EUCS: controversial data sovereignty issues continue to drive debate for cloud services

12 June 2024

The European Union Cloud Services Scheme ("EUCS") is a certification framework for cloud services introduced under the EU Cybersecurity Act. Currently still under consultation, the EUCS, once finalised, will be implemented by relevant EU bodies, with the European Union Agency for Cybersecurity ("ENISA") likely playing a key role. The first EUCS draft was published in December 2020, and since then there have been several proposals and revisions to the scheme. The most contentious points to have emerged throughout the drafting of the EUCS are the requirements relating to governing law and sovereignty. The outcome will have a significant impact on EU and non-EU cloud service providers and businesses across the EU that rely on cloud services.

Background

The European Union Cloud Services Scheme ("**EUCS**") is one of three certification schemes being developed by the European Union Agency for Cybersecurity ("**ENISA**") under the EU Cybersecurity Act. These certification schemes have two key purposes: (1) to enhance the level of cybersecurity for ICT products, services and processes across the EU; and (2) to harmonise cybersecurity standards and avoid fragmentation within the EU between multiple certification schemes in different Member States.

The EUCS, once established, will allow cloud service providers ("**CSPs**") to voluntarily obtain a certification to demonstrate that their services adhere to high standards of security for the protection of customers. The certification scheme is being developed by ENISA and is expected to supersede existing national certification schemes after a transition period. The EUCS is an integral part of the European Commission's broader strategy to enable access to secure, sustainable, and interoperable cloud infrastructure and services for European businesses and public authorities. This broader strategy complements existing and upcoming EU cybersecurity laws including the second Network and Information Security Directive ("**NIS2**"), which requires Member States to impose a variety of cybersecurity and incident reporting obligations on various entities including cloud service providers.

It is too soon to say exactly when the EUCS will become operational or what the final certification requirements will entail, in part due to controversy over unresolved certification requirements. Following the publication of the first draft of the text on 22 December 2020, there have been several revisions. Among the most controversial developments are the governing law and sovereignty requirements which seek to ensure that CSPs are not subject to non-EU laws and regulatory powers. We consider the current state of play below.

Who does the EUCS apply to?

The EUCS is applicable to cloud services. “Cloud services” covers any ICT service implementing one or more capabilities offered via cloud computing invoked using a defined interface (a definition based on ISO17788). The EUCS is intended to cover a wide range of services, from Infrastructure as a Service, Platform as a Service and Software as a Service to small application services with limited reliance on cloud computing.

Only CSPs will be able to apply for EUCS certification. The EUCS is intended to assist customers to make informed decisions about the security of certain cloud services.

Whilst the certification is voluntary under the EUCS, NIS2 provides EU Member States with the ability to require ‘essential’ or ‘important’ entities to only use EUCS certified ICT services. Therefore CSPs providing services to these entities may in practice need to obtain certification under the EUCS. It could also become commonplace for customers to require EUCS certification as a requirement of a tender.

Certification Requirements

The EUCS assigns three assurance levels to the CSPs: ‘basic’, ‘substantial’ or ‘high’. The assurance level indicates that the CSPs have met the corresponding security requirements and evaluation assigned to that level.

Since the release of the draft EUCS in December 2020 for public review, there have been ongoing discussions and revisions to the proposed requirements for certification, particularly in relation to the ‘high’ assurance level which include demanding requirements that are close to state-of-the-art.

We focus below on some of the key requirements that cloud services industry players should be aware of. It should be noted that these requirements are not necessarily set in stone as changes may be made before the EUCS text is finalised.

Internal Controls

CSPs must separate conflicting tasks and responsibilities to reduce the risk of unauthorised or unintended changes or misuse of cloud customer data processed, stored or transmitted by the cloud service. CSPs must also monitor the competency and integrity of their internal and external employees and employees with direct or indirect access to EU customer data, including through support operations, need to be located in the EU, and must undergo specific screening or be supervised by an EU-based employee who has passed an appropriate review. Where access is supervised, this must be done through a secure solution whereby the supervisor can authorise or prevent actions of employees and ask for explanations in real-time.

1. **Risk Assessment**

CSPs must assess risks related to non-EU legislation that may have extra-territorial application. This includes the risk of foreign governments or authorities obtaining access to commercially sensitive information and trade secrets.

2. **Obligations to Customers**

CSPs must include in their contract with customers an undertaking that they will only consider investigation requests issued under EU law or the national law of a Member State. This is coupled with an obligation on the CSP to take organisational and technical measures to ensure no other investigation requests are considered. CSPs will also have to inform their customers about any residual risk and provide all the relevant information upon request from customers to allow them to perform their own risk assessment.

3. **Traditional Security Controls**

CSPs must implement robust security controls including with respect to network security, storage, encryption, penetration tests and audits. The exact measures required will vary according to the assurance level.

4. **Governing Law**

Contracts between CSPs and their customers must be governed by the laws of an EU Member State, and only the courts, tribunals or arbitration bodies from an EU Member State can have jurisdiction to settle any disputes arising from such contracts. This requirement applies to all three levels of assurance.

5. **Data Localisation**

All data processing activities must take place in the EU unless cloud customers have agreed to some limited exceptions. In practice, this would mean non-EU CSPs having to rely on a trusted service provider located in the EU to deliver certain trusted services such as the validation of electronic signatures.

6. **Digital Sovereignty**

Perhaps most controversially, cloud services and their accompanying data must be located within the EU, and CSPs must register their head office and global headquarters in a Member State to be able to obtain certification under the EUCS. According to publicly available information, the sovereignty requirement has since been removed from the latest EUCS draft in 2024 but there have been calls to reinstate this (see below).

Sovereignty Requirement: latest position

The latest EUCS draft in Q1 2024 has not been officially published, but according to reports there is no longer the pre-requisite that a CSP is headquartered in the EU in order to meet the highest assurance level. However, the removal of the sovereignty requirement is not necessarily a closed issue.

The sovereignty requirement was removed following strong pressure from Member States and certain industry bodies, including a joint statement from AmCham EU, BSA, CCIA Europe and ITI objecting to the sovereignty requirement on the basis that it would create significant barriers for non-EU headquartered companies to enter into the EU cloud market and create complex legal compliance procedures.

However, other industry bodies are applying pressure to Member States in the Council to reintroduce the sovereignty requirement. For example, an Industry Letter dated 10 April 2024 whose signatories included Airbus, Orange among other European companies, urged Member States to “reject any proposals that

remove sovereignty requirements" in order to mitigate the risk of data being accessed under foreign laws, ensure harmonisation of sovereignty requirements in the EU and therefore offer customers clarity and transparency about the level of protection of their hosted data.

Certain Member States have been eager to increase national digital sovereignty. For example, the French National Assembly voted in favour of the "SREN Bill" on 10 April 2024, a bill which creates digital sovereignty requirements and prevents foreign governments from gaining unauthorised access to certain types of data.

France also maintains a national cybersecurity certification scheme, 'SecNumCloud', that prohibits non-EU providers from government procurement (and it remains unclear whether national schemes will or can continue to operate once the EUCS comes into effect).

A compromise on the sovereignty requirement was proposed by Belgium, who suggested drawing a distinction between "functional" requirements and "sovereignty" requirements, with the main scheme dealing only with the functional requirements, and sovereignty requirements being satisfied by filing an International Company Profile Attestation. This proposal, however, was not welcomed by signatories of the Industry Letter mentioned above.

Voting on the EUCS – originally scheduled for 15 April 2024 – has been delayed, but is expected to take place in the coming months.

Next Steps

The requirements for certification under the EUCS are still under discussion. Given that voting has been delayed and the sovereignty issue may be reopened, it is difficult to anticipate when the EUCS text will finally be agreed. Cloud services industry players should continue to monitor developments until then, especially CSPs supplying important or essential entities under NIS2.

For CSPs whose customers are financial entities operating in the EU, they will also be focusing closely on the requirements of the Digital Operational Resilience Act (DORA). The financial sector's reliance on ICT services, including cloud, is a key focus for supervisory authorities and the European Central Bank's consultation and guidance on outsourcing to CSPs could significantly impact CSPs by increasing the demands that customers have on them with respect to the location of hosted data.

Authored by John Salmon, Louise Crawford, Lavan Thasarathakumar, Daniel Lee, Alex Nicol, and Joyce Hoi Wun Leung.