Position Paper

Requirements for standardisation

of compliant use of public cloud technology

in regulated European Financial Institutions (FIs)

Version 3.0

26th of February 2025

Contact: info@ecuc.group

Table of contents

1 Introduction 7
2 Requirements on Privacy 9
2.1 CSPs are required to provide Personal Data Protection in Accordance with European General Data Protection Regulation (GDPR) 9
2.2 CSPs should provide supplementary Measures to enable effective GDPR Compliance in 3rd Countries 9
2.3 CSPs need to implement basic Security Principles 9
2.4 Cloud Services should facilitate Data Sovereignty by offering Services processing Data exclusively in the EU/EEA 10
2.5 Global and Regional Cloud Services must be made Transparent to FIs 10
2.6 Contractually agreed Data Processing Roles and Responsibilities must be adhered to by the CSPs 10
2.7 CSPs should enable FIs to contract with EEA based Legal Entities 11
2.8 CSPs must assess the Impact of 3rd Country Transfers 11
2.9 CSPs should achieve holistic Effectiveness of Encryption 11
2.10 Disclosure Request must be challenged by the CSPs 12
2.11 Transparency Reports must be provided by the CSPs 12
2.12 CSPs should provide Warrant Canary on Request of FI 12
2.13 Personal Data Protection Audits should be supported 13
2.14 Personal Data Breaches must be reported immediately 13
2.15 CSPs personnel Accessing Customer Data must be traceable 13
3 Requirements on Security 14
3.1 Strong and Transparent Data at Rest Security 14
3.2 Strong and Transparent Data in Transit Security 15
3.3 Fully Featured Logging and Monitoring 15
3.4 Data Exfiltration and Customer Policy Enforcement 16
3.5 Service Certifications and Evidence 16
3.6 Separation of Identities and Contacts 16
3.7 Maturity of Data-in-Use Security 16
3.8 Backup Functionality, High Availability, and Disaster Recovery 17
3.9 Software Supply Chain Transparency 17
3.10 IAM and Privilege Escalation 17
3.11 Workload Isolation 18
3.12 Malware Defence 18

4 Requirements on Governance and Organisation 18
4.1 Control Measures on outsourced Services 19
4.2 CSPs should provide Information for a sound 3rd Party Risk Management 19
4.3 CSPs Audits and Oversight 19
5 Requirements on Contractual Clauses 20
5.1 Data 20
5.2 Resilience 20
5.3 Audit Rights 20
5.4 Sub- Contracting 20
5.5 Service Descriptions and Service Level Agreements 21
5.6 Termination 22
6 Requirements on Portability, Resilience and Exit 23
6.1 Exit Strategy Requirements 23
6.2 CSPs should apply internationally recognized Standards 23
6.3 CSPs should offer Open-Source Technology and Standards 23
6.4 CSPs should work towards creating Portability Standards for Commodity Services 24
6.5 CSPs should provide Methods and Tools to allow Workload Portability 24
6.6 CSPs should provide Standardised Data Formats and Export Processes 24
6.7 CSPs should be transparent about Ingress and Egress Costs 25
6.8 CSPs should provide detailed Information on Data Center Location 25
6.9 CSPs should run independent Network Connections 26
6.10 Routing of Data in Transit 26
7 ECUC's Positions on DORA 27
7.1 General Feedback on DORA 27
7.2 RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework under Article 15 and 16(3) of Regulation (EU) 2022/2554 27
7.3 RTS to specify the policy on ICT services supporting critical or important functions under Article 28(2) Regulation (EU) 2022/2554 28
7.4 Draft RTS on subcontracting ICT services supporting Critical and Important Functions under Article 30(5) of Regulation (EU) 2022/2554 28
7.5 DORA Harmonization with Industry Standards 28
7.6 Certification Schemes 29
7.7 DORA Section II Oversight Framework of Critical ICT Third-Party Service Providers (CTPPs) and accompanying Documents 29
7.8 Technical Advice on the Criteria for CTPPs and Fees for Oversight Framework under Articles 31 and 43 of Regulation (EU) 2022/2554 30
7.9 Challenges on DORA 30
8 Outlook 31

Changelog

The third version of the position paper has some minor and major changes. To ease the reading if you've already read and analysed the ECUC Position Paper 2.1, we've highlighted the most important ones here. To get the exact details of the changes, please read the corresponding chapters.

We've listed the changes based on the chapter numbers from the previous version.

Chapter number in version 2.1	Change	Chapter number in version 3.0
1. Introduction		
	Small changes	
2. Requirements on Privacy		
2.1	Small changes	2.1
2.2	Reformulation of the requirement	2.2
2.3	Small clarifications	2.3
2.4	Small clarifications	2.4
2.5	Small clarifications	2.5
2.6	Chapter has been removed	
2.7	Small clarifications	2.6
2.8	Small clarifications	2.7
2.9	Small clarifications	2.8
2.10	Small clarifications	2.9
2.11	Small clarifications	2.10
2.12	Formatting changes	2.11
2.13	Formatting changes	2.12
2.14	Formatting changes	2.13
2.15	Small clarifications	2.14
2.16	Small clarifications	2.15
3. Requirements on Security		
Intro	added explanation	Intro
3.1	Small clarifications	3.1
3.2	Small clarifications	3.2
3.3	Small clarifications	3.3
3.4	Small clarifications	3.4
3.5	Small clarifications	3.5
3.6	Small clarifications	3.6
3.7	Formatting changes	3.7
3.8	Small clarifications	3.8
3.9	Small clarifications	3.9
3.10	Formatting changes	3.10
3.11	Small clarifications	3.11
3.12	Small clarifications	3.12
4. Requirements on Governance and Organisation		
Intro	title changed, remark regarding DORA	Intro
4.1	Formatting change	4.1
4.2	Formatting change	4.2
4.3	Chapter moved to subchapter 6.1	
4.4	Changed with respect to DORA	4.3

5. Requirements on Contractual Clauses		
Intro	Small changes	Intro
	Added	5.1
	Added	5.2
5.1	Changes and clarifications	5.3
5.2	Major changes	5.4
5.3	Major changes	5.5
5.4	Chapter removed	
	Added	5.6
6. Requirements on Portability, Resilience and Exit		
	Added	6.1
6.1	Small changes	6.2
6.2	Small changes	6.3
	Added	6.4
6.3	Small clarifications	6.5
6.4	Small changes and clarifications	6.6
6.5	Changes	6.7
6.6	Small clarifications	6.8
6.7	Chapter removed	
6.8	Small clarifications	6.9
	Added	6.10
7. ECUC's Positions on DORA		
	Due to DORA taking effect on 17th January 2025, the main chapter with all sub-chapters have been re-written.	
8. Outlook		
	Small changes	

Glossary

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

1 Introduction

Established in 2021, the European Cloud User Coalition (ECUC) seeks to support cloud transformation and enable the compliant use of public cloud technology in European financial institutions (FIs). Enabling the use of cloud computing is fundamental to achieving digital transformation of the European financial sector. The ECUC aims to reach its goals by developing joint positions on common challenges that European FIs experience with solutions provided by non-European Cloud Service Providers (CSPs) and with requirements set by European legislators.

Following the first ECUC Position Paper, published in May 2021, the aim of this third version is to address updated challenges experienced by ECUC members as we seek to ensure the compliant and safe use of cloud technology by European FIs. The positions outlined in this paper are the aggregated views of ECUC´s members, derived from their experiences in public cloud adoption. As Position Paper 3.0 has major changes and additions it replaces Position Paper 2.1.

This paper is mainly addressed to CSPs in relation to their responsibilities for supplying services to European FIs but is also addressed to policy makers such as the European Commission (EC), the European Supervisory Authorities (ESA) and National Competent Authorities (NCAs).

When the term CSP is used in this document, ECUC shall mean service providers providing services in accordance with the essential characteristics and service models of the NIST definition of cloud computing. In this sense, neither banks nor insurance companies are referred to as cloud service providers.[1] This paper consists of five chapters: Privacy, Security, Governance & Organisation, Contractual Clauses, and Portability, Resilience & Exit. These chapters also include discussions on the implementation of the Digital Operation Resilience Act[2] (DORA). Focus is on the relationship between cloud adoption and the following regulatory requirements:

- Challenges with outsourcing to non-European cloud services
- Implications of court rulings (such as Schrems II) and regulations (such as DORA)
- The considerable administrative overhead for all FIs engaging with CSPs on an individual basis, e.g. custom contractual agreements, and cloud set-up.

References are also made to the ECUC Checklist, which translates the Position Paper into questions, including references to regulatory requirements and international standards. 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 will allow CSPs to structure their solutions in a manner that matches the legal, regulatory and technical requirements of the financial sector.

The Position Paper 3.0 is supplemented by a chapter on DORA, which clarifies the position of the ECUC and provides feedback to those responsible on the Lex specialis.

The ECUC would like to thank all partners for the fruitful discussions on the Position Paper and we look forward to continued dialogue in relation to the topics covered herein.

Please always refer to the ECUC website (www.ecuc.group) to find the most recent version.

[1] The NIST Definition of Cloud Computing: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf
[2] Publications Office: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

32 European FIs are members of the ECUC. Amongst others these are:

ABN AMRO Bank N.V., Allied Irish Banks, Bank of Ireland, BAWAG Group, BayernLB, Belfius Bank, Berenberg, Commerzbank AG, Creditplus Bank AG, Deutsche Börse AG, Deutsche Kreditbank AG, Deutsche Pfandbriefbank AG, DNB Bank ASA, Erste Group, Euroclear, Gothaer Finanzholding AG, ING Groep N.V., KBC Bank NV, Landesbank Saar, Nordea Bank Abp, OP Financial Group, PTSB, Raiffeisen Bank International, Swedbank AB, Traton Financial Services AB and UniCredit S.p.A.

2 Requirements on Privacy

Addressed to CSP

Personal data protection, or privacy, concerns the protection of individuals with regards to the storage and processing of personal data. This section specifies the requirements for privacy of individuals' data for employees, customers, and other natural persons whose data is stored and/or processed.

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[3]), 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.

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*[4]) 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.

2.3 CSPs need to implement basic Security Principles

According to the recommendations of the European Data Protection Board (EDPB[5]) and the Standard Contractual Clauses 2021/914 of the European Commission (EU SCC 2021/914[6]), data controllers and data processors should implement additional measures to ensure GDPR equivalent protection

[3]REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation): https://eur-lex.europa.eu/eli/reg/2016/679/oj
[4]CURIA - Dokumente:https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode-=lst&dir=&occ=first&part=1&cid=12312155
[5] EDPB | European Data Protection Board: https://edpb.europa.eu/edpb_en
[6] L_2021199EN.01003101.xml: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN

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.

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[7], 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.

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.

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[8], 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.

[7] EU Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-U.S. Data Privacy Framework, OJ L 231/118, 20.9.2023; similar developments in relation to the UK and Swiss, see https://www.dataprivacyframework.gov/EU-US-Framework.

[8] 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 e.g., bank customer, employee data etc.

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.

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.

2.9 CSPs should achieve holistic Effectiveness of Encryption

In its Guideline[9] 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

[9] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board: https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

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.

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.

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.

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.

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.

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.

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.

3 Requirements on Security

Addressed to CSP

Information Security has the purpose of ensuring the security principles of confidentiality, integrity, and availability of data and services. When making use of cloud, the shared responsibility model is commonly used to describe the division of responsibilities between CSPs and customers. The image below clearly depicts how the responsibilities of the customer shift to the CSPs the higher one goes in the cloud stack (OnPrem->SaaS). In this section we will refer to the shared responsibility model when defining CSPs requirements.

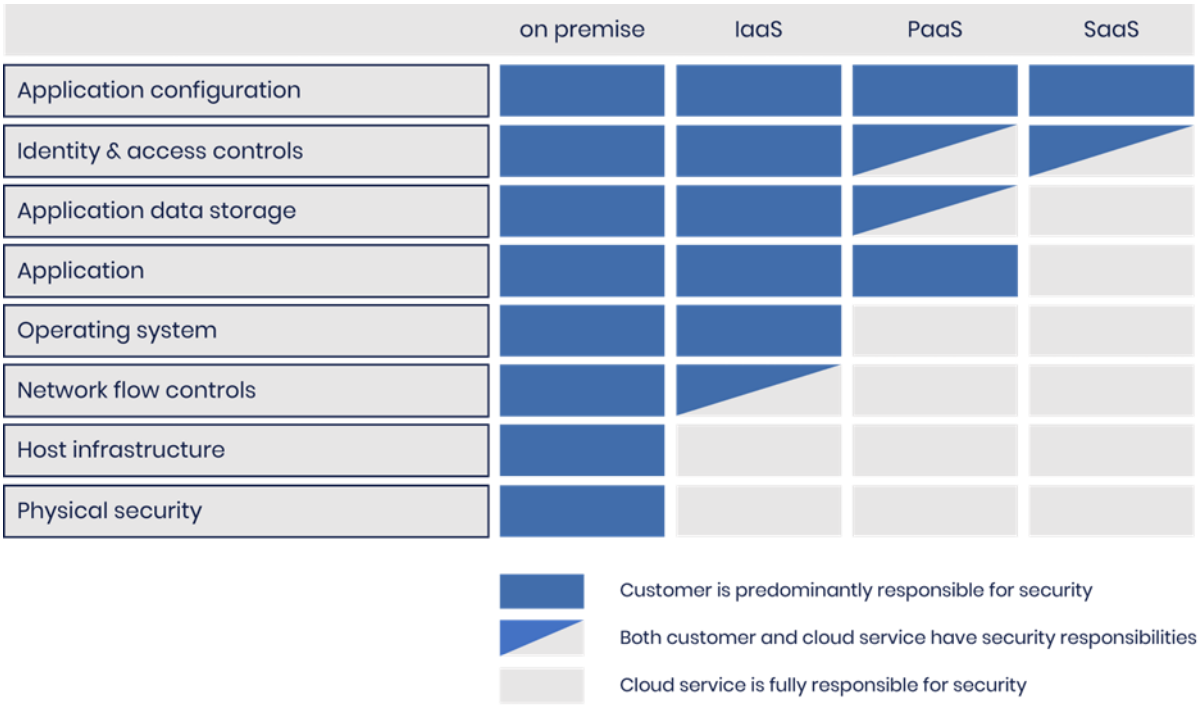

Figure: Cloud Shared Responsibility Model (Source: UK NCSC)

The following requirements should be fulfilled by the responsible CSPs providing technical and organizational measurements to secure an appropriate baseline in line with the shared responsibility model.

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.

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.

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.

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. 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. Also, a precise description of the CSPs 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 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). 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.

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 systems. Furthermore, customer log data should not be shared with 3rd parties without the explicit consent of the customer. 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).

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.

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). 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 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. The security certifications should at least include the de facto market standards for cloud technology[10], as well as further certifications that are specific to the financial industry[11].

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.

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.

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.

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

[10] 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.
[11] German Federal Office for Information Security: Cloud Computing Compliance Criteria Catalogue (C5:2020), Payment Card Industry Data Security Standards (PCI DSS).

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.

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. This functionality should be provided for 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 CSPs perform business continuity and resilience exercises affecting customers, the customers should be informed of the process and have the ability to veto.

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. 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. CSPs customers should be able to customize a multi-region or select from several pre-defined multi-regions in the same geographical region.

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[12] and DORA requirements. Where applicable CSPs should also provide detailed information related to the delivery of its service chain.

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

[12] EBA/GL/2019/02 Chap. 13.1, Para. 76-80): https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf

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.

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.

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.

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.

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.

4 Requirements on Governance and Organisation

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.

The topics are directly related to DORA Regulation (EU) 2022/2554, CHAPTER II ICT risk management, Section I, Article 5 Governance and Organisation and include, among others:

- Article 6: ICT risk management framework
- Article 11: Response and Recovery
- Article 13: Learning and evolving

From ECUCs point of view, the following points represent topics that require appropriate standardization in the design between the provider and the customer.

4.1 Control Measures on outsourced Services

Addressed to 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 and
- Supplied information should include the CSPs´ supply chain and sub-outsourcing, where applicable.

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

Addressed to CSP

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.

4.3 CSPs Audits and Oversight

Attention EBA, ECB, NCA

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.

Addressed to CSP

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).

5 Requirements on Contractual Clauses

Addressed to CSP

The ECUC appreciates the use of Standard Contractual Clauses as envisaged by DORA. At the same time our Financial Institutions determine that extensive follow-up activities like renegotiations are required. To avoid intensive and costly negotiations, the ECUC recommends including the following topics in providers Financial Services Addendums (FSA).

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.

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.

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).

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.

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.

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.

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.

In accordance with EBA Guidelines on Outsourcing and DORA, CSPs should provide clear financial obligations within the contract. 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 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, or that a change or termination of the service will be announced with a prenotification period and without undue delay.

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.

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.

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.

All terms, changes, and level of information should apply without exception to all FIs and not only to individual institutions.

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.

6 Requirements on Portability, Resilience and Exit

Addressed to CSP

This section covers requirements to achieve portability of cloud applications on the one hand and to ensure their resilience on the other hand. 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 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.

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.

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.

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.

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[13].

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.

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:

[13] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302854

- 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.
- 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.
- 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.
- CSPs should enable open market standards (cf. "The Open Data Institute"[14]) (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
- Example open standards to comply with: Egeria[15]: opensource metadata standard, maintained by the LF AI & Data Foundation
- Where requested by the customer, the CSPs should offer professional services in support of data portability and export.

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.

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

[14] The ODI – Open Data Institute: https://theodi.org/
[15] Open metadata standard schema by GitHub: https://odpi.github.io/egeria-docs/

- 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).

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.

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.

7 ECUC's Positions on DORA

Attention EC, ESAs, ECB, NCAs

In comparison to the prior chapters where we focus on technical aspects assigned to different addressees, we now concentrate on the lex specialis DORA and address the European Commission as they are the party responsible. To provide one all-encompassing document, we have integrated our former separate paper 'ECUC's Positions on DORA' in this chapter.

DORA, the Digital Operation Resilience Act - Regulation (EU) 2022/2554, aims to increase the resilience of the European financial sector by unifying and simplifying compliance with existing regulation on risk management and security of information and communication technology (ICT). The regulation entered into force on 16th January 2023 and applies from the 17th of January 2025. DORA includes several supporting technical acts (Regulatory Technical Standards RTS/Implementing Technical Standards ITS), which contain more practical aspects related to governance and reporting requirements. Public consultations on these supporting acts have been held and the official publications of these documents were published in the second half of 2024 – which created a challenge for all institutions that were required to be compliant with the regulation by January 2025. The ECUC welcomes DORA and its ambitions to ensure that necessary safeguards are in place to mitigate growing cyber-attacks and other ICT-risks to increase financial organizations digital resilience. Even though DORA in the short term will have a high impact on financial institutions ability to use cloud computing. We also appreciate the harmonization with other legal standards and frameworks where appropriate and look forward to and appreciate the oversight of designated critical ICT third-party service providers (TPPs).

7.1 General Feedback on DORA

Taking this into account and not to restrict the use of cloud computing further we have the following comments:

- Article 4 introduces the principles of proportionality for a practice-oriented implementation of DORA. These should be used for ICT-risk management, ICT-related incident management and resilience testing. We believe that competent authorities should also take the principles into account when reviewing ICT-risk management frameworks.
- As the requirements resulting out of DORA are very complex and deadlines were very tight, it has been difficult for European FIs to implement them fully, especially considering that some supporting legislative texts are pending adoption and publication in the Official Journal.

7.2 RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework[16] under Article 15 and 16 (3) of Regulation (EU) 2022/2554

The ECUC provided feedback to European Supervisory Authorities´ consultation on the draft RTS on ICT-Risk Management Framework. With the provision of the final draft, clarifications and improvements have been introduced in various areas of the RTS. The clarification of proportionality principles, ICT project and change management, encryption and cryptography, risk-based approach,

[16] JC 2023 86 - Final report on draft RTS on ICT Risk Management Framework and on simplified ICT Risk Management Framework: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-_Final_report_on_draft_RTS_on_ICT_Risk_Management_Framework_-_and_on_simplified_ICT_Risk_Management_Framework.pdf

the reduction of overlap with other requirements and omission on details of security awareness programs and governance are especially welcomed.

On network security, we acknowledge and appreciate the change in the final version with regards to documentation of networks and data flows which earlier required mapping of them. However, the requirement to review ICT systems supporting critical or important functions at least every 6-months causes particular concern (RTS Article 13 (1), lit. h). For larger organizations, given the multitude of systems in operation, this will in practice result in organizations conducting continuous, rolling reviews.

The ECUC positions and possible solutions to relevant topics can be found in the specific chapters of the ECUC Position Paper and related ECUC Checklist.

7.3 RTS to specify the policy on ICT services supporting critical or important functions[17] under Article 28 (2) Regulation (EU) 2022/2554

With reference to the RTS which specifies the policy on ICT services supporting critical or important functions Article 3(3), stating "a methodology for determining which ICT services support critical or important functions", an alternative proposal would be to refer to the ICT services supporting critical/important functions as outlined within the Register of Information.

7.4 Draft RTS on subcontracting ICT services supporting Critical and Important Functions under Article 30 (5) of Regulation (EU) 2022/2554

DORA's ambition to give the financial sector greater control over the sub-outsourcing chain is a noble goal, and highly relevant in the context of cloud outsourcing. However, there is a large gap between reality and the envisaged objectives.

According to the ECUC, to properly determine the relationship between cloud users and CSPs, and avoid discussions, we welcome a more detailed legislation, including extensive explanation of the elements that should be taken into account when deciding upon the acceptability of subcontracting.

Without withholding the financial entity's final responsibility, ECUC is also in favour of allowing CSPs to give assurance that their sub outsourcing chains have adequate abilities, expertise, resources, controls, etc. on which assurance the FIs are only required to perform marginal checks.

7.5 DORA Harmonization with Industry Standards

DORA also aims to harmonize with other industry standards and regulations, this is something that we appreciate, however in some areas it may require further clarification. Below are some areas where harmonization is desirable:

- Threat led penetration testing has been aligned with most of the requirements from the TIBER EU framework, we also noticed that there have been enhancements or improvements to the requirements provided in DORA such as purple teams, allowing internal testers for a certain period. This leaves the question of the future role for TIBER-EU.

[17] JC 2023 84 - Final report on draft RTS to specify the policy on ICT services supporting critical or important functions: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_84_-_Final_report_on_draft_RTS_to_specify_the_policy_on_ICT_-services_supporting_critical_or_important_functions.pdf

- The policy on the use of ICT services is incorporating requirements from the EBA Guidelines on Outsourcing Arrangements such as due diligence, risk assessments and exit strategy. However, the data points on the register of information for third parties and sub-contractors are overly detailed and require some practicality in terms of implementation.
- The requirements on incident reporting are extracted from repealed PSD2 requirements and further enhanced by removing the complications of working days to submit interim and final reports. However, with the new DORA timelines and regulatory reporting requirements it is not explicitly specified whether we need to continue reporting based on FI's regulatory requirements. It is prudent to unify ICT-related incident reporting and address overlapping reporting requirements.
- For network and information security, DORA is considered lex specialis, the provisions of DORA relating to ICT risk management (Article 6 et seq.), management of ICT-related incidents and, in particular, major ICT-related incident reporting (Article 17 et seq.), as well as on digital operational resilience testing (Article 24 et seq.), information-sharing arrangements (Article 45) and ICT third-party risk (Article 28 et seq.) shall apply instead of those provided for in the NIS 2 Directive. The DORA precedence holds true also for the Critical Entities Directive (CER).

7.6 Certification Schemes

We would encourage ESAs to establish standardized certification schemes to facilitate third party assurance. For instance, financial entities could rely on standard certification schemes such as ISO 27001, SOC II, EU Cloud Certification Scheme and other internationally accepted standards. This should not limit the use of using third parties which do not have certifications, in which case the financial entity should take appropriate measures to ensure assurance.

7.7 DORA Section II Oversight Framework of Critical ICT Third-Party Service Providers (CTPPs) and accompanying Documents

The requirements for direct oversight of designated CTPPs described under DORA Section II and the associated RTS on harmonisation of oversight activities [18] and Joint Guidelines on oversight cooperation [19] leave potential for customers, ICT TPPs and supervisors unused. The ECUC encourages the following items to be considered for future adjustments and enhancements.

The ECUC would appreciate if the ESAs could provide audit catalogues and audit results to all (contractual) parties to achieve full transparency and to avoid multiple audits of the same subject areas, which is not conducive to safety.

Alternatively, the ECUC proposes that the monitored CTPPs make the full results available to their clients in order to provide transparency on the scope and outcome of the supervision. In particular, since serious or unresolved findings are intended for further mitigation, the proposed practice would also - in a positive sense - create transparency and certainty about the proper and DORA-compliant management by CTPPs.

[18] JC 2024-35 - Final report on RTS on harmonisation of conditions for OVS conduct: https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-35_-_Final_report_on_RTS_on_harmonisation_of_conditions_for_OVS_conduct.pdf

[19] JC-GL-2024-36_Guidelines_on_DORA_oversight_cooperation.pdf: https://www.esma.europa.eu/sites/default/files/2024-11/JC-GL-2024-36_Guidelines_on_DORA_oversight_cooperation.pdf

7.8 Technical Advice on the Criteria for CTPPs and Fees for Oversight Framework[20] under Articles 31 and 43 of Regulation (EU) 2022/2554

Regarding the Commission Delegated Regulation specifying the criteria for designation of ICT TPPs as critical for financial entities, the ECUC maintains that:

- The criteria do not take concentration risk on a member state level into account (a provider can be critical on a national level but according to the proposed criteria and calculation method would not be considered critical on the EU level)
- The criteria do not consider what type of service an ICT TPP provides (ICT service vs e.g. the provision of market data)
- The criteria to assess systematic impact of the ICT TPP is based on a number of financial entities serviced but does not take into account the size of financial entities (e.g. by number of customers/size of the market)
- The criteria to determine criticality or importance of the function could be divided to distinguish between criticality and the number of very critical functions
- The criteria to estimate the degree of substitutability should have been based on the total assets instead of number of financial entities of a category of financial entities.

DORA describes how oversight fees are calculated based on the turnover of a CTPP which are the revenues generated in the EU from the provision of defined ICT services (see Article 28 (9) of Regulation (EU) 2022/2554).

We propose an effort-based approach that explicitly promotes the transparency of service providers in auditing and creates positive incentives. Effort could be reflected e.g. like this:

Effort-related coefficient in year (n) = hours of ESA oversight performance for a CTPP concerned in year (n-1) / hours of all ESA oversight performance for all critical ICT third-party services in year (n-1).

7.9 Challenges on DORA

The ECUC foresees several challenges implementing DORA such as:

- First and foremost, the timelines to implement are relatively short for a regulation that has several levels of details that are yet to be finalized. For instance, some RTSs of the second batch were finalized and delegated very late.
- Although there is a certain level of harmonization with other frameworks, the definitions provided in DORA are very broad for ICT services and thus increasing the scope of activities to be performed by multiple folds. In certain cases, the definitions are too vague or not provided leaving room for interpretation.
- DORA emphasises time and again regarding harmonization with other standards and frameworks like TIBER EU framework, EBA guidelines, where we see multiple overlaps. However there is no clarity that we do not have to double report or completely stop activities on other frameworks once DORA is adopted.

[20] Joint-ESAs__response_to_the_Call_for_advice_on_the_designation_criteria_and_fees_for_the_DORA_oversight_framework_final.pdf: https://www.esma.europa.eu/sites/default/files/2023-09/Joint-ESAs__response_to_the_Call_for_advice_on_the_designation_criteria_-and_fees_for_the_DORA_oversight_framework_final.pdf

8 Outlook

The ECUC Position Paper represents the positions of the member institutions. In general, there will be updates of the ECUC Position Paper and the corresponding ECUC Checklist, when new regulations, recognized standards or new experiences by implementing them occur.

Refer to our website www.ecuc.group.

For all questions upon ECUC, inclusive Position Paper please contact us via info@ecuc.group.