General Data Protection Regulations

Data protection in public cloud environments is required to comply with the relevant European data protection regulations, in particular EU General Data Protection Regulation (EU) 2016/679[1] (GDPR), binding guidance of the European Data Protection Board, relevant European Court decisions, and European member state legislations. Within the EU and the European Economic Area (EU/EEA), GDPR is applicable for both, FIs (data-controller as cloud consumers) as well as for CSPs (data-processor).

As data processors, CSPs are independent of their place of business, accountable to provide adequate technical and organisational security and compliance measures in the European market. Such measures should be state of the art, include data protection by design and default, and aim to even go beyond setting the benchmark. Furthermore, European citizens need to be able to trust that their FI take measures to respect and protect their privacy, including both contractual and technical aspects of such a relationship.

2.2 CSP should provide supplementary Measures to enable effective GDPR Compliance in 3rd Countries

With regards to entering into contracts with CSPs established outside of the EU/EEA *(3rd countries)*, the European Court of Justice (C-311/18 *Schrems II*[2]) declared, that if applied standard contractual clauses ensure a GDPR equivalent environment for the individual, they can be an appropriate tool of transfer. Hence, the data controller (e.g. the FI) needs to ensure that the storage, transfer, and/or processing of data maintains GDPR equivalence does not increase the risks of, for instance, unauthorised 3rd country processing.

However, the outcome of adequacy evaluation and implementing contractual clauses potentially does not achieve a GDPR equivalent level of protection in the country the CSPs is established and/or where the data processing takes place. This is especially a challenge in countries where there are legislative requirements that authorizes public authorities to access data broadly beyond legitimate objective. Therefore this may interfere with the contractually agreed confidentiality to access any personal data where the FI is the controller and is

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[2] https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12312155

processed on its behalf by the CSP. The CSP should provide technical and organisational measures that ensure the compliance with GDPR in 3rd countries also.

2.3 CSPs need to implement basic Security Principles

In case a 3rd country can request access to personal data, according to the recommendations of the European Data Protection Board (EDPB[3]) and the Standard Contractual Clauses 2021/914 of the European Commission[4] (EU SCC 2021/914), data controllers and data processors should implement additional measures to ensure GDPR equivalent protection in the 3rd country.

These technical measures are typically based on the principles of data security, data minimisation, anonymisation or pseudo-anonymisation. In the case of pseudonymisation, the CSP should support an approach where additional information for attribution of personal data to a specific data subject shall remain under the exclusive control of the FI. All CSPs and cloud operating models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) are in scope for these requirements.

2.4 Cloud Services should facilitate Data Sovereignty by processing Data exclusively in the EU/EEA

With the declared invalidation of the EU-US Privacy Shield by the European Court of Justice (*Schrems II* decision), FIs as cloud consumers should be able to apply data localisation to a certain country or geographic region, i.e. EEA. Furthermore, all cloud services should support storing and processing of customer and individual data exclusively in a dedicated country or geographic region e.g. in the EU/EEA.

2.5 Global and regional Cloud Services must be made transparent to FIs

CSP must make it transparent what cloud services are operated only globally (so called Global services). In addition, CSPs must make transparent if a cloud service necessarily requires transfers and/or processes personal data outside the EU. This information must be publicly accessible at any time, and it must not be limited to cloud services that potentially transfer customer data outside the EU as an essential function of the service. In addition, the CSP must proactively inform their FI customers if they add or alter any privacy and data protection features and/or capabilities as well as and region expansion announcements as they are released.

[3] https://edpb.europa.eu/edpb_en
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN

2.6 Provide robust and multi region-based Global Services

CSP should ensure that global cloud services are hosted in multiple regions and must not rely on one region only. Alternatively, CSP must be transparent to their customers whether or not global services are localised in a single region.

2.7 Contractually agreed Data Processing Roles and Responsibilities must be adhered to by the CSPs

Although CSPs aim to have differentiated approaches concerning the roles of being a data processor for the FI and a data controller for own interests (e.g. data analytics), ECUC asks CSPs to refrain from any data processing going beyond what has been contracted with respect to the data of the FI. When involving a CSP as 3rd party in the processing of customer data[5], the FI needs to be confident that the involvement of the additional processing party does not increase the risk of unauthorized processing/access to such data. CSPs also need to ensure that the processing of customer data remains within the limits of the contract with the FI. After contract expiration all data shall be returned and the CSP needs to certify that all data has been deleted.

2.8 CSP should enable FIs to contract with EU based Legal Entities

CSPs should offer FIs to contract with their legal entities based in the EU. Trilateral contractual relationship between FIs and both, the CSPs EU and non-EU based legal entities, contain uncertainties in terms of "Who is responsible for the control and contractual safeguarding of data transfers to countries outside the EU?"

The ECUC regards the CSP EU based legal entities as the primary data processors for the personal data of the FI. If the CSP EU based legal entities send data to non-EU based CSP legal entities, the EU based legal entities is not only in breach of the contract but also act as data exporters, and thus being responsible to perform data transfer assessments and apply standard contractual clauses with their non-EU based entities.

2.9 CSP must assess the Impact of 3rd Country Transfers

The CSP must warrant that it has no reason to believe that the laws and practices in a 3rd country of destination, applicable to the processing of the personal data by one of its data importers, prevent such data importers from fulfilling its obligations under these clauses. This includes requirements to disclose personal data and/or measures authorising access by government authorities. It has to take due account of the specific circumstances of the transfer; the legislative requirements, practices, limitations and safeguards of countries of destination

[5] customer data: any sort of data inserted and generated by the FI as a cloud customer. What is not meant here is the differentiation of what this data is to the FI i.e. bank customer, employee data etc.

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.

The CSP shall conduct this assessment regularly (at least annually) in best efforts to continuously ensure compliance with obligations and to make the outcome with supporting information available to the FI upon request. A risk deemed low or medium by the CSP could be deemed differently by the FI due to its specific requirements. If the CSP has reason to believe that it can no longer comply with its commitments it shall immediately (at least within one day) inform the FI and identify appropriate protective measures. If instructed by the FI the data exporter should suspend the transfer in accordance with EU SCC 2021/914 Recital 17.

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.

2.10 CSP should achieve holistic Effectiveness of Encryption

In its Guideline on supplementary measures the EDPB emphasises the use of effective encryption as an adequate supplementary measure to the Standard Contractual Clauses to ensure adequate and effective protection in case of a data transfer outside of the EU/EEA or 3rd countries with established equivalence. Therefore, the ECUC encourages CSPs to seek and proceed in developing new encryption techniques and other data protection measures to protect the data adequate and effective at any given time.

Hence, guaranteeing encryption and ensuring that the encryption keys are kept under the full control of an EU entity is an option to legally transfer personal data e.g. data transferred to the US.

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 (i.e. data in use). Bring-your-own-key and hold-your-own-key approaches (using HSM technologies) are valuable first steps, but the CSP need to find a holistic approach towards trusted computing giving the FI the opportunity to stay fully in control and deny technically any 3rd party and even the CSP potential access to personal data in clear text.

2.11 Disclosure Request must be challenged by the CSP

The CSP shall review the legality of disclosure requests and challenge them if it concludes that the request is unlawful. The CSP therefore needs to pursue possibilities of appeal, seek interim measures with an objective to suspend the request and not disclose the personal data requested but instead forward the request to the individual FI. If disclosing, the CSP shall provide the minimum amount permissible.

The CSP shall notify the FI and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it receives a legally binding request or becomes aware of any direct access by public authorities. Prior

information should be given as soon as the CSP is made aware to give the FI the opportunity to object or limit access (CSP should support embedding a kill switch or similar technologies or procedures to block autonomously 3rd country access as soon such is identified).

Furthermore, the CSP should deny access before the affected FI was able to take actions. If the CSP is prohibited from notifying the FI and/or the data subject under the laws of the country of destination, the CSP shall ensure best efforts to obtain a waiver of the prohibition or forward the request to the FI, with the ambition to communicate as much information as possible and as soon as possible.

2.12 Transparency Reports must be provided by the CSPs

Where legally permissible in destination country, the CSP agrees to provide the FI, in regular intervals for the duration of the contract, with as much relevant information as possible on the requests received, in particular, number of requests, type of data requested, requesting authorities, whether requests have been challenged and the outcome of such challenges, etc. If the CSP acts as a data processor, it shall forward the information to the FI as data controller as quickly as possible.

2.13 CSP should provide Warrant Canary on Request of FI

Upon request, the CSP should provide information through a *Warrant Canary* or similar process to inform each FI on a regular basis (e.g. at least every 24 hours) that no access requests have been received from authorities acting against GDPR. This may be done e.g. by sending a cryptographically signed message informing the FI that as of a certain date and time it has received no order to disclose personal data or the like, if this is permitted by the regulation of the CSP place of business in a 3rd country. The CSP must ensure that its private key for signing the Warrant Canary is kept safe and that it cannot be forced to issue false Warrant Canaries by the regulations of the 3rd country, e.g. by appointing a person outside of the 3rd country jurisdiction. The absence of an update of this notification will indicate from FI perspective that the CSP may have received an order and enable the FI to take defence actions.

2.14 Personal Data Protection Audits should be supported

The CSP shall be able to demonstrate compliance with its contractual safeguard provisions. In particular, the CSP shall keep appropriate documentation on the processing activities carried out on behalf of the FI. The CSP shall make available all information necessary for the FI to demonstrate compliance with the obligations set out in these Clauses and at the FIs request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may consider relevant certifications held by the data importer.

The FI may choose to conduct the audit by itself, mandate an independent auditor or choose to perform the audit in a pooled audit together with other FIs. Audits may include inspections at the premises or physical facilities of the CSP and shall, where appropriate, be carried out with reasonable notice.

2.15 Personal Data Breaches must be reported immediately

In the event of a personal data breach processed for an FI including government request, the CSP shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The CSP shall also notify the FI without undue delay after having become aware of the breach and to allow the FI to report the breach latest within 72h to the respective regulator. Such notification shall contain a description of the nature of the breach including categories and numbers of affected data subjects and personal data), the details of a data protection officer or contact point where more information can be obtained, the likely consequences of the affected breach and the measures taken or proposed to address the breach and mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide all information at the same time, CSP shall send an initial notification containing the information then available and deliver further information as it becomes available without undue delay. The first notification of the breach must not be delayed by the CSP performing internal investigations on the question if this is a breach that needs to be notified as this assessment of this question is a prerogative of the FI as data controller.

2.16 CSP Personnel accessing Customer Data must be traceable

In the event where CSP support personnel need access to cloud services, FIs must be able to grant access, monitor and trail access made by such personnel. The CSP must provide details to trace and protocol these support access activities. There must be no backdoor where CSP support personnel accesses customer data/cloud services without the ability to trail. Amongst others these activities include internal support networks. The CSP must provide a reliable “technical vault mechanism” including surrounding controls and processes around to prevent unauthorized (administrative) access to customer data as well as meta data by any support party, CSP support personnel and sub-contractors.

3 Requirements on Security

Responsibility CSP

Information Security has the goal to ensure the security principles of confidentiality, integrity, and availability of data and services. As part of this goal, the following requirements should be fulfilled by the responsible CSP providing technical and organizational measurements to provide the appropriate baseline.

3.1 Strong and Transparent Data at Rest Security

Data at Rest refers to the storing of data. To fulfil this basic need for cloud customers, transparent and strong security in the cloud is a necessity. Therefore, CSPs should provide solutions to ensure adequate security is in place.

Firstly, a data encryption methodology should be implemented in such a way that the CSP cannot be forced to disclose the keys to decrypt customer data without approval, consent or knowledge of the data owners.

More precisely, a CSP should employ at least a level three, 140-2 Financial Information Processing Standard (FIPS) Hardware Security Module (HSM) which supports state of the art cryptographic processes as well as provides a scalable and managed Key Management System based on HSMs, including key import and re-import, rotation, re-encryption, grouping, and labelling. A CSP should also offer multiple methods for customers to encrypt data at rest, for example:

- Supply Your Own Key upon each request
- Bring Your Own Key into CSPs HSM
- External Key Management where key encryption keys reside outside CSPs HSM
- Privately hosted HSMs in a co-location.

Secondly, it should be transparent to cloud customers which encryption keys are used for specific actions or on what grounds they are updated, when data assets are encrypted and by whom, thus ensuring auditability.

A CSP should offer customers organisation-wide encryption policies and a central place to define Data at Rest encryption for all services. Furthermore it should enable all services to support the cryptographic key management options mentioned above as well as provide access sovereignty and access transparency logs to justify usage of cryptographic keys and provide a holistic dashboard for all key involvement.

3.2 Strong and Transparent Data in Transit Security

For FIs currently using public cloud services, it is often unclear to them where their data is transferred and how it is secured in transit. However, it should always be transparent to the FI how and where their data is being transferred, particularly the security measures in place to protect data-in-transit.

The CSP should use state of the art security to secure data-in-transit, e.g., TLS version 1.3. Hence, vulnerable data security protection should be avoided. To provide clarity on the data transport architecture, the CSP should provide a consistent, central place to configure and monitor data in transit security, rather than only per individual service. Also, a precise description of the CSP's internal data transfer channels and applied security measures should be made transparent to the FI. In addition, for each cryptographic process, a clear justification should be available and included in log files, e.g., certificate renewal.

3.3 Fully Featured Logging and Monitoring

To ensure full control of customer data assets, robust, and complete audit logging of all cloud application and service activity is required. This applies to both customer and CSP actions and the retention time should be defined by the customer. Logging and Monitoring includes customer service access (Access Transparency with approvals), CSP and customer admin access (Admin Activity/Read/Write), as well as data that have been accessed (Data Access/Read/Write). If only the CSP accesses customer assets, the customer should be provided with functionality to control effectively the access for this specific resource before any access happens.

A CSP should, for all services, consistently log identity, performed action, service usage, corresponding purpose, and involved data. Cloud customers should be able to access comprehensive logs to the service related activities on the platform; this could be provided via for instance an Application Programming Interface (API), a Graphical User Interface (GUI) or some other mechanisms to integrate with their own security logging systems. Furthermore, customer log data should not be shared with 3rd parties without the consent of the customer. With respect to monitoring, there is a lack of standardised monitoring interfaces across CSPs. Therefore, to leverage multiple CSPs, there should be a standardised monitoring interface provided across all services.

3.4 Data Exfiltration and Customer Policy Enforcement

Since data sharing is quite effortless to perform on the cloud, customers are interested in strictly controlled data sharing capabilities to prevent data exfiltration to unwanted locations.

Hence, CSP should provide consistent visibility and control of all workloads and communication flow perimeters regardless of location, size, or architecture. This also applies to communication between CSP services and 'private endpoints', including the direction of data flow (ingress/egress). A CSP should also provide an effective set of security posture management tools to enable customers to assess security configurations at a global cloud control layer in line with their security frameworks and standards.

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.

3.5 Service Certifications and Evidence

Certifications for cloud services assure an adequate level of security and therefore are one of the key requisites for all cloud users to rely upon. Hence, the services of a CSP should be independently certified by independent certification authority. The security certifications should at least include the de facto market standards for cloud technology[6], as well as further certifications that are specific to the financial industry[7].

A CSP should disclose evidence of certifications upon request to the customer. Furthermore, a CSP should provide its customers with the ability to conduct their own audits on the CSP.

3.6 Separation of Identities and Contacts

In the event an FI's identity and contact information are identical, there's a possibility that their associated contexts may get mixed up. A CSP should therefore provide the measures to associate federated and non-federated identities with valid routable contact information (i.e., email addresses) to ensure notifications are successfully delivered to the user. More precisely, identity identifier and contact information should be separated but able to be grouped by identities. For example, if an identity cannot be routed for notifications, at least a valid and routable email address should be able to be associated and used to send any notifications to and from the CSP.

A CSP should provide specific communication channels for certain event types, such as critical data and service events, e.g., data breaches, security issues, or technical blockers. This should be provided, in addition to email by other channels that can be configured by the customer.

3.7 Maturity of Data-in-Use Security

As of now, to achieve data-in-use security, the only generic and practical method in the industry is to rely on Trusted Execution Environments as part of the computing processors. This functionality is often referred to as Confidential Computing. This feature is only offered by some CSPs for a few selected services restricted to specific hardware specifications. To enable customers to protect their data during usage, the CSP should provide Confidential Computing or similar implementations as an option for a broad set of hardware configurations as well as backends of managed services.

[6] Cloud Security Alliance (CSA): Security, Trust & Assurance Registry Program (STAR) (CSA STAR); ISO/IEC: 27001, 27017, 27018; AICPA SSAE 18 / ISAE 3402 Type II: SOC 2.
[7] German Federal Office for Information Security: Cloud Computing Compliance Criteria Catalogue (C5:2020), Payment Card Industry Data Security Standards (PCI DSS).

3.8 Backup Functionality, High Availability, and Disaster Recovery

A CSP should provide a geo-redundant backup solution which is independent of the service's API enablement status. The backup functionality should support service independent storage locations and should not rely on 3rd parties. Also, the backup measure should be coherent with the shared responsibility model for the cloud service models for IaaS, PaaS, SaaS. This functionality should be provided by all services storing customer data or service configurations and be manageable through a single interface.

For business continuity reasons, cloud services should be available in both High Availability and Disaster Recovery mode, so as not to create a single point of failure for FIs. Furthermore, if the CSP performs business continuity and resilience exercises affecting customers, they should be informed of the process and able to veto.

Due to the central relevance of a Key Management System (KMS) to provide cryptographic processes, a solution should be in place that enables CSP services to perform cryptographic tasks even when the main KMS is unavailable. This holds true especially for single region services. 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.

While multi-regional services enable a geo-redundant setup, the set of single regions should be clearly defined for the multi-region. A CSP's customer should be able to customize a multi-region or select of several pre-defined multi-regions in the same geographical region.

3.9 Software Supply Chain Transparency

Customer assets such as applications run on various underlying infrastructure managed by the CSP. This consists also of software, such as operating systems and management tools. Since the layer below the customer's view is only available to the CSP, the responsibility for this software stack is with the CSP.

Therefore, a CSP should provide methods such as auditing processes and security evidence in order to provide transparency on its underlying software supply chain towards the customer. This helps FIs to comply with EBA requirements[8], where applicable CSP should provide detailed information to deliver the service chain.

3.10 IAM and Privilege Escalation

Assets, such as data of customers, reside in CSP's services and access to these are controlled via Identity & Access Management (IAM). This is a core feature and should be a foundation to build upon, where user access rules are defined, controlled and managed solely by the cloud customers. However, if this is not implemented correctly, the risk of privilege escalation may emerge (with associated risks such as identity theft and data leakage),

[8] EBA/GL/2019/02 Art. 13.1.67-80

resulting in higher privileges than users should have in the first place. It should not be possible to gain access to a system without proper IAM settings.

The CSP is responsible to deliver a sound IAM implementation across all its services in order 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.

3.11 Workload Isolation

Various workloads of different customers will reside at the same CSP. Therefore, it should never be possible to access any other customer's assets without explicit consent. This includes data, software, infrastructure, and containers or virtual machines.

The CSP should deliver evidence of periodic review of isolation controls that are effective including corrective measures. Updating systems and publishing reports will increase transparency.

3.12 Malware Defence

Due to the variety of services offered by a CSP, this enables different entry points for malware, such as ransomware.

For the parts of the shared responsibility model the CSP is responsible for, the malware needs to be kept away from customer systems while at the same time the customers should have the possibility to use specialized tools to prevent, detect, and mitigate malware impact. Thus, the CSP should provide a threat intelligence to isolate threats without disruption and alert the customer with the option to clean infected systems.

For the parts of the shared responsibility model the customer is responsible for, the CSP should offer tools to prevent misuse and infection of its services.

4 Requirements for Governance and Regulation

This section covers requirements for the management of risk associated with outsourced services, as well as its regulatory framework. In the latter case, the intention is not to move responsibility away from cloud customers or to lower the given standards, but to point out a more effective way of operationalisation.

4.1 Control measures on Outsourced Services

Responsibility CSP

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
- Defined, implemented and tested contingency measures for the used services and infrastructure
- Adequate contingency solutions to allow instant action to keep the service running or to fix problems
- Conditions upon which contingency measures can be justified when it comes to 3rd country data transfer
- Contingency measures that include or risk 3rd country data transfer should be made transparent in standard contractual clauses
- Supplied information should include the CSP supply chain and sub-outsourcing, where applicable.

4.2 CSP should provide Information for a sound 3rd Party Risk Management

Responsibility CSP

For a sound governance of 3rd Party Risk Management, CSPs should provide FIs with the following information for the used cloud services and infrastructure, that is deemed to be sufficient for an FI specific Business Continuity and Disaster Recovery Plans:

- Overview of cloud services including a detailed supply-chain service mapping of underlying dependent sub-contractors or sub-hosting services
- Supply-chain information detailing the roles and responsibilities of the underlying sub-contractors for the related cloud services
- Supply-chain information detailing the dataflow, data exchange and data location/region between the CSP and each sub-contractor for the related cloud services.

4.3 Exit Strategy Requirements

Attention EBA

The European Banking Authority (EBA) guidelines on outsourcing arrangements require FIs as part of their risk assessment to have an exit strategy in place when outsourcing any “Critical / Important function” to CSPs. This is to cover relevant exit triggering events, e.g. bankruptcy of CSP, sanctions, or a changing legal environment.

Relevant exit triggering events can be observed, and the occurrence anticipated. On that basis along with empirical data from such events, an exit and migration time slot can be defined to exit a cloud platform and migrate the bank critical service. We ask to outline feasible time slots for exit plan execution that is connected to the materiality assessment of the outsourcing.

4.4 CSP Audits and Oversight

We propose simplifications in audit procedures insofar as the cloud service offerings are not checked by every FI, but centrally at the CSP. We want to facilitate the implementation of regulatory requirements at CSPs:

Responsibility CSP

Collaborative audits organised by the financial industry should become a generally accepted approach by CSPs and free of charge. Different institutions form a collaborative team to audit one specific CSP. The audit results can be regarded valid within the respective individual institution. Collaborative audits are already supported by the EBA Guidelines on Outsourcing Arrangements (Art. 13.3.91.a).

Attention ECB

Currently CSPs are audited by European supervision along onsite inspections at Financial Institutes. On that basis a particular CSP is audited multiple times whenever Financial Institutes as CSP customers are inspected on their public outsourcing activities. National and European supervision are asked to form collaborative audit teams to audit CSPs across countries and for all Financial Institutions being customers of a CSP. Such an approach could improve consistency of observations, and additionally be more efficient. In addition, we point out that the systemic risk of the entire industry using CSP cannot be managed by individual institutions. However, the institutions specific cloud adoption is still inspected individually and resulting observations are assigned to the respective institution.

5 Requirements on Standard Contractual Clauses

Responsibility CSP

The ECUC appreciates the European Commission's work on "Model Contractual Clauses for Cloud" which covers privacy topics and will align the positions below in the upcoming public hearings.

CSPs should include the hereinafter described topics in their financial service addendum.

5.1 Audit Rights for Customers

To meet industry's obligations to audit, audit rights to data centres and its services, Customers Audit Rights should be granted per standard contractual clauses. There is also a need to audit the relevant infrastructure on a regular basis.

5.2 Sub-Outsourcing

In accordance with the EBA "Guidelines on Outsourcing Arrangements" (EBA/GL/2019/02 §14/15) the CSP provides information regarding sub outsourcing at any time without limitations. In addition, all changes are shown with a minimum advance of 90 days and a right of consultation. The CSP should ensure that the objections of FIs are examined favourably. In the event of use of unsuitable subcontractors, the FI should be granted a special right of termination including termination support.

5.3 Embedded URLs in Contracts and Service Level Agreements

CSPs should offer contracts that include a cost cap for subsequent periods. 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.

Likewise, the CSP should only change the service in a way that guarantees all cloud customers at least equal or improved services in terms of function, security, technology and data protection, or that a change or termination of the service will be announced with at least 18 months' notice.

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 without additional charge (without additional chargeable services).

The CSP should offer additional communication channels to transmit critical event and service level information (e.g. on data breaches, penetration test findings, logfiles for problem analysis) besides email and a definition of which channels are to be used for different types of information, e.g., via phone. All such events should be

available to the customer regardless if the CSP has concluded that the customer is impacted or not. The customer must have the possibility to assess impact and not only rely on the CSP impact analysis.

All deadlines, changes, and level of information should apply without exception to all consumers and not only to individual consumers.

Any changes to product terms (incl. FSA, DPA and SLA) should be highlighted on paragraph level in order to facilitate FI identification of the exact change and subsequent impact analysis. Documentation of changes should be logged by the CSP to allow for back-tracking what changes have happened over time.

5.4 CSP as Controllers or Processors

There should be clarification on the categorisation of CSPs as controllers or processors. CSPs no longer limit themselves to just being a processor.

In Accordance with "2.8 CSP to enable FIs to contract with EU based legal entities" the ECUC regards the CSP EU based legal entities as the primary data processors for the personal data of the FI.

5.5 Insurance

The contracts between CSPs and FIs should have an insurance clause that needs to increase with the number of assets on the cloud.

6 Requirements on Portability, Resilience and Exit-Strategy

Responsibility CSP

This section covers requirements to achieve portability of cloud application on the one hand and to ensure their resilience on the other hand. Please also refer to chapter 4.3 Exit Strategy Requirements.

Another important aspect is vendor lock-in, CSPs using proprietary technology that makes transferring data and/or services to other providers unfeasible. At a minimum the following conditions should be met by CSPs.

6.1 CSP should apply Technology Standards

CSP should make sure to apply technology standards of internationally recognised institutes to their services. These include:

- NIST (National Institute of Standards and Technology)
- ISO (International Organization for Standardization)
- CNCF (Cloud Native Computing Foundation)
- an institute that implements the general requirements for the EU Cybersecurity Act (EUCA) e.g. BSI (Bundesamt für Sicherheit in der Informationstechnik): C5 (Cloud Computing Compliance Criteria Catalogue)
- CSA (Cloud Security Alliance): STAR (Security, Trust, Assurance, and Risk)

In order to prove the certification of the standards of these bodies, the adherence to these standards should be publicly documented by the CSP.

6.2 CSP should offer Open-Source Technology and Standards

CSP should embrace open-source technology and provide such components as software stacks, interfaces, and APIs. The provided services should build upon or be efficiently referable to open-source solutions from the open-source community. Effective pre-checks as part of the system lifecycle management should be in place before using open-source technology.

This especially holds for standards in software, data, communication, and processes, which should be preferred in comparison to proprietary solutions.

6.3 CSP should provide methods and tools to allow Workload Portability

CSPs should strongly support FIs to perform their exit plans for their workloads, services and applications as required by European Banking Authority (EBA) guidelines on outsourcing arrangements.

CSPs should provide methods and tools to help migrate IaaS and PaaS to other IT service providers quickly and securely:

- The methods and tools provided should enable a seamless migration to the most widely used commercial and open-source infrastructures, networks, platforms, and databases (state of the art technologies). Tools provided should enable homogeneous and heterogeneous migrations from any supported source within the CSP environment to a state-of-the-art technology target environment.
- CSPs should provide tools to create infrastructure as a code-artifacts that describe existing resources and their properties in order to prepare for automated implementation in target environments.
- Licenses for on-premise (or equivalent) solutions for a fair price to ensure clients have the option to return to an on premise solution should an exit scenario occur.
- For SaaS, the CSPs should offer a version/installation which is compatible with other cloud platforms or provides other alternatives, such as licenses for desktop installations. The exception here would be SaaS CSP proprietary solutions that needs cloud-native capabilities to provide the service(s) to the customer. Alternatives are especially relevant for Office products and should ensure that a migration during an exit is realistic and economically possible. CSPs should respect the requirement for FIs to have an exit plan.

6.4 CSP should provide standardised Data Formats and Export Processes

CSP should provide standardised data formats and processes for data extraction and transport to other environments and platforms. The paragraph will only cover data portability and export requirements not already covered in other chapters, e.g. chapter 2 Requirements on Privacy:

- CSP should establish bi-directional data portability by providing contract/service contract/SLA, processes, products, data formats, metadata and professional services to customers for all data owned as intellectual property by the customer.
- Data portability includes both data and meta-data which give the data its meaning. Amongst others these are operational data, secrets, metadata and their backups as well.
- CSPs should establish processes that support the customer to execute data portability and export.
- CSPs should offer products and services that support the customer to execute bi-directional (in and out) online and offline (bulk) data portability. Data at rest and in transit should be secured and privacy needs to be ensured.
- Customers must be able to choose data portability products and services depending on the urgency, the data volume to exchange, different data querying (e.g. SQL) and representation (e.g. JSON) formats and cost.
- CSPs should enable open market standards (cf. “The Open Data Institute”[9]) (additional requirements in paragraph on “Technology Standards”) for:

[9] The ODI – Open Data Institute

- 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

- Example open standards to comply with:
  - Egeria[10]: opensource metadata standard, maintained by the LF AI & Data Foundation
  - SWIPO[11] develops Codes of Conduct for the proper application of the EU Free Flow of Non-Personal Data Regulation / Art. 6 "Porting of Data"
- Where requested by the customer, the CSP should offer professional services in support of data portability and export.

6.5 CSP should harmonize Ingress and Egress Costs

CSPs charge customers when they export data (so called egress cost) from the cloud to anywhere else. Compared to importing data exporting data is usually more expensive. Portability of applications and data is required in certain scenarios and in most cases part of the required exit strategy. FIs must have an exit strategy in place. The cost of leaving a cloud infrastructure or a service due to substantial egress cost contrasts with this requirement:

CSPs should harmonize ingress and egress costs or provide ways for temporary and agreed exceptions to the costs so that when an exit is required it can be achieved in an economical way.

6.6 CSP should provide detailed Information on Data Centre Location

FIs should know CSPs' data centre physical locations to ensure proper planning for resilience and portability. Data Centre information within every availability zone or region needs to be provided in a standardised format and made available directly to FIs as part of contractual obligations. Information is needed to support:

- Mitigation of risks of CSP data centre outages and impacts of regional disaster events impacting multiple CSP data centres
- A clear understanding that each data centre has access to separate power supplies and utility services as well as redundant paths that are isolated from the other data centres (in the same location / region).

[10] Open metadata standard schema by GitHub: https://odpi.github.io/egeria-docs/
[11] SWIPO (Switching Cloud Providers and Porting Data): https://swipo.eu/

6.7 CSP should safeguard Interoperability of selected Data Centres

It is common to establish at least two interoperable but independent data centre locations, meeting national localisation requirements for redundant implementation to shift workload and to allow disaster recovery. Examples of standards to be implemented in the CSP DC-migration solution:

- Service modelling: Open-SCA (service composition and interaction), USDL/SoaML/CloudML (multi-view services), EMML (mashups)
- Service interfaces: OCCI (infrastructure management), CIMI (infrastructure management), EC2 (de-facto standard), TOSCA (portability), CDMI (data management)
- Infrastructure: OVF (virtual machines)
- CSPs should provide a managed and supported data centre migration option leveraging existing standards according to the related domains.

6.8 CSP should run independent Network Connections

CSPs should establish and provide multiple independent network connection options to ensure that communication and applications, are still available in the chosen data centres/regions when (hazardous) incidents occur. Also, operational and scheduled maintenance of these network connection must be independent and respect clients' configuration, ensuring that no back-up connection is unintentionally stopped. In more detail, it should be ensured that at least one stable connection is provided by the CSP at all times and that backup and main connections are not in maintenance mode at the same time.

7 Digital Operational Resilience Act

Addressed EC

The Digital Operation Resilience Act (DORA) has been published by the European Commission as a proposal for the Financial Sector. The aim is to make the financial sector safer, unifying and simplifying compliance with existing regulation on information and communication technology (ICT) risk management and security. Taking this into account and not to hinder the use of cloud computing, while respecting its particularities, we have the following recommendations. Generally, a period of 36 months should be provided for the implementation of DORA once it enters into force.

7.1 Lex Specialis

DORA should be the "lex specialis" and requires clear precedence over the NIS 2 or the RCE Resilience of Critical Entities directive (RCE) proposals regarding scope:

- This should be clarified in the respective articles of NIS 2 / RCE and not only in recitals, further FIs shall be excluded from the list of entities within the respective annex of NIS 2 and RCE.
- This would unify ICT-related incident reporting and address overlapping reporting requirements.

7.2 EBA and ESMA Guidelines should be aligned with DORA Requirements

The EBA "Guidelines on ICT and security risk management" (EBA/GL/2019/04) and the ESMA "Guidelines on outsourcing to cloud service providers" should be aligned once DORA requirements are published to avoid fragmentation and to maintain clarity.

7.3 TIBER Framework for Threat Led Pen Testing should be reused

Given the positive experience with the ECB's TIBER-EU framework for cyber resilience testing, this framework should be used instead of developing new standards by the ESAs. Therefore, a reference to the Tiber-EU framework should be included. In addition, we advocate within the EU for mutual recognition of Threat Led Penetration Test results.

7.4 DORA should be aligned with Industry Standards

The definitions of DORA should be aligned with industry standards to avoid regulatory fragmentation. We believe the industry should help define the "state of the art" of technology and terms used within DORA which should be aligned with global standards and key definitions. Here we advocate for proportionality and a risk-based approach as well.

7.5 The Designation of critical ICT 3rd Party Service Providers is not fully defined

The scope of the oversight framework should be clarified regarding entities based outside of the EU and servicing EU FIs entities.

7.6 Intra-group Relationships should be out of Scope of DORA

Intra-group relationships should be classified as non-3rd-party relationships for the purpose of the DORA requirements. The principle of proportionality should be extended to all requirements considering a risk-based approach.

7.7 More Clarification is needed for the effective Assessment of sub-contracting Chains

This requirement should be aligned with the EBA Outsourcing Guidelines for consistency with existing approaches. Further clarity on the roles and responsibilities of these different stakeholders should be provided to ensure regulatory certainty and efficiency of reporting and oversight.

7.8 Multi-Vendor Approach is not necessary to mitigate Concentration Risks

The multi-vendor approach requirement should be excluded in DORA. In the current market it is not feasible to force a multi-vendor strategy upon FIs in order to mitigate concentration risk and limit vendor lock-in as many ICT services are not easily interchangeable, and it negatively impacts complexity of the market, costs, and agility.

7.9 Acknowledged Certification Schemes should be promoted

Acknowledged certification schemes, recognised by supervisory authorities for 3rd party provider (TPP) as well as a central consortium for assessing TPP's risks, should be promoted.

7.10 Reviews and Assessments should take a risk-based Approach

Reviews and assessments should be scheduled to take a risk-based approach and not on a uniform annual cycle:

- There should be a certification scheme based on prescribed criteria to show the TPP is fit and certified to deliver services to FIs.
- It is important that oversight information is transparent and can be used by FIs to decrease their own monitoring on these providers as they can trust on the Lead Overseer.

- The termination of contractual arrangements by the competent authority should not be a standard enforcement tool, but only a measure of last resort.

7.11 The definition of "intra-group Service Provider" should be sufficiently flexible

We acknowledge that an intra-group service provider should predominantly provide services to financial entities within the same group or to financial entities belonging to the same institutional protection scheme. However, a certain threshold for exceptions should be applied to ensure a certain level of flexibility.

7.12 Communication to Clients should be proportional and have informative Value

While annual communication on ICT threats is welcomed, we want to emphasise that it needs clear and workable definitions. To prevent over-information we propose to disclose all major incidents with relevant impact for clients and counterparts. This would exclude incidents that did not have any relevant impact and therefore aren't of interest to the clients.

7.13 Termination of Contract

While termination of contract is and will continue to be the last resort, we think any additional burden for FIs to terminate their contracts with CSPs are counterproductive.

8 Outlook

As with the publication of the first ECUC Position Paper the publication of Version 2.0 will be followed by a consultative process. The consultation phase serves to collect feedback from CSPs, regulatory bodies and other regulated institutions. The feedback will be incorporated into the future works and initiatives of the Coalition.

The ECUC represents the position of the member institutions. Refer to our website. We kindly ask you to use the following contacts:

consultation@ecuc.group	For questions upon the Position Paper e.g. from CSPs
press@ecuc.group	For inquiries from media and press
https://ecuc.group/	Website

*